This document is scheduled to be published in the
Federal Register on 04/14/2023 and available online at
**federalregister.gov/d/2023-05775**, and on **govinfo.gov**

BILLING CODE 8011-01P

**SECURITIES AND EXCHANGE COMMISSION**

**17 CFR Parts 242 and 249**

**[Release No. 34-97143; File No. S7-07-23]**

**RIN 3235-AN25**

**Regulation Systems Compliance and Integrity**

**AGENCY:** Securities and Exchange Commission.

**ACTION:** Proposed rule.

**SUMMARY:** The Securities and Exchange Commission ("Commission" or "SEC") is proposing amendments to Regulation Systems Compliance and Integrity ("Regulation SCI") under the Securities Exchange Act of 1934 ("Exchange Act"). The proposed amendments would expand the definition of "SCI entity" to include a broader range of key market participants in the U.S. securities market infrastructure, and update certain provisions of Regulation SCI to take account of developments in the technology landscape of the markets since the adoption of Regulation SCI in 2014. The proposed expansion would add the following entities to the definition of "SCI entity": registered security-based swap data repositories ("SBSDRs"); registered broker-dealers exceeding an asset or transaction activity threshold; and additional clearing agencies exempted from registration. The proposed updates would amend provisions of Regulation SCI relating to systems classification and lifecycle management; third party/vendor management; cybersecurity; the SCI review; the role of current SCI industry standards; and recordkeeping and related matters. Further, the Commission is requesting comment on whether significant-volume alternative trading systems (ATSs) and/or broker-dealers

using electronic or automated systems for trading of corporate debt securities or municipal securities should be subject to Regulation SCI.

**DATES:** Comments should be received on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

**ADDRESSES:** Comments may be submitted by any of the following methods:

Electronic comments:

- Use the Commission's internet comment form (https://www.sec.gov/rules/proposed.shtml); or
- Send an email to rule-comments@sec.gov. Please include File Number S7-07-23 on the subject line.

Paper comments:

- Send paper comments to, Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

All submissions should refer to File Number S7-07-23. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method of submission. The Commission will post all comments on the Commission's website (https://www.sec.gov/rules/proposed.shtml). Comments are also available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549 on official business days between the hours of 10 a.m. and 3 p.m. Operating conditions may limit access to the Commission's Public Reference Room. All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment

submissions. You should submit only information that you wish to make available publicly.

Studies, memoranda, or other substantive items may be added by the Commission or staff to the comment file during this rulemaking. A notification of the inclusion in the comment file of any materials will be made available on our website. To ensure direct electronic receipt of such notifications, sign up through the "Stay Connected" option at www.sec.gov to receive notifications by email.

**FOR FURTHER INFORMATION CONTACT:** Heidi Pilpel, Senior Special Counsel; David Liu, Special Counsel; Sara Hawkins, Special Counsel; Gita Subramaniam, Special Counsel; Josh Nimmo, Special Counsel; An Phan, Special Counsel, at (202) 551-5500, Office of Market Supervision, Division of Trading and Markets, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

**SUPPLEMENTARY INFORMATION:** The Commission is proposing amendments to the following rules under the Exchange Act and conforming amendments to Form SCI.

| Commission Reference | CFR Citation (17 CFR) |
|---|---|
| Rule 1000 | § 242.1000 |
| Rule 1001 | § 242.1001 |
| Rule 1001(a) | § 242.1001(a) |
| Rule 1001(a)(2) | § 242.1001(a)(2) |
| Rule 1001(a)(2)(v) | § 242.1001(a)(2)(v) |
| Rule 1001(a)(2)(vi) | § 242.1001(a)(2)(vi) |
| Rule 1001(a)(2)(vii) | § 242.1001(a)(2)(vii) |
| Rule 1001(a)(4) | § 242.1001(a)(4) |
| Rule 1002 | § 242.1002 |
| Rule 1002(b) | § 242.1002(b) |
| Rule 1002(b)(4)(ii)(B) | § 242.1002(b)(4)(ii)(B) |
| Rule 1002(b)(5) | § 242.1002(b)(5) |
| Rule 1002(b)(5)(i) | § 242.1002(b)(5)(i) |
| Rule 1002(b)(5)(ii) | § 242.1002(b)(5)(ii) |
| Rule 1002(c) | § 242.1002(c) |
| Rule 1002(c)(3) | § 242.1002(c)(3) |
| Rule 1002(c)(4) | § 242.1002(c)(4) |

| | |
|---|---|
| Rule 1002(c)(4)(i) | § 242.1002(c)(4)(i) |
| Rule 1002(c)(4)(ii) | § 242.1002(c)(4)(ii) |
| Rule 1003 | § 242.1003 |
| Rule 1003(b) | § 242.1003(b) |
| Rule 1003(b)(1) | § 242.1003(b)(1) |
| Rule 1003(b)(2) | § 242.1003(b)(2) |
| Rule 1003(b)(3) | § 242.1003(b)(3) |
| Rule 1004 | § 242.1004 |
| Rule 1004(a) | § 242.1004(a) |
| Rule 1004(b) | § 242.1004(b) |
| Rule 1005 | § 242.1005 |
| Rule 1005(c) | § 242.1005(c) |


I. Introduction

II. Background and Overview

A. History of Regulation SCI

B. Current Regulation SCI

1. SCI Entities and SCI Systems

2. Reasonably Designed Policies and Procedures

3. SCI Events

4. Systems Changes and SCI Review

5. Business Continuity and Disaster Recovery Testing with Members/Participants

6. Recordkeeping and Other Provisions (Rules 1005-1007)

C. Overview of Proposed Amendments to Regulation SCI

III. Proposed Amendments to Regulation SCI

A. Definition of SCI Entity

1. Evolution: Current and Proposed SCI Entities

2. New Proposed SCI Entities

3. General Request for Comment on Proposed Expansion of SCI Entities

B. Request for Comment Regarding Significant-Volume Fixed Income ATSs and Broker-Dealers Using Electronic or Automated Systems for Trading of Corporate Debt Securities or Municipal Securities

1. Discussion

2. Request for Comment

C. Strengthening Obligations of SCI Entities

1. Systems Classification and Lifecycle Management

2. Third-Party Provider Management

3. Security

4. SCI Review

5. Current SCI Industry Standards
6. Other Changes
D. SCI Entities Subject to the Exchange Act Cybersecurity Proposal and/or Regulation S-P
1. Discussion
2. Request for Comment
IV. Paperwork Reduction Act
A. Summary of Collections of Information
B. Proposed Use of Information
1. Rule 1001 of Regulation SCI
2. Rule 1002 of Regulation SCI
3. Rule 1003 of Regulation SCI
4. Rule 1004 of Regulation SCI
5. Rule 1005 and 1007 of Regulation SCI
6. Rule 1006 of Regulation SCI
C. Respondents
D. Total Initial and Annual Reporting Burdens
1. Rule 1001
2. Rule 1002
3. Rule 1003
4. Rule 1004
5. Rule 1005
6. Rule 1006
7. Summary of the Information Collection Burden
E. Collection of Information is Mandatory
F. Confidentiality of Responses to Collection of Information
G. Request for Comment
V. Economic Analysis
A. Introduction
B. Baseline
1. New SCI Entities
2. Existing SCI Entities:
3. Current Market Practice
4. Other Affected Parties
C. Analysis of Benefits and Costs of Proposed Amendments
1. General Benefits and Costs of Proposed Amendments
2. Expansion to New SCI Entities

3. Specific Benefits and Costs of Regulation SCI Requirements for All SCI Entities
D. Efficiency, Competition, and Capital Formation Analysis
E. Reasonable Alternatives
1. Limiting the Scope of the Regulation SCI Provisions for New SCI Entities
2. Mandating Compliance with Current SCI Industry Standards
3. Requiring Diversity of Back-Up Plan Resources
4. Penetration Testing Frequency
5. Attestation for Critical SCI System Vendors
6. Transaction Activity Threshold for SCI Broker-dealers
7. Limitation on Definition of "SCI Systems" for SCI Broker-Dealers
VI. Regulatory Flexibility Act Certification
A. "Small Entity" Definitions
B. Current SCI Entities
1. SCI SROs
2. The MSRB
3. SCI ATSs
C. Proposed SCI Entities
1. SBSDRs
2. SCI Broker-dealers
3. Exempt Clearing Agencies
D. Certification
Statutory Authority

## I. Introduction

The U.S. securities markets are among the largest and most liquid in the world, attracting a wide variety of issuers and broad investor participation, and are essential for capital formation, job creation, and economic growth, both domestically and across the globe. The fair and orderly functioning of the U.S. securities markets is critically important to the U.S. economy. In 2014, recognizing the decades-long transformation of many U.S. securities markets from primarily manual markets to those that had become almost entirely electronic and highly dependent on sophisticated technology, including

complex and interconnected trading, clearing, routing, market data, regulatory, surveillance and other technological systems, the Commission adopted 17 CFR 242.1000 through 242.1007 ("Regulation SCI") to supersede and replace the Commission's voluntary Automation Review Policy Program ("ARP") and certain provisions of 17 CFR 242.300 through 242.304 ("Regulation ATS").[1] Regulation SCI, which applies to "SCI entities" with respect to their "SCI systems" and "indirect SCI systems," was the Commission's first formal extensive regulatory framework for oversight of the core technology of the U.S. securities markets.

The U.S. securities markets have demonstrated resilience since the adoption of Regulation SCI, with some market observers crediting Regulation SCI in helping to ensure that markets and market participants were prepared for the unprecedented trading volumes and volatility experienced in March 2020 at the onset of the COVID-19 pandemic.[2] The U.S. securities markets continue to experience changes and new challenges, however. The growth of electronic trading allows ever-increasing volumes of securities transactions in a broader range of asset classes to take place at increasing speed by competing trading platforms, including those offered by broker-dealers that play

---

1 *See* Securities Exchange Act Release No. 73639 (Nov. 19, 2014), 79 FR 72252 (Dec. 5, 2014) ("SCI Adopting Release").

2 *See, e.g.*, Shane Remolina, *Is Remote Trading Leading to a Paradigm Shift on the Trading Desk?*, Traders Magazine (May 20, 2020), *available at* www.tradersmagazine.com/departments/buyside/is-remote-trading-leading-to-a-paradigm-shift-on-the-trading-desk (observing "no outages" at the stock exchanges in Mar. 2020 in contrast to "glitches" experienced in 2000s); Financial Industry Regulatory Authority, Inc. ("FINRA"), *Market Structure & COVID-19: Handling Increased Volatility and Volumes* (Apr. 28, 2020), *available at* https://www.finra.org/media-center/finra-unscripted/market-structure-covid19-coronavirus (observing that market infrastructure and integrity held during the challenges in Mar. 2020, and crediting Regulation SCI, among other regulatory protections).

multiple roles in the markets.[3] In addition, new types of registered entities that are highly dependent on interconnected technology have entered the markets.[4] The prevalence of remote workforces, furthered by the COVID-19 pandemic,[5] and increased outsourcing to third-party providers, including cloud service providers, continue to drive the markets' and market participants' reliance on new and evolving technology.[6] While these advances demonstrate the dynamic and adaptable nature of the U.S. securities markets and market participants, the greater dispersal, sophistication, and interconnection of the technology underpinning our markets bring potential new risks. These risks include not only the heightened risk of exposure to cybersecurity events from threat actors intent on doing harm, but also operational systems problems that can and do arise inadvertently.

As the Commission has acknowledged, Regulation SCI is not, nor can it be, designed to guarantee that SCI entities have flawless systems.[7] Rather, its goals are to

---

3 *See, e.g.*, Securities Industry and Financial Markets Association ("SIFMA"), *SIFMA Insights: Electronic Trading Market Structure Primer* (Oct. 2019*), available at* https://www.sifma.org/wp-content/uploads/2019/10/SIFMA-Insights-Electronic-Trading-Market-Structure-Primer.pdf (summarizing electronic trading history and trends in different markets). *See also* SEC *Staff Report on Algorithmic Trading in U.S. Capital Markets* at 16-19, 37 (Aug. 5, 2020), *available at* https://www.sec.gov/files/marketstructure/research/algo_trading_report_2020.pdf (discussing broker-dealer ATSs and internalizers, and other in-house sources of liquidity, such as single-dealer platforms ("SDPs"), and central risk books operated by broker-dealers) ("Algorithmic Trading Report"). Staff reports, Investor Bulletins, and other staff documents (including those cited herein) represent the views of Commission staff and are not a rule, regulation, or statement of the Commission. The Commission has neither approved nor disapproved the content of these staff documents and, like all staff statements, they have no legal force or effect, do not alter or amend applicable law, and create no new or additional obligations for any person.

4 *See infra* section III.A.2.a (discussing registered SBSDRs).

5 *See* FS-ISAC, *Navigating Cyber 2021* (Apr. 2021), *available at* https://www.fsisac.com/navigatingcyber2021-report. *See also* Vikki Davis, *Combating the cybersecurity risks of working home*, Cyber Magazine (Dec. 2, 2021), *available at* https://cybermagazine.com/cyber-security/combating-cybersecurity-risks-working-home.

6 *See, e.g.*, Angus Loten, Cloud Demand Drives Data Center Market to New Records, Wall St. J. (Feb. 27, 2020); Angus Loten, CIOs Accelerate Pre-Pandemic Cloud Push, Wall St. J. (Apr. 26, 2021).

7 *See* SCI Adopting Release, *supra* note 1, at 72291, 72351.

strengthen the technology infrastructure of the U.S. securities markets and improve its resilience when technology falls short.[8] To help achieve these goals, the regulation requires that SCI entities have 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 requires measures that facilitate the Commission's oversight of securities market technology infrastructure.[9] Consistent with the goals of addressing technological vulnerabilities and improving oversight of the core technology of key U.S. securities market entities, the Commission is proposing amendments to Regulation SCI that would expand its application to additional key market participants and update certain of its provisions to take account of the evolution of technology and trading since the rule's adoption in 2014. The application of Regulation SCI to a broader range of entities together with updates to certain provisions – including to account for heightened cybersecurity risks, wider use of cloud service providers, and the increasingly complex and interconnected nature of SCI entities' systems – should help ensure that the technology infrastructure of the U.S. securities markets remains robust, resilient, and secure.

---

[8] *See id.* at 72257.

[9] *See generally* SCI Adopting Release, *supra* note 1, at 72299, 72372, 72402, 72404-05.

The Commission has issued other proposals related to cybersecurity that would apply to SCI entities as well as other entities under the Commission's jurisdiction.[10] Regulation SCI, currently, and as proposed to be amended, however, differs from these proposals in terms of its purpose and scope. Regulation SCI applies to entities designated as key market participants because they play a significant role in the U.S. securities markets and/or have the potential to impact investors, the overall market, or the trading of individual securities in the event of a systems issue. Regulation SCI requires key market participants to (i) have policies and procedures in place to help ensure the robustness and resiliency of their market technology systems, and (ii) provide certain notices and reports to the Commission, and in some cases, market participants, to facilitate Commission

---

[10] These include a proposal to adopt new rules requiring broker-dealers, major security-based swap participants, national securities exchanges, national securities associations, security-based swap data repositories, security-based swap dealers, transfer agents, and the Municipal Securities Rulemaking Board ("MSRB") to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks to their "information systems" and notify the Commission and the public of significant cybersecurity incidents affecting their information systems. *See* Securities Exchange Release No. 97142 (Mar. 15, 2023), 88 FR 20212 (April 5, 2023) (proposing 17 CFR 242.10) (for ease of reference, this proposal is referred to as the "Exchange Act Cybersecurity Proposal"). *See also* Securities Exchange Release No. 97141 (Mar. 15, 2023), 88 FR 20616 (April 6, 2023) (proposing to amend 17 CFR part 248, subpart A ("Regulation S-P"), to, among other things, require broker-dealers, investment companies, SEC-registered investment advisers, and transfer agents to adopt incident response programs to address unauthorized access to or use of customer records and information, including procedures for providing timely notification to individuals affected by an information security incident designed to help affected individuals respond appropriately) ("Regulation S-P 2023 Proposing Release"). *See infra* section III.D (discussing of how SCI entities would be affected if the Exchange Act Cybersecurity Proposal, Regulation S-P 2023 Proposing Release, and this proposal are all adopted as proposed). In addition, the Commission has pending proposals to address cybersecurity risk with respect to investment advisers, investment companies, and public companies. *See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Release Nos. 33-11028, 34-94917, IA-5956, IC-34497 (Feb. 9, 2022), 87 FR 13524 (Mar. 9, 2022) ("IA/IC Cybersecurity Proposing Release"); *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11038, 34-94382, IC-34529 (Mar. 9, 2022), 87 FR 16590 (Mar. 23, 2022). The Commission has reopened the comment period for the IA/IC Cybersecurity Proposing Release to allow interested persons additional time to analyze the issues and prepare their comments in light of other regulatory developments, including the proposed rules and amendments regarding this proposal, the Exchange Act Cybersecurity Proposal and the Regulation S-P 2023 Proposing Release. The Commission encourages commenters to review those proposals to determine whether they might affect their comments on this proposing release.

oversight of securities market infrastructure. While Regulation SCI has cybersecurity aspects and certain of the proposed amendments to Regulation SCI would update policies and procedures requirements designed to keep SCI systems and indirect SCI systems secure, the proposed amendments are designed, more broadly, to ensure that SCI entities (current and proposed) have systems technology adequate to maintain operational capability of the systems on which the maintenance of fair and orderly markets depend.

## II. Background and Overview

### A. History of Regulation SCI

The Commission adopted Regulation SCI in 2014 to supersede and replace the Commission's legacy voluntary ARP Program as well as certain provisions of Regulation ATS.[11] In doing so, the Commission sought to strengthen the technology infrastructure of the U.S. securities markets, reduce the occurrence of systems issues in those markets, improve their resiliency when technological issues arise, and establish an updated and formalized regulatory framework, thereby helping to ensure more effective Commission oversight of such systems.[12] Several factors contributed to the Commission's decision to adopt this regulation. Recognizing the growing importance of technology in the securities markets, the Commission issued the ARP I and ARP II Policy Statements in 1989 and 1991, respectively.[13] In the decades that followed, key market participants in the securities industry increasingly relied on ever more complex technologies for trading and clearance and settlement of securities. The increased reliance on technology introduced

---

[11] *See generally* SCI Adopting Release, *supra* note 1.

[12] *See* SCI Adopting Release, *supra* note 1, at 72252–56 (discussing the background of Regulation SCI).

[13] *See* Securities Exchange Act Release Nos. 27445 (Nov. 16, 1989), 54 FR 48703 (Nov. 24, 1989), and 29185 (May 9, 1991), 56 FR 22490 (May 15, 1991).

challenges for the securities markets, as evidenced by a variety of market disruptions occurring in a relatively short time period.[14] The Commission convened a roundtable entitled "Technology and Trading: Promoting Stability in Today's Markets" ("Technology Roundtable") in 2012.[15] Shortly thereafter, following Superstorm Sandy on the U.S. East Coast, the U.S. national securities exchanges closed for two business days in light of concerns over the physical safety of personnel and the possibility of technical issues.[16] These and other developments in U.S. securities markets led the Commission to consider the effectiveness of the 1980s and 90s-era ARP Program. The focus of the ARP Program was to ensure that the self-regulatory organizations ("SROs") had adequate capacity, security, and business continuity plans by, among other things, reporting to the Commission staff their planned systems changes 30 days in advance and reporting outages in trading and related systems.[17] While the ARP Policy Statements were rooted in

---

[14] *See* Securities Exchange Act Release No. 69077 (Mar. 8, 2013), 78 FR 18083, 18089 (Mar. 25, 2013) ("SCI Proposing Release") (citing, among other things, Findings Regarding the Market Events of May 6, 2010, Report of the Staffs of the Commodity Futures Trading Commission ("CFTC") and SEC to the Joint Advisory Committee on Emerging Regulatory Issues (Sept. 30, 2010) ("Staff Report") and discussing hackers penetrating certain Nasdaq OMX Group, Inc. computer networks in 2011, a "software bug" that hampered the initial public offerings of BATS Global Markets, Inc. in 2012, and issues with Nasdaq's trading systems delaying the start of trading in the high-profile initial public offering of Facebook, Inc.).

[15] *See* Securities Exchange Act Release No. 67802 (Sept. 7, 2012), 77 FR 56697 (Sept. 13, 2012) (File No. 4-652); Technology Roundtable Transcript, *available at* https://www.sec.gov/news/otherwebcasts/2012/ttr100212-transcript.pdf. A webcast of the Roundtable is *available at* www.sec.gov/news/otherwebcasts/2012/ttr100212.shtml. The Technology Roundtable examined the relationship between the operational stability and integrity of the securities market and the ways in which market participants design, implement, and manage complex and interconnected trading technologies. The Technology Roundtable also highlighted that quality standards, testing, and improved response mechanisms were issues ripe for consideration. *See* SCI Proposing Release, *supra* note 14, at 18090-91 (providing for further discussion of the Technology Roundtable).

[16] *See* SCI Proposing Release, *supra* note 14, at 18091. *See also* SCI Adopting Release, *supra* note 1, at 72254-72255 (summarizing additional disruptions during the period between publication of the SCI Proposing and Adopting Releases).

[17] *See supra* note 13.

Exchange Act requirements, as policy statements rather than Commission rules, compliance was voluntary and in many instances the SROs did not fully disclose problems that occurred. In the SCI Proposing Release, the Commission stated that "the continuing evolution of the securities markets to the current state, where they have become almost entirely electronic and highly dependent on sophisticated trading and other technology (including complex regulatory and surveillance systems, as well as systems relating to the provision of market data, intermarket routing and connectivity, and a variety of other member and issuer services), has posed challenges for the ARP Inspection Program."[18] Informed by its review of recent technology problems in the markets, the discussions at the Technology Roundtable, and its evaluation of the ARP Program,[19] the Commission proposed Regulation SCI in 2013 to help address the technological vulnerabilities, and improve Commission oversight, of the core technology of key U.S. securities markets entities, including national securities exchanges and associations, significant-volume ATSs, clearing agencies, and plan processors.[20] After

---

[18] SCI Proposing Release, *supra* note 14, at 18089.

[19] *See* SCI Proposing Release, *supra* note 14, at 18085-91 for a further discussion of these considerations.

[20] As further explained in the SCI Adopting Release, the term "plan processor" means "any self-regulatory organization or securities information processor acting as an exclusive processor in connection with the development, implementation and/or operation of any facility contemplated by an effective national market system plan." *See* SCI Adopting Release, *supra* note 1, at 72270 n. 196. This term refers to the securities information processors that are exclusive processors (and frequently referred to as the "SIPs") that collect and process (for distribution) quotation data and/or transaction reports on behalf of the Consolidated Tape Association System ("CTA Plan"), Consolidated Quotation System ("CQS Plan"), Joint Self-Regulatory Organization Plan Governing the Collection, Consolidation, and Dissemination of Quotation and Transaction Information for Nasdaq-Listed Securities Traded on Exchanges on an Unlisted Trading Privileges

considering the views of a wide variety of commenters, the Commission adopted Regulation SCI in 2014.[21] In the SCI Adopting Release, the Commission stated that it was taking a "measured approach" and pursuing an "incremental expansion from the entities covered under the ARP Inspection Program" given the potential costs of compliance with Regulation SCI.[22] It added, however, that this approach would allow it "to monitor and evaluate the implementation of Regulation SCI, the risks posed by the systems of other market participants, and the continued evolution of the securities markets, such that it may consider, in the future, extending the types of requirements in Regulation SCI to additional categories of market participants, such as non-ATS broker-dealers, security-based swap dealers, investment advisers, investment companies, transfer agents, and other key market participants."[23] In 2021, the Commission amended Regulation SCI to add certain "competing consolidators" to the definition of SCI entity.[24]

---

Basis ("Nasdaq UTP Plan"), and Options Price Reporting Authority ("OPRA Plan"). The CTA Plan and Nasdaq UTP Plan (applicable to national market system ("NMS") stocks) are each a "transaction reporting plan" as well as a "national market system plan" as defined in 17 CFR 242.600 ("Rule 600" of Regulation NMS). The OPRA Plan (applicable to exchange-listed options) is a national market system plan. *See infra* note 212. *See also* text accompanying note 212 (discussing these Plans and how transaction reports containing the price and volume associated with a transaction involving the purchase or sale of a security are currently, and anticipated in the future to be, readily available to enable SCI ATSs and SCI broker-dealers to ascertain the total average daily dollar volume traded in NMS stock and exchange-listed options in a calendar month and self-assess if they exceed the proposed transaction activity thresholds discussed below).

21 *See generally* SCI Adopting Release, *supra* note 1.

22 *Id.* at 72259.

23 *Id. See also supra* note 10 and accompanying text (referencing other cybersecurity rules proposed to apply to Commission registrants).

24 *See* Securities Exchange Act Release No. 90610 (Dec. 9, 2020), 86 FR 18596, 18659-18676 (Apr. 9, 2021) ("Market Data Infrastructure Adopting Release") (adopting rules with respect to competing consolidators and defining "competing consolidator" to mean a securities information processor required to be registered pursuant to 17 CFR 242.614 ("Rule 614") or a national securities exchange or national securities association that receives information with respect to quotations for and transactions in NMS stocks and generates a consolidated market data product for dissemination to any person).

Specifically, a competing consolidator that exceeds a five percent consolidated market data gross revenue threshold over a specified time period is an SCI competing consolidator because it is a significant source of consolidated market data for NMS stocks on which market participants rely.[25]

### B. Current Regulation SCI

#### 1. SCI Entities and SCI Systems

Regulation SCI applies to "SCI entities."[26] SCI entities are those that the Commission has determined are market participants that play a significant role in the U.S. securities markets and/or have the potential to impact investors, the overall market, or the trading of individual securities in the event of certain types of systems problems.[27] Today SCI entities comprise the self-regulatory organizations (excluding securities futures exchanges) ("SCI SROs"), ATSs meeting certain volume thresholds with respect to NMS stocks and non-NMS stocks ("SCI ATSs"), exclusive disseminators of consolidated market data ("plan processors"), certain competing disseminators of

---

25 An "SCI competing consolidator" is any competing consolidator, which during at least four of the preceding six calendar months, accounted for five percent or more of consolidated market data gross revenue paid to the effective national market system plan or plans required under 17 CFR 242.603(b) ("Rule 603(b)") for NMS stocks (1) listed on the New York Stock Exchange, (2) listed on The Nasdaq Stock Market, or (3) listed on national securities exchanges other than the New York Stock Exchange or The Nasdaq Stock Market, as reported by such plan or plans pursuant to the terms thereof. *See* Rule 1000. An SCI competing consolidator is subject to Regulation SCI, and a competing consolidator for which Regulation SCI does not apply is subject the systems capability requirement in 17 CFR 242.614(d)(9) ("Rule 614(d)(9)" of Regulation NMS). *See infra* note 28 and accompanying text.

26 *See* 17 CFR 242.1000 (defining the term "SCI entity" and terms included therein).

27 *See* SCI Adopting Release, *supra* note 1, at 72259. Although some commenters had urged that Regulation SCI apply to fewer entities and only the most systemically important entities, the Commission disagreed, stating, "[L]imiting the applicability of Regulation SCI to only the most systemically important entities posing the highest risk to the markets is too limited of a category of market participants, as it would exclude certain entities that, in the Commission's view, have the potential to pose significant risks to the securities markets should an SCI event occur." *Id.*

consolidated market ("SCI competing consolidators"[28]), and certain exempt clearing agencies.[29]

An SCI entity has obligations with respect to its "SCI systems," "critical SCI systems," and "indirect SCI systems."[30] "SCI systems" are, broadly, the technology systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support at least one of six market functions: (i) trading; (ii) clearance and settlement; (iii) order routing; (iv) market data; (v) market regulation; or (vi) market surveillance.[31] In addition, Regulation SCI defines "critical SCI systems," which are a

---

28 *See supra* notes 24-25 (stating the definitions of competing consolidator and SCI competing consolidator). SCI competing consolidators are subject to Regulation SCI after a one-year transition period. *See* Market Data Infrastructure Adopting Release, *supra* note 24, at 18604. Competing consolidators in the transition period and competing consolidators below the gross revenue threshold are subject to a tailored set of operational capability and resiliency obligations designed to help ensure that the provision of consolidated market data products is prompt, accurate, and reliable. *See* Market Data Infrastructure Adopting Release, *supra* note 24, at 18690-97 (providing for a full discussion of systems capability requirements for competing consolidators (that are not subject to Regulation SCI), but instead subject to Rule 614(d)(9)).

29 *See* 17 CFR 242.1000 (defining the term SCI entity to mean "an SCI self-regulatory organization, SCI alternative trading system, plan processor, exempt clearing agency subject to ARP, or SCI competing consolidator" and also separately defining each of these terms ). *See also* SCI Adopting Release, *supra* note 1, at 72258-72 (discussing the rationale for inclusion of SCI SROs, SCI ATSs, plan processors, and certain exempt clearing agencies in the original adopted definition of SCI entity); *infra* notes 83-84 and accompanying text (citing the releases explaining the expansion the definition of SCI entity to include SCI competing consolidators, and the recent proposal to further expand the definition of SCI entity to include certain ATSs that trade U.S. Treasury Securities or Agency Securities exceeding specified volume thresholds ("Government Securities ATSs")).

30 *See* 17 CFR 242.1000 (defining the terms "SCI systems," "critical SCI systems," and "indirect SCI systems").

31 *Id.* (defining SCI systems to mean "all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, routing, market data, market regulation, or market surveillance").

subset of SCI systems,[32] and designated as such because they represent potential single points of failure in the U.S. securities markets.[33]

The term "indirect SCI systems" describes systems of, or operated by or on behalf of, an SCI entity that, "if breached, would be reasonably likely to pose a security threat to SCI systems."[34] The distinction between SCI systems and indirect SCI systems seeks to encourage SCI entities physically and/or logically to separate systems that perform or directly support securities market functions from those that perform other functions (*e.g.*, corporate email; general office systems for member regulation and recordkeeping).[35]

Currently, the application of Regulation SCI is triggered when an entity meets the definition of SCI entity. If an entity meets the definition of SCI entity, Regulation SCI applies to its SCI systems and indirect SCI systems. The scope of an SCI entity's technology systems is determined by whether they are operated "by or on behalf of" the SCI entity and whether they directly support any of the six market functions enumerated in the definition. As a result, the SCI systems and indirect SCI systems of an SCI entity

---

32 *Id*. (defining critical SCI systems to mean any SCI systems of, or operated by or on behalf of, an SCI entity that: (1) Directly support functionality relating to: (i) Clearance and settlement systems of clearing agencies; (ii) Openings, reopenings, and closings on the primary listing market; (iii) Trading halts; (iv) Initial public offerings; (v) The provision of consolidated market data; or (vi) Exclusively listed securities; or (2) Provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets).

33 As discussed in the SCI Adopting Release, "critical SCI systems" are subject to certain heightened resilience and information dissemination provisions of Regulation SCI on the rationale that, lacking or having limited substitutes, these systems pose the greatest risks to the continuous and orderly function of the markets if they malfunction. *See* SCI Adopting Release, *supra* note 1, at 72277-79 (providing additional discussion of critical SCI systems).

34 *Id.* at 72279.

35 *See* SCI Adopting Release, *supra* note 1, at 72281 ("[I]f an SCI entity designs and implements security controls so that none of its non-SCI systems would be reasonably likely to pose a security threat to SCI systems, then it will have no indirect SCI systems. If, however, an SCI entity does have indirect SCI systems, then certain provisions of Regulation SCI will apply to those indirect SCI systems.").

are neither limited by the type of security nor by the type of business in which an SCI entity primarily conducts its securities market activities. Thus, if an SCI entity elects to, or obtains the necessary approvals to, engage in market functions in multiple types of securities, Regulation SCI's obligations apply to the relevant functional systems relating to all such securities.[36] Accordingly, the SCI systems of an SCI entity may include systems pertaining to any type of security, whether those securities are NMS stocks, over-the-counter (OTC) equity securities, listed options, debt securities, security-based swaps ("SBS"), crypto asset securities,[37] or another type of security.[38]

---

36 The current definition of "SCI systems," includes the clause, "with respect to securities," without limitation. SCI systems "means all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect *to securities*, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance." *See* 17 CFR 242.1000 (emphasis added). *But see infra* section III.A.2.b.iv (discussing the proposed limitation to the definition of SCI systems for certain SCI broker-dealers).

37 The term "digital asset" refers to an asset that is issued and/or transferred using distributed ledger or blockchain technology ("distributed ledger technology"), including, but not limited to, so-called "virtual currencies," "coins," and "tokens." *See Custody of Digital Asset Securities by Special Purpose Broker-Dealers*, Securities Exchange Act Release No. 90788 (Dec. 23, 2020), 86 FR 11627, 11627 n.1 (Feb. 26, 2021) ("Crypto Asset Securities Custody Release"). A digital asset may or may not meet the definition of a "security" under the Federal securities laws. *See*, *e.g.*, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Securities Exchange Act Release No. 81207 (July 25, 2017) ("DAO 21(a) Report"), *available at* https://www.sec.gov/litigation/investreport/34-81207.pdf. *See also SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). To the extent digital assets rely on cryptographic protocols, these types of assets also are commonly referred to as "crypto assets," and "digital asset securities" can be referred to as "crypto asset securities." For purposes of this release, the Commission does not distinguish between the terms "digital asset securities" and "crypto asset securities."

38 Today, under the current definition of SCI systems, an SCI entity (current or future) that engages in market functions for any type of securities, including crypto asset securities, is required to assess whether the technological systems of, or operated by or on its behalf, with respect to securities, directly support at least one of six market functions: (i) trading; (ii) clearance and settlement; (iii) order routing; (iv) market data; (v) market regulation; or (vi) market surveillance. As discussed below, however, the Commission is proposing an amendment to the definition of SCI systems that would limit its scope solely for certain proposed SCI broker-dealers. *See infra* section III.A.2.b.iv.

### 2. Reasonably Designed Policies and Procedures

The foundational principles of Regulation SCI are set forth in Rule 1001, which 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 their operational capability and promote the maintenance of fair and orderly markets.[39] Rule 1001(a)(2) of Regulation SCI requires that, at a minimum, such policies and procedures include: current and future capacity planning; periodic stress testing; systems development and testing methodology; reviews and testing to identify vulnerabilities; business continuity and disaster recovery planning (inclusive of backup systems that are geographically diverse and designed to meet specified recovery time objectives); standards for market data collection, processing, and dissemination; and monitoring to identify potential systems problems.[40] Under 17 CFR 242.1001(a)(3) ("Rule 1001(a)(3)" of Regulation SCI), SCI entities must periodically review the effectiveness of these policies and procedures and take prompt action to remedy any deficiencies.[41] Rule 1001(a)(4) of Regulation SCI provides that an SCI entity's policies and procedures will be deemed to be reasonably designed if they are consistent with "current SCI industry standards," which is defined 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.

---

[39] *See* 17 CFR 242.1001(a)(1).

[40] *See* 17 CFR 242.1001(a)(2).

[41] *See* 17 CFR 242.1001(a)(3).

governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization; however, Rule 1001(a)(4) of Regulation SCI also makes clear that compliance with such "current SCI industry standards" is not the exclusive means to comply with these requirements.[42]

Under 17 CFR 242.1001(b)(1) ("Rule 1001(b)(1)" of Regulation SCI), each SCI entity is required to establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Exchange Act and the rules and regulations thereunder and the entity's rules and governing documents, as applicable, and specifies certain minimum requirements for such policies and procedures.[43] In addition, 17 CFR 242.1001(b)(2) ("Rule 1001(b)(2)") requires that at a minimum, these policies and procedures must include: testing of all SCI systems and any changes to SCI systems prior to implementation; a system of internal controls over changes to SCI systems; a plan for assessments of the functionality of SCI systems designed to detect systems compliance issues, including by "responsible SCI personnel" (defined below) and by personnel familiar with applicable provisions of the Exchange Act and the rules and regulations thereunder and the SCI entity's rules and governing documents; and a plan of coordination and communication between regulatory and other personnel of the SCI entity, including by responsible SCI personnel, regarding SCI systems design, changes, testing, and controls designed to detect and prevent systems compliance issues.[44]

---

42 *See* 17 CFR 242.1001(a)(4).

43 *See* 17 CFR 242.1001(b)(1).

44 *See* 17 CFR 242.1001(b)(2).

Under 17 CFR 242.1001(b)(3) ("Rule 1001(b)(3)" of Regulation SCI), SCI entities must periodically review the effectiveness of these policies and procedures and take prompt action to remedy any deficiencies.[45] Under 17 CFR 242.1001(b)(4) ("Rule 1001(b)(4)" of Regulation SCI), individuals are provided with a safe harbor from liability under Rule 1001(b) if certain conditions are met.[46]

Further, 17 CFR 242.1001(c) ("Rule 1001(c)" of Regulation SCI), requires SCI entities to establish, maintain, and enforce reasonably designed written policies and procedures that include the criteria for identifying responsible SCI personnel, the designation and documentation of responsible SCI personnel, and escalation procedures to quickly inform responsible SCI personnel of potential SCI events.[47] Rule 1000 of Regulation SCI defines "responsible SCI personnel" to mean, for a particular SCI system or indirect SCI system impacted by an SCI event, such senior manager(s) of the SCI entity having responsibility for such system, and their designee(s).[48] Rule 1000 also defines "SCI event" to mean an event at an SCI entity that constitutes a systems disruption, a systems compliance issue, or a systems intrusion.[49] Under 17 CFR 242.1001(c)(2) ("Rule 1001(c)(2)" of Regulation SCI), SCI entities are required periodically to review the effectiveness of these policies and procedures and take prompt action to remedy any deficiencies.[50]

---

45 *See* 17 CFR 242.1001(b)(3).

46 *See* 17 CFR 242.1001(b)(4).

47 *See* 17 CFR 242.1001(c).

48 17 CFR 242.1000.

49 *Id.*

50 *See* 17 CFR 242.1001(c)(2).

### 3. SCI Events

Under Rule 1002 of Regulation SCI, SCI entities have certain obligations regarding SCI events. An "SCI event" is defined as: (i) a "systems disruption," which is an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system; and/or (ii) a "systems intrusion," which is any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity; and/or (iii) a "systems compliance issue," which is an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Exchange Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable.[51]

When any responsible SCI personnel has a reasonable basis to conclude that an SCI event has occurred, the SCI entity must begin to take appropriate corrective action which must include, at a minimum, mitigating potential harm to investors and market integrity resulting from the SCI event and devoting adequate resources to remedy the SCI event as soon as reasonably practicable.[52] With limited exceptions,[53] Rule 1002(b) provides the framework for notifying the Commission of SCI events including, among other things, requirements to: notify the Commission of the event immediately; provide a written notification on Form SCI within 24 hours that includes a description of the SCI event and the system(s) affected, with other information required to the extent available

---

51 *See* 17 CFR 242.1000.

52 *See* 17 CFR 242.1002(a).

53 *See* 17 CFR 242.1002(b)(5) (relating to the exception for de minimis SCI events).

at the time; provide regular updates regarding the SCI event until the event is resolved; and submit a final detailed written report regarding the SCI event.[54]

Rule 1002(c) of Regulation SCI also requires that SCI entities disseminate information to their members or participants regarding SCI events.[55] These information dissemination requirements are scaled based on the nature and severity of an event. SCI entities are required to disseminate certain information about the event to certain of its members or participants (*i.e.*, those that are reasonably estimated to have been affected) promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event has occurred. For "major SCI events," such dissemination must be made to all of its members or participants. In addition, dissemination of information to members or participants is permitted to be delayed for systems intrusions if such dissemination would likely compromise the security of the SCI entity's systems or an investigation of the intrusion.[56] In addition, 17 CFR 242.1002(c)(4) ("Rule 1002(c)(4)" of Regulation SCI) provides exceptions to the dissemination requirements under Rule 1002(c) of Regulation SCI for SCI events to the extent they relate to market regulation or market surveillance systems or SCI events that have had, or the SCI entity reasonably estimates would have, either a de minimis or no impact on the SCI entity's operations or on market participants.[57]

---

54 *See* 17 CFR 242.1002(b).

55 *See* 17 CFR 242.1002(c).

56 *See id.* The rule also requires that the SCI entity document its reasons for delayed notification. *Id.*

57 *See* 17 CFR 242.1002(c)(4).

### 4. Systems Changes and SCI Review

Under 17 CFR 242.1003(a) ("Rule 1003(a)" of Regulation SCI), SCI entities are required to provide reports to the Commission relating to system changes, including a report each quarter describing completed, ongoing, and planned material changes to their SCI systems and the security of indirect SCI systems, during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion.[58] Rule 1003(b) of Regulation SCI also requires that an SCI entity conduct an "SCI review" not less than once each calendar year.[59] "SCI review" is defined in Rule 1000 of Regulation SCI to mean a review, following established procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems, and which review contains: a risk assessment with respect to such systems of an SCI entity; and an assessment of internal control design and effectiveness of its SCI systems and indirect SCI systems to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards.[60] Under Rule 1003(b)(2) and (3), SCI entities are also required to submit a report of the SCI review to their senior management, and must also submit the report and any response by senior management to the report, to their board of directors, as well as to the Commission.[61]

---

58 *See* 17 CFR 242.1003(a).

59 *See* 17 CFR 242.1003(b).

60 *See* 17 CFR 242.1000. Rule 1003(b)(1) of Regulation SCI also states that penetration test reviews of an SCI entity's network, firewalls, and production systems must be conducted at a frequency of not less than once every three years, and assessments of SCI systems directly supporting market regulation or market surveillance must be conducted at a frequency based upon the risk assessment conducted as part of the SCI review, but in no case less than once every three years. *See* 17 CFR 242.1003(b)(1)(i) and (ii) ("Rule 1003(b)(1)(i) and (ii)").

61 *See* 17 CFR 242.1003(b)(2) and (3).

### 5. Business Continuity and Disaster Recovery Testing with Members/Participants

Rule 1004 of Regulation SCI sets forth certain requirements for testing an SCI entity's business continuity and disaster recovery plans with its members or participants. This rule requires that, with respect to an SCI entity's business continuity and disaster recovery plan, including its backup systems, each SCI entity shall: (a) establish standards for the designation of those members or participants that the SCI entity reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of such plans; (b) designate members or participants pursuant to the standards established and require participation by such designated members or participants in scheduled functional and performance testing of the operation of such plans, in the manner and frequency specified by the SCI entity, provided that such frequency shall not be less than once every 12 months; and (c) coordinate the testing of such plans on an industry- or sector-wide basis with other SCI entities.[62]

### 6. Recordkeeping and Other Provisions (Rules 1005-1007)

SCI entities are required by Rule 1005 of Regulation SCI to make, keep, and preserve certain records related to their compliance with Regulation SCI.[63] In addition, 17 CFR 242.1006 ("Rule 1006" of Regulation SCI), provides for certain requirements relating to the electronic filing, on Form SCI, of any notification, review, description,

---

62 *See* 17 CFR 242.1004.

63 *See* 17 CFR 242.1005. Unlike 17 CFR 242.1005(a) ("Rule 1005(a)") of Regulation SCI, which relates to recordkeeping provisions for SCI SROs, 17 CFR 242.1005(b) ("Rule 1005(b)") relates to the recordkeeping provision for SCI entities other than SCI SROs.

analysis, or report to the Commission required to be submitted under Regulation SCI.[64] Finally, 17 CFR 242.1007 ("Rule 1007" of Regulation SCI) requires a written undertaking when records required to be filed or kept by an SCI entity under Regulation SCI are prepared or maintained by a service bureau or other recordkeeping service on behalf of the SCI entity.[65]

### C. Overview of Proposed Amendments to Regulation SCI

The Commission is proposing amendments to Regulation SCI that would expand the definition of "SCI entity" to include a broader range of key market participants in the U.S. securities market infrastructure and update certain provisions of Regulation SCI to take account of developments in the technology landscape of the markets and the Commission and its staff's oversight experience since the adoption of Regulation SCI in 2014. As discussed in section III.A, the Commission is proposing to expand the definition of SCI entity to include registered SBSDRs, registered broker-dealers exceeding a size threshold ("SCI broker-dealers"), and additional clearing agencies exempt from registration.[66] As discussed in section III.C, the Commission is also proposing to update several requirements of Regulation SCI to acknowledge certain technology changes in the market, including cybersecurity and third-party provider management challenges since the adoption of Regulation SCI in 2014, and to account for the experience and insights the Commission and its staff have gained with respect to technology issues surrounding SCI entities and their systems. These include:

---

64 *See* 17 CFR 242.1006.

65 *See* 17 CFR 242.1007.

66 *See infra* section III.A.2.a. through c. (providing a detailed discussion of each of these categories of entities and associated proposed definitions).

- Amendments to Rule 1001(a) to require that an SCI entity's policies and procedures for SCI systems, critical SCI systems, and indirect SCI systems, address with specificity:
    - Systems classification and life cycle management;[67]
    - Management of third-party providers, including cloud service providers and providers of critical SCI systems;[68]
    - Access controls;[69] and
    - Identification of current SCI industry standards, if any;[70]
- Expansion of the definition of "systems intrusion" in Rule 1000 to include a wider range of cybersecurity events;[71]
- Amendments to Rule 1002 regarding notice of systems intrusions to the Commission and affected persons;[72]
- Amendments to the definition of "SCI review" and Rule 1003(b) to specify in greater detail the contents of the SCI review and associated report, and to require annual penetration testing;[73]

---

67 *See infra* section III.C.1.

68 *See infra* section III.C.2.

69 *See infra* section III.C.3.a.

70 *See infra* section III.C.5.c.

71 *See infra* section III.C.3.c.

72 *See infra* section III.C.3.c.

73 *See infra* sections III.C.3.b and III.C.4.

- Amendments to Rule 1004 to require that SCI entities designate key third-party providers for participation in annual business continuity/disaster recovery testing;[74]
- Amendments to Rule 1001(a)(4) to address how an SCI entity may avail itself of the safe harbor provision;[75]
- Amendments to Rule 1005 to address the maintenance of records by a former SCI entity; and
- Changes to Form SCI consistent with the proposed changes.[76]

The amendments to Regulation SCI are proposed independently of the proposals discussed in the Exchange Act Cybersecurity Proposal and Regulation S-P 2023 Proposing Release. However, the relationship of all three proposals, as each may apply to an SCI entity, is discussed in section III.D.

## III. Proposed Amendments to Regulation SCI

### A. Definition of SCI Entity

#### 1. Evolution: Current and Proposed SCI Entities

Currently, SCI entities are the SCI SROs, SCI ATSs, plan processors, certain exempt clearing agencies, and, as of 2020, SCI competing consolidators.[77] In 2013, the Commission proposed to include other entities: specifically, ATSs trading corporate debt or municipal securities (hereafter, "Fixed Income ATSs") exceeding specified volume

---

[74] *See infra* section III.C.2.d.

[75] *See infra* section III.C.5.

[76] *See infra* section III.C.6.

[77] *See supra* notes 27-29 and accompanying text; *infra* note 83 and accompanying text.

thresholds.[78] The Commission did not include any Fixed Income ATSs as SCI entities at adoption in 2014, however, based on consideration of comments regarding the risk profile of Fixed Income ATSs at that time.[79] In 2013, the Commission also solicited comment on the inclusion of several other types of entities, including SBSDRs and broker-dealers (beyond SCI ATSs).[80] At adoption in 2014, comments regarding these and other entities were summarized, with specific proposals deferred for possible future consideration.[81] In sum, the Commission stated in 2014 that it was neither limiting the applicability of Regulation SCI to only the most systemically important entities as urged by some commenters, nor taking a broad approach at the outset, but rather that it was taking a "measured" approach in establishing the initial scope of SCI entities.[82] Since the initial adoption of Regulation SCI, the Commission has considered expansion of the definition of SCI entity several times: first to propose and adopt certain competing consolidators as SCI entities,[83] and more recently to propose and repropose adding ATSs

---

78 *See* SCI Proposing Release, *supra* note 14, at 18097.

79 *See* SCI Adopting Release, *supra* note 1, at 72270, 72409 (discussing determination not to apply Regulation SCI to ATSs trading only corporate debt and municipal securities at that time).

80 *See* SCI Proposing Release, *supra* note 14, at 18133-41. The Commission also solicited comment on the inclusion of security-based swap execution facilities ("SB SEFs"), which entities are now the subject of another proposal. *See Rules Relating to Security-Based Swap Execution and Registration and Regulation of Security-Based Swap Execution Facilities*, Release No. 94615 (Apr. 6, 2022), 87 FR 28872 (May 11, 2022) (proposing that SB SEFs be subject to 17 CFR 242.800 through 242.835 ("Regulation SE") which includes operational capability requirements closely modeled on a detailed CFTC rule for SEFs (17 CFR 37.1401)). SB SEFs are not further discussed herein.

81 *See* SCI Adopting Release, *supra* note 1, at 72364-66 (contemplating possible future proposals).

82 *See* SCI Adopting Release, *supra* note 1, at 72259 (stating that this measured approach would enable the Commission to "monitor and evaluate the implementation of Regulation SCI, the risks posed by the systems of other market participants, and the continued evolution of the securities markets, such that it may consider, in the future, extending the types of requirements in Regulation SCI to additional categories of [key] market participants . . . .").

83 *See* Market Data Infrastructure Adopting Release, *supra* note 24, at 18659-18676.

that trade U.S. Treasury Securities or Agency Securities exceeding specified volume thresholds ("Government Securities ATSs") as SCI entities.[84]

The Commission now proposes a further expansion of the definition of SCI entity to include SBSDRs, certain registered broker-dealers (*i.e.,* SCI broker-dealers), and additional clearing agencies exempted from registration. The Commission also solicits comment on whether, in light of technological changes in the fixed income markets in recent years, Fixed Income ATSs should again be proposed to be subject to Regulation SCI, rather than 17 CFR 240.301(b)(6) ("Rule 301(b)(6)" of Regulation ATS), and also whether and how broker-dealers trading corporate debt and municipal securities should be considered.[85]

---

[84] *See* Securities Exchange Act Release Nos. 90019 (Sept. 28, 2020), 85 FR 87106 (Dec. 31, 2020) ("Government Securities ATS Proposing Release"); 94062 (Jan. 26, 2022), 87 FR 15496 (Mar. 18, 2022) ("Government Securities ATS Reproposal") (among other things, citing operational similarities between Government Securities ATSs and NMS stock ATSs). In the Government Securities ATS Reproposal, the Commission proposed amendments to 17 CFR 240.3b-16(a) ("Rule 3b-16(a)" of the Exchange Act), which defines certain terms used in the statutory definition of "exchange" under section 3(a)(1) of the Exchange Act, to include systems that offer the use of non-firm trading interest and provide communication protocols to bring together buyers and sellers of securities. Trading systems that may fall within the criteria of proposed 17 CFR 240.3b-16 ("Rule 3b-16"), as proposed to be amended, would likely operate as ATSs, and possibly SCI ATSs. Because the proposed amendments to Rule 3b-16(a) could result in a greater number of ATSs, and the amendments proposed to expand and update SCI could impact newly designated ATSs, commenters are encouraged to review both the Government Securities ATS Reproposal and this proposal to determine whether it might affect their comments on this proposal, as well as their responses to the Commission's request for comment on application of Regulation SCI to Fixed Income ATS contained herein.

[85] Currently, Rule 301(b)(6) of Regulation ATS applies to Fixed Income ATSs exceeding a volume threshold. Under Rule 301(b)(6), an ATS that trades only municipal securities or corporate debt at a threshold of 20% or more of the average daily volume traded in the United States, during at least four of the preceding six calendar months, is required to comply with capacity, integrity, and security requirements with respect to those systems that support order entry, order routing, order execution, transaction reporting, and trade comparison. *See* 17 CFR 242.301(b)(6). As discussed further below, the amendments proposed in this release do not include amendments to modify the numerical volume thresholds or to otherwise modify Rule 301(b)(6) of Regulation ATS, or move systems requirements for Fixed Income ATSs from Regulation ATS to Regulation SCI. The Commission does, however, request comment on the state of electronic trading and automation in the corporate debt and municipal securities markets, as well as the risks associated with entities with significant activity in these markets. *See infra* section III.B.

### 2. New Proposed SCI Entities

When it adopted Regulation SCI, the Commission acknowledged that there may be other categories of entities not included in the definition of SCI entity that, given their increasing size and importance, could pose risks to the market should an SCI event occur, but decided to include only certain key market participants at that time.[86] The Commission proposes to expand the definition of SCI entity to include SBSDRs, certain types of broker-dealers, and additional clearing agencies exempted from registration as additional key market participants that would also have to comply with Regulation SCI because they play a significant role in the U.S. securities markets and/or have the potential to impact investors, the overall market, or the trading of individual securities in the event of a systems issue. If this amendment is adopted, these new SCI entities would become subject to all provisions of Regulation SCI, including the provisions proposed to be amended as discussed in section III.C of this release.

#### a. Registered Security-Based Swap Data Repositories (SBSDRs)

The Commission proposes to expand the application of Regulation SCI to SBSDRs. As registered securities information processors that disseminate market data and provide price transparency in the SBS market, and centralized trade repositories for SBS data for use by regulators, SBSDRs play a key role in the SBS market.[87]

---

86 *See* SCI Adopting Release, *supra* note 1, at 72259. *See also supra* note 82 and accompanying text.

87 Rule 1000 would define the term registered security-based swap data repository to mean "a security-based swap data repository, as defined in 15 U.S.C. 78c(a)(75), and that is registered with the Commission pursuant to 15 U.S.C. 78m(n) and §240.13n-1," with a proviso that compliance with Regulation SCI would not be required until six months after the entity's registration is effective. *See* proposed Rule 1000.

As noted, the Commission solicited comment on the inclusion of SBSDRs as SCI entities when it first proposed Regulation SCI in 2013.[88] At that time, the Commission anticipated that SBSDRs would "play an important role in limiting systemic risk and promoting the stability of the SBS market [and] also would serve as information disseminators in a manner similar to plan processors in the equities and options markets."[89] But it also acknowledged that there may be differences between the equities and options markets and the SBS market, "including differing levels of automation and stages of regulatory development."[90]

Comments received on the inclusion of SBSDRs as SCI entities in the SCI Proposing Release were limited. One commenter stated that "the similarities between certain SCI entities and SB SDRs . . . do not provide a clear justification for a different set of rules."[91] Another commenter stated that SBSDRs should have standards that are consistent with, but not identical to, those of SCI entities because the functions that SBSDRs perform are significantly different from those performed by SCI entities.[92] Other commenters, however, felt the practical differences between options and equities and derivatives called for some form of harmonization of rules, but not direct application of Regulation SCI to these entities.[93] The Commission deferred and stated in the SCI Adopting Release that, "should [it] decide to propose to apply the requirements of

---

88 *See supra* text accompanying note 80.

89 SCI Proposing Release, *supra* note 14, at 18135 (citation omitted).

90 *Id.*

91 SCI Adopting Release, *supra* note 1, at 72364.

92 *See id.*

93 *See id.*

Regulation SCI to SB SDRs [it] would issue a separate release discussing such a proposal."[94] Taking into account the role of SBSDRs in the SBS market, their reliance on technology to perform their functions, and the current state of regulatory development in the SBS market, the Commission is doing so now.

**i. Role of SBSDRs and Associated Risks**

Title VII of the Dodd-Frank Act, enacted in 2010, provided for a comprehensive, new regulatory framework for swaps and security-based swaps, including regulatory reporting and public dissemination of transactions in security-based swaps.[95] In 2015, the Commission established a regulatory framework for SBSDRs to provide improved transparency to regulators and help facilitate price discovery and efficiency in the SBS market.[96] Under this framework, SBSDRs are registered securities information processors and disseminators of market data in the SBS market,[97] thereby serving Title VII's goal of having public dissemination of price information for all security-based swaps, to enhance price discovery for market participants.[98] Like FINRA's Trade Reporting and Compliance Engine ("TRACE") and the MSRB's Electronic Municipal Market Access

---

94 SCI Adopting Release, *supra* note 1, at 72364; SCI Proposing Release, *supra* note 14, at 18134.

95 Pub. L. 111-203, section 761(a) (adding Exchange Act section 3(a)(75) (defining SBSDR)) and section 763(i) (adding Exchange Act section 13(n) (establishing a regulatory regime for SBSDRs)).

96 *See Security-Based Swap Data Repository Registration, Duties, and Core Principles*, Securities Exchange Act Release No. 74246 (Feb. 11, 2015), 80 FR 14438, 14441 (Mar. 19, 2015) ("SBSDR Adopting Release"); *Regulation SBSR—Reporting and Dissemination of Security-Based Swap Information*, Securities Exchange Act Release No. 74244 (Feb. 11, 2015), 80 FR 14563 (Mar. 19, 2015) ("SBSR Adopting Release").

97 *See* 17 CFR 242.909 ("A registered security-based swap data repository shall also register with the Commission as a securities information processor on Form SDR."); *see also* Form SDR ("With respect to an applicant for registration as a security-based swap data repository, Form SDR also constitutes an application for registration as a securities information processor.").

98 *See, e.g.*, SBSR Adopting Release, *supra* note 96, at 14604-05.

("EMMA"),[99] SBSDRs serve an important function for market participants because they disseminate market data, thereby providing price transparency in the SBS market.[100] Just as TRACE and EMMA provide price transparency to market participants and regulatory information to regulators, SBSDRs are designed to meet two purposes as mandated by Title VII of the Dodd-Frank Act: (1) to provide SBS data and information to regulators to surveil the markets and assess for market risks; and (2) to enhance price discovery to market participants.[101] As discussed in detail below, given that SBSDRs rely on automated systems and are designed to limit systemic risk and promote the stability of the markets they serve, the Commission believes that including SBSDRs in the definition of SCI entities would better ensure that SBSDR systems are robust, resilient, and secure. Additionally, this approach is reasonable and consistent as other entities that play a key price transparency role in their respective markets, such as plan processors, SCI

---

99 FINRA members are subject to transaction reporting obligations under FINRA Rule 6730, while municipal securities dealers are subject to transaction reporting obligations under MSRB Rule G–14. *See* FINRA Rule 6730(a)(1) (requiring FINRA members to report transactions in TRACE-Eligible Securities, which FINRA Rule 6710 defines to include a range of fixed-income securities). *See also* MRSB Rule G-14 (requiring transaction reporting by municipal bond dealers). EMMA, established by the MSRB in 2009, serves as the official repository of municipal securities disclosure providing the public with free access to relevant municipal securities data, and is the central database for information about municipal securities offerings, issuers, and obligors. Additionally, the MSRB's Real-Time Transaction Reporting System ("RTRS"), with limited exceptions, requires municipal bond dealers to submit transaction data to the MSRB within 15 minutes of trade execution, and such near real-time post-trade transaction data can be accessed through the MSRB's EMMA website.

100 *See* Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, *Principles for financial market infrastructures*, at 1.14, Box 1 (Apr. 16, 2012) ("PFMI"), *available at* https://www.bis.org/publ/cpss101a.pdf (stating that "[a] TR [trade repository] may serve a number of stakeholders that depend on having effective access to TR services, both to submit and retrieve data. In addition to relevant authorities and the public, other stakeholders can include exchanges, electronic trading venues, confirmation or matching platforms, and third-party service providers that use TR data to offer complementary services.").

101 *See, e.g.*, SBSR Adopting Release, *supra* note 96, at 14604-05.

competing consolidators, FINRA and the MSRB, are SCI entities, and their systems that directly support market data, among other functions, are currently SCI systems.[102]

As centralized repositories for SBS data for use by regulators, SBSDRs provide important infrastructure that assists relevant authorities in performing their market oversight.[103] Data maintained by SBSDRs may assist regulators in preventing market abuses, performing supervision, and resolving issues and positions if an institution fails.[104] SBSDRs are required to collect and maintain accurate SBS transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby putting the regulators in a better position to monitor for potential market abuse and risks to financial stability.[105] SBSDRs also have the potential to reduce operational risk and enhance operational efficiency, such as by maintaining transaction records that would help counterparties to ensure that their records reconcile on all of the key economic details.[106]

---

102 *See* SBSDR Adopting Release, *supra* note 96.

103 *See generally* PFMI, *supra* note 100, at 1.14 (stating that "[b]y centralising the collection, storage, and dissemination of data, a well-designed TR that operates with effective risk controls can serve an important role in enhancing the transparency of transaction information to relevant authorities and the public, promoting financial stability, and supporting the detection and prevention of market abuse.").

104 *See* Security-Based Swap Data Repository Registration, Duties, and Core Principles, Exchange Act Release No. 63347 (Nov. 19, 2010), 75 FR 77306, 77307 (Dec. 10, 2010), corrected at 75 FR 79320 (Dec. 20, 2010) and 76 FR 2287 (Jan. 13, 2011) ("SBSDR Proposing Release").

105 *See* SBSDR Adopting Release, *supra* note 96, at 14440 (stating that "SDRs are required to collect and maintain accurate SBS transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby putting them in a better position to monitor for potential market abuse and risks to financial stability.").

106 *See* SBSDR Proposing Release, *supra* note 104, at 77307 (stating that "[t]he enhanced transparency provided by an SDR is important to help regulators and others monitor the build-up and concentration of risk exposures in the SBS market . . . . In addition, SDRs have the potential to reduce operational risk and enhance operational efficiency in the SBS market.").

Furthermore, SBSDRs themselves are subject to certain operational risks that may impede the ability of SBSDRs to meet the goals set out in Title VII of the Dodd-Frank Act and the Commission's rules.[107] For instance, the links established between an SBSDR and other entities, including unaffiliated clearing agencies and other SBSDRs, may expose the SBSDR to vulnerabilities outside of its direct control.[108] Without appropriate safeguards in place for the systems of SBSDRs, their vulnerabilities could lead to significant failures, disruptions, delays, and intrusions, which could disrupt price transparency and oversight of the SBS market. For instance, an SBSDR processes and disseminates trade data using electronic systems, and if these systems fail, public access to timely and reliable trade data for the derivatives markets could potentially be compromised.[109] Also, if the data stored at an SBSDR is corrupted, the SBSDR would not be able to provide accurate data to relevant regulatory authorities, which could hinder the oversight of the derivatives markets. Moreover, because SBSDRs receive and maintain proprietary and sensitive information (*e.g.*, trading data, non-public personal

---

107 *See* SBSDR Adopting Release, *supra* note 96 at 14450 ("SDRs themselves are subject to certain operational risks that may impede the ability of SDRs to meet these goals, and the Title VII regulatory framework is intended to address these risks.").

108 *See* PFMI, *supra* note 100, at 3.20.20 (stating that "A TR should carefully assess the additional operational risks related to its links to ensure the scalability and reliability of IT [information technology] and related resources. A TR can establish links with another TR or with another type of FMI. Such links may expose the linked FMIs to additional risks if not properly designed. Besides legal risks, a link to either another TR or to another type of FMI may involve the potential spillover of operational risk. The mitigation of operational risk is particularly important because the information maintained by a TR can support bilateral netting and be used to provide services directly to market participants, service providers (for example, portfolio compression service providers), and other linked FMIs.").

109 *See* PFMI, *supra* note 100, at 1.14, Box 1 (stating that "[t]he primary public policy benefits of a TR, which stem from the centralisation and quality of the data that a TR maintains, are improved market transparency and the provision of this data to relevant authorities and the public in line with their respective information needs. Timely and reliable access to data stored in a TR has the potential to improve significantly the ability of relevant authorities and the public to identify and evaluate the potential risks posed to the broader financial system.").

information), it is essential that their systems be capable of ensuring the security and integrity of this data.

Along with the reliance of SBSDRs on automated systems to perform their functions, regulatory development of the SBS market has proceeded significantly since 2015. In particular, security-based swap dealers have registered with the Commission,[110] SBSDRs have registered with the Commission,[111] security-based swap execution facilities ("SBSEF") registration has been proposed,[112] and straight-through processing has increased in the market.[113] On November 8, 2021, SBS data began being reported to SBSDRs, which in turn began disseminating such data to the Commission and the public.[114] In light of the important role of SBSDRs in the markets for security-based swaps, their level of automation, and the regulatory development of the SBS market in recent years, the Commission believes it is timely to propose enhanced requirements for

---

110 *See List of Security-Based Swap Dealers and Major Security-Based Swap Participants*, Commission (last updated Jan. 4, 2023), *available at*: https://www.sec.gov/files/list_of_sbsds_msbsps_1_4_2023locked_final.xlsx.

111 The Commission approved the registration of two SBSDRs in 2021. *See* Security-Based Swap Data Repositories, DTCC Data Repository (U.S.), LLC, Order Approving Application for Registration as a Security-Based Swap Data Repository, Securities Exchange Act Release No. 91798 (May 7, 2021), 86 FR 26115 (May 12, 2021); Security-Based Swap Data Repositories, ICE Trade Vault, LLC, Order Approving Application for Registration as a Security-Based Swap Data Repository, Securities Exchange Act Release No. 92189 (Jun. 16, 2021), 86 FR 32703 (Jun. 22, 2021).

112 *See* Rules Relating to Security-Based Swap Execution and Registration and Regulation of Security-Based Swap Execution Facilities, Securities Exchange Act Release No. 94615 (Apr. 6, 2022), 87 FR 28872 (May 11, 2022).

113 *See, e.g.*, Security-Based Swap Data Repositories, DTCC Data Repository (U.S.), LLC, Notice of Filing of Application for Registration as a Security-Based Swap Data Repository, Securities Exchange Act Release No. 91071 (Feb. 5, 2021), 86 FR 8977 (Feb. 10, 2021) ("[T]he SDR process is an end-to-end straight through process; from the receipt of data, processing and maintenance of data, and dissemination of data, processes are automated and do not require manual intervention.").

114 *See* SEC Approves Registration of First Security-Based Swap Data Repository; Sets the First Compliance Date for Regulation SBSR, Press Release, Commission (May 7, 2021), available at: https://www.sec.gov/news/press-release/2021-80.

registered SBSDRs with respect to their technology systems that are central to the performance of their regulated activities.

### ii. Current Regulation

The Commission believes the current technology regulation framework for SBSDRs should be strengthened. SBSDR technology regulation is currently governed by 17 CFR 240.13n-6 ("Rule 13n-6"), a broad, principles-based operational risk rule,[115] which the Commission adopted in 2015 when regulatory development of the SBS market was still nascent and SBSDRs were not yet registered with the Commission under 17 CFR 240.13n-1 ("Rule 13n-1").[116] Additionally, Rule 13n-6 was adopted shortly after the adoption of Regulation SCI, with modifications that did not include some of the more detailed proposed requirements.[117] As a result, the two currently-registered SBSDRs

---

115 *See* 17 CFR 240.13n-6.

116 *See* SBSDR Adopting Release, *supra* note 96, at 14499, 14550 ("[T]he Commission may consider the application of any features of Regulation SCI to SDRs in the future."); SCI Adopting Release, *supra* note 1, at 72364.

117 *See* SBSDR Adopting Release, *supra* note 96, at 14499 (stating that "[t]he Commission is not adopting Rule 13n-6 as proposed because, after proposing Rule 13n-6, the Commission considered the need for an updated regulatory framework for certain systems of the U.S. securities trading markets and adopted Regulation Systems Compliance and Integrity ('Regulation SCI')."). Specifically, the Commission stated that the rule as adopted better sets an appropriate core framework for the policies and procedures of SBSDRs with respect to automated systems and that the framework adopted is "broadly consistent" with Regulation SCI. *See id.* Therefore, the Commission declined to adopt more prescriptive elements of the rule as proposed, including proposed Rule 13n-6(b), which would have required that every security-based swap data repository, with respect to those systems that support or are integrally related to the performance of its activities: (1) establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its systems provide adequate levels of capacity, resiliency, and security. These policies and procedures shall, at a minimum: (i) establish reasonable current and future capacity estimates; (ii) conduct periodic capacity stress tests of critical systems to determine such systems' ability to process transactions in an accurate, timely, and efficient manner; (iii) develop and implement reasonable procedures to review and keep current its system development and testing methodology; (iv) review the vulnerability of its systems and data center computer

(which are affiliated with registered clearing agencies that are subject to Regulation SCI)[118] remain subject to the broad principles-based rule, Rule 13n-6, which is the only applicable operational risk requirement for SBSDRs in the Commission's current regulatory framework.

Rule 13n-6 requires that SBSDRs, with respect to those systems that support or are integrally related to the performance of their activities, establish, maintain, and enforce written policies and procedures reasonably designed to ensure that their systems provide adequate levels of capacity, integrity, resiliency, availability, and security.[119] The operational risk principles underlying Rule 13n-6 are an essential part of the rules that comprise the core framework for SBSDRs that the Commission established in 2015 at the opening of its regulatory regime governing SBSDRs. The core framework influences all applicable requirements relevant to SBSDRs that follow. The core framework not only

---

operations to internal and external threats, physical hazards, and natural disasters; and (v) establish adequate contingency and disaster recovery plans; (2) on an annual basis, submit an objective review to the Commission within thirty calendar days of its completion. Where the objective review is performed by an internal department, an objective, external firm shall assess the internal department's objectivity, competency, and work performance with respect to the review performed by the internal department. The external firm must issue a report of the objective review, which the security-based swap data repository must submit to the Commission on an annual basis, within 30 calendar days of completion of the review; (3) promptly notify the Commission of material systems outages and any remedial measures that have been implemented or are contemplated (prompt notification includes the following: (i) immediately notify the Commission when a material systems outage is detected; (ii) immediately notify the Commission when remedial measures are selected to address the material systems outage; (iii) immediately notify the Commission when the material systems outage is addressed; and (iv) submit to the Commission within five business days of the occurrence of the material systems outage a detailed written description and analysis of the outage and any remedial measures that have been implemented or are contemplated); and (4) notify the Commission in writing at least thirty calendar days before implementation of any planned material systems changes. *See* SBSDR Proposing Release, *supra* note 104, at 77370.

118 The two registered SBSDRs, DTCC Data Repository (U.S.), LLC and ICE Trade Vault, LLC, are affiliated with the registered clearing agencies, Depository Trust Company and ICE Clear Credit LCC, respectively.

119 *See* 17 CFR 240.13n-6.

addresses SBSDR operational risk, but also other SBSDR enumerated duties, including registration, market access to services and data, governance arrangements, conflicts of interest, data collection and maintenance, privacy and disclosure requirements, and chief compliance officers,[120] thereby implementing the provisions of Exchange Act section 13(n).[121] Therefore, the SBSDR core framework, which Rule 13n-6 is a part, is different in focus and broader in scope than proposed Regulation SCI—as it relates to SBSDRs—which is focused on, among things, protecting the security of SBSDR systems. While Rule 13n-6 may not provide the absolute requirements relating to SBSDR operational risk, as the Commission's regulatory regime continues to evolve, Rule 13n-6 sets forth an enumerated duty for operational risk concerns that registered SBSDRs must address—at the time of registration and throughout its registration with the Commission. Compliance with the core principles and requirements in the SBSDR rules, including Rule 13n-6, is, thus, an important building block for better ensuring the integrity of an SBSDR's data quality upon which the Commission and the securities markets rely. In this regard, the Commission believes that Rule 13n-6 should be preserved, with the requirements of this proposal, if adopted, working to complement Rule 13n-6.[122] Specifically, the proposed

---

120 *See* 17 CFR 240.13n-1 through 240.13n-12; *See* SBSDR Adopting Release, *supra* note 96, at 14440-42.

121 15 U.S.C. 78m(n).

122 When adopting Rule 13n-6, the Commission acknowledged the potential application of Regulation SCI provisions to SBSDRs in the future. *See* SBSDR Adopting Release, *supra* note 96, at 14438, 14499 (stating that "[c]onsistent with this approach and in recognition of the importance of SDRs as the primary repositories of SBS trade information, the Commission may consider the application of any features of Regulation SCI to SDRs in the future."). Additionally, as guidance, the Commission stated that, in preparing their policies and procedures to comply with Rule 13n-6,

requirements of Regulation SCI on SBSDRs would exist and operate in conjunction with Rule 13n-6 and would prescribe certain key features and more detailed functional requirements to help ensure that SBSDR market systems are robust, resilient, and secure.[123]

Regulation SCI, among other things, defines the scope of systems covered, and requires: the establishment, maintenance, and enforcement of written policies and procedures to ensure that SCI systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain operational capacity and promote the maintenance of fair and orderly markets, with minimum elements that include, among others, standards designed to facilitate the successful collection, processing, and dissemination of market data and robust business continuity and disaster recovery plans; policies and procedures designed to ensure compliance with the federal securities laws;

---

SBSDRs may consider whether to incorporate aspects of Regulation SCI that may be appropriate for their particular implementation of Rule 13n-6. *See id.*, at 14499, n.826 (stating that "[i]n preparing their policies and procedures, SDRs may consider whether to incorporate aspects of Regulation SCI that may be appropriate for their particular implementation of Rule 13n-6, including where an SDR is related by virtue of its corporate structure to an entity subject to Regulation SCI.").

[123] In 2014, the SEC's SBSDR regulatory framework was subject to a Level 2 assessment by the Bank for International Settlements' Committee on Payments and Market Infrastructures ("CPMI") and the International Organization of Securities Commissions ("IOSCO"), which concluded that "the U.S. jurisdiction has developed rules or proposed rules that completely and consistently implement the majority of Principles that are applicable to CCPs [central counterparties] [but that] [t]he progress of the U.S. jurisdiction towards completely and consistently implementing the Principles for [trade repositories] has been more limited." *See* CPMI-IOSCO, *Implementation Monitoring of PFMIs: Level 2 assessment report for central counterparties and trade repositories -- United States* (Feb. 26, 2015), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD477.pdf. Additionally, CPMI-IOSCO issued guidance for cyber resilience for financial market infrastructures ("FMIs"), including trade repositories. *See* CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures* (June 2016), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf; *see also* CPMI-IOSCO*, Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience* (Nov. 2022), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD723.pdf (presenting the results of an assessment of the state of cyber resilience (as of Feb. 2021) at 37 FMIs from 29 jurisdictions that participated in this exercise in 2020 to 2022).

corrective action and reporting and dissemination of SCI events, quarterly reporting of material systems changes, and an annual SCI review; and participation of key members in SCI entity's business continuity and disaster recovery plans.

The Commission believes that SBSDRs operate with similar complexity and in a similar fashion as other registered securities information processors that are currently subject to Regulation SCI and that they play an important role in the SBS market and face similar technological vulnerabilities as existing SCI entities, such as FINRA's TRACE and MSRB's EMMA. For example, were an SBSDR to experience a systems issue, market participants could be prevented from receiving timely information regarding accurate prices for individual SBSs. Given SBSDRs' reliance on automated systems and their dual Dodd-Frank mandated role of providing price transparency to market participants and SBS data to regulators to surveil markets to better ensure that systemic risk is limited and market stability is enhanced, the Commission believes it appropriate to include SBSDRs into the scope of the Regulation SCI proposal.

Currently, there are two registered SBSDRs that would become subject to Regulation SCI should the Regulation SCI amendments be adopted.[124]

**iii. Request for Comment**

1. The Commission requests comment generally on the inclusion of SBSDRs as SCI entities. Is their inclusion appropriate? Why or why not? Please be specific and provide examples, if possible, to illustrate your points.
2. Should all or some aspects of Regulation SCI apply to SBSDRs? Why or why not? If only a portion, please specify which portion(s) and explain why. If all, explain why.

---

[124] *See supra* note 118.

3. Are the definitions of SCI systems and indirect SCI systems appropriate for SBSDRs? Why or why not? Are there any systems of SBSDRs that should be included but would not be covered by these definitions? Please explain. Are there any systems of SBSDRs that should be excluded by these definitions? Please explain. Do SBSDRs have any systems that would or should be covered by the definition of critical SCI systems? Please explain.
4. Is current Rule 13n-6 sufficient to govern the technology of SBSDRs? If not, why not? Would the Regulation SCI proposed requirements, together with Rule 13n-6, be sufficient to address operational risk concerns posed by SBSDRs? Why or why not? Should Rule 13n-6 serve as an operational risk requirement for new SBSDR registrants during the first year registered with the Commission, with Regulation SCI proposed requirements imposed after the first year of registration? Why or why not? Please be specific and respond with examples, if possible.
5. Given the current practices of SBSDRs, would the proposed Regulation SCI requirements pose unreasonable or unworkable difficulties for them, technologically, legally, operationally, or procedurally? Why or why not? Please be specific and respond with examples, if possible.
6. Should Regulation SCI distinguish among different types of SBSDRs such that some requirements of Regulation SCI might be appropriate for some SBSDRs but not others? Why or why not? If so, what are those distinctions and what are those requirements? For example, should any requirements be based on criteria such as number of transactions or notional volume reported to a SBSDR? If so, what would

be an appropriate threshold for any such criteria, and why? Please be specific and provide examples, if possible.

7. Because proposed Regulation SCI would include SBSDRs as "SCI entities," SBSDRs that share systems with affiliated clearing agencies could be required to classify those shared systems as SCI systems of the SBSDR and indirect SCI systems of the clearing agency, and vice versa. Is this outcome appropriate? Why or why not? Please be specific and provide examples, if possible.
8. Is Regulation SCI, including as proposed to be amended, comprehensive and robust enough to address SBSDRs that rely on third-party providers to support core SBSDR operations? Why or why not? Please be specific and provide examples, if possible.

**b. SCI Broker-Dealers**

The Commission further proposes to expand the application of Regulation SCI by including certain broker-dealers—to be referred to as "SCI broker-dealers"—in the definition of SCI entity. An SCI broker-dealer would be a broker or dealer registered with the Commission pursuant to section 15(b) of the Exchange Act that exceeds one or more size thresholds. An SCI broker-dealer would be a broker-dealer that meets or exceeds: (i) a total assets threshold, or (ii) one or more transaction activity thresholds.

The proposed thresholds are designed to identify the largest U.S. broker-dealers by size, as measured in two different ways. The first is analysis of broker-dealer size based on total assets reported on Form X-17A-5 (Financial and Operational Combined Uniform Single ("FOCUS") Report Part II, Item 940),[125] which reveals the largest firms

---

[125] *See* Form X-17A-5, FOCUS Report, Part II, at 3, *available at* https://www.sec.gov/files/formx-17a-5_2_2.pdf (requiring broker-dealers to report their total assets in Item 940).

based on their balance sheets at a point in time, and which is a measure used by the Board of Governors of the Federal Reserve System ("Federal Reserve Board") to calculate and provide to the public on a quarterly basis a measure of total assets of all security broker-dealers.[126] The second is a measure of broker-dealer size using transaction activity to identify significant firms active in certain enumerated types of securities. As discussed further below, the total assets threshold is expressed in terms of the broker-dealer's total assets at specified points in time as a percentage of the "total assets of all security broker-dealers" with "total assets of all security-broker-dealers" being calculated and made publicly available by the Federal Reserve Board for the associated preceding calendar quarter, or any subsequent provider of such information.[127] The trading activity threshold is expressed in terms of the sum of buy and sell transactions that the broker-dealer transacted during a specified time period as a percentage of reported total average daily dollar volume in one or more enumerated types of securities. The proposed total assets threshold is broadly similar to the approach banking regulators use to assess the appropriate capital and liquidity requirements for banks.[128] The proposed transaction

---

126 *See infra* note 127.

127 For additional detail on the calculation of total assets of all security broker-dealers, *see* Z.1: Financial Accounts of the United States, *available at* https://www.federalreserve.gov/apps/fof/Guide/z1_tables_description.pdf; ((i) stating that the term "security broker-dealers" refers to firms that buy and sell securities for a fee, hold an inventory of securities for resale, or do both; and firms that make up this sector are those that submit information to the Commission on one of two reporting forms, either the Financial and Operational Combined Uniform Single Report of Brokers and Dealers (FOCUS) or the Report on Finances and Operations of Government Securities Brokers and Dealers (FOGS); and (ii) describing the major assets of the security brokers and dealers sector). Currently, this information is readily accessible on the Federal Reserve Economic Data ("FRED") website. *See* Board of Governors of the Federal Reserve System (US), Security Brokers and Dealers; Total Assets (Balance Sheet), Level [BOGZ1FL664090663Q], retrieved from FRED, Federal Reserve Bank of St. Louis, available at: https://fred.stlouisfed.org/series/BOGZ1FL664090663Q (making publicly available the total assets of all security brokers and dealers, as calculated and updated quarterly by the Federal Reserve Board).

128 *See infra* notes 178-180 and accompanying text.

activity thresholds are similar to, but distinguishable from, the market share thresholds for SCI ATSs.[129] The proposed threshold approaches in the proposed definition of SCI broker-dealer are designed to identify entities that play key roles in the U.S. securities markets due to the magnitude of their activity in these markets.[130]

### i. Background

There are approximately 3,500 broker-dealers registered with the Commission pursuant to section 15(b) of the Exchange Act, and these entities encompass a broad range of sizes, business activities, and business models.[131] In 2013, the Commission proposed to include significant volume ATSs in the definition of SCI entity but at that time did not propose to include any other aspects of broker-dealer operations.[132] Rather,

---

129 *See infra* section III.A.b.iii.

130 *See infra* text accompanying notes 138-142 (summarizing comments on the SCI Proposing Release from commenters urging that application of Regulation SCI to broker-dealers should be limited to those with substantial transaction volume or having a large "footprint").

131 This estimate is derived from information on broker-dealer FOCUS Report Form X-17A-5 Schedule II filings as of Dec. 31, 2021, as well as the third quarter of 2022. *See also* FINRA, *2022 FINRA Industry Snapshot* (Mar. 2022), *available at* https://www.finra.org/sites/default/files/2022-03/2022-industry-snapshot.pdf. Section 15(b)(8) of the Exchange Act prohibits any broker-dealer from effecting transactions in securities unless it is a member of a registered national securities association (*i.e.*, FINRA) or effects securities transactions solely on a national securities exchange of which it is a member. *See* 15 U.S.C. 78*o*(b)(8); *see also* 17 CFR 240.15b9-1 ("Rule 15b9-1") (exempting proprietarily trading dealers from section 15(b)(8)'s national securities association membership requirement if they are a member of a national securities exchange and meet certain other requirements). *But see* Securities Exchange Act Release No. 95388 (July 29, 2022), 87 FR 49930 (Aug. 12, 2022) (proposing amendments to Exchange Act Rule 15b9-1 that would generally require proprietary trading firms that are registered broker-dealers to become a registered member of a national securities association (*i.e.,* FINRA) if they effect securities transactions otherwise than on an exchange of which they are a member). *See also* Securities Exchange Act Release No. 94524 (Mar. 28, 2022), 87 FR 23054 (Apr. 18, 2022) ("Dealer-Trader Release") (proposing to further define "dealer" and "government securities dealer" to identify certain activities that would constitute a "regular business" requiring a person engaged in those activities to register as a "dealer" or a "government securities dealer," absent an exception or exemption). Because the proposed amendments to further define the definition of dealer could result in a greater number of dealers and the amendments proposed to expand and update Regulation SCI could impact these newly designated dealers, commenters also are encouraged to review the Dealer-Trader Release to determine whether it might affect their comments on this proposal.

132 *See* SCI Proposing Release, *supra* note 14, at 18138-42.

the Commission solicited comment on whether certain classes of broker-dealers should be covered. In particular, the Commission sought comment on whether Regulation SCI should apply, for example, to OTC market makers[133] (either all or those that execute a significant volume of orders), exchange market makers[134] (either all or those that trade a significant volume on exchanges), order-entry firms that handle and route order flow for execution (either all or those that handle a significant volume of investor orders), clearing broker-dealers (either all or those that engage in a significant amount of clearing activities), and/or large multi-service broker-dealers that engage in a variety of order handling, trading, and clearing activities.[135] Although OTC market makers and clearing broker-dealers were noted specifically as examples of categories of broker-dealers that could pose significant risk to the market if a large portion of the order flow they handle or process were disrupted due to a systems issue, the Commission broadly solicited commenters' views on the importance of different categories of broker-dealers to the stability of overall securities market infrastructure and the risks posed by their systems.[136]

As summarized in the SCI Adopting Release, commenters' views varied.[137] One commenter opined that market makers and brokers or dealers that execute orders

---

133 An OTC market maker is a dealer that holds itself out as willing to buy and sell NMS stocks on a continuous basis in amounts of less than block size otherwise than on an exchange. *See* 17 CFR 242.600(b)(64).

134 An exchange market maker is any member of a national securities exchange that is registered as a specialist or market maker pursuant to the rules of such exchange. *See* 17 CFR 242.600(b)(32).

135 *See* SCI Proposing Release, *supra* note 14, at 18139-40.

136 *See* SCI Proposing Release, *supra* note 14, at 18138-40 (including questions 194-196 soliciting comment on whether and how to distinguish between and among categories of broker-dealers, such as OTC market makers, order entry firms that handle and route order flow for execution, clearing broker-dealers, and large multi-service broker-dealers that engage in a variety of order handling, trading, and clearing activities).

137 *See* SCI Adopting Release, *supra* note 1, at 72365.

internally by trading as a principal or crossing orders as an agent and handle market share that exceeds that of certain SCI ATSs should be subject to Regulation SCI.[138] Others stated that market makers, high frequency trading firms, or any firm with market access should be included, arguing that these market participants could present systemic risks to the market and had "a significant footprint in the markets."[139] Others stated that broker-dealers should be SCI entities because 17 CFR 240.15c3-5 ("Rule 15c3-5" or "Market Access Rule"),[140] requiring the implementation of risk management and supervisory controls to limit risk associated with routing orders to exchanges or ATSs, was not sufficient by itself, as it does not address the reliability or integrity of the systems that implement such controls.[141] One commenter stated that Regulation SCI should be extended to any trading platforms that transact significant volume, including systems that are not required to register as an ATS because all executions are against the bids and offers of a single dealer.[142] In contrast, other commenters argued that broker-dealers should not be subject to Regulation SCI because they must comply with other Exchange Act and FINRA rules and the proposed Regulation SCI requirements would be "duplicative and unduly burdensome."[143] At adoption, the Commission stated that "should [it] decide to propose to apply the requirements of Regulation SCI to [broker-

---

138 *See id.* (citing letter from the New York Stock Exchange, Inc. ("NYSE")).

139 *See id.* (citing letters from Liquidnet, Inc., David Lauer, and R.T. Leuchtkafer).

140 *See* 17 CFR 240.15c3-5.

141 *See* SCI Adopting Release, *supra* note 1, at 72365 (citing letters from David Lauer and the NYSE).

142 *See id.* (citing letter from BlackRock at 4, in which BlackRock stated that trading systems that "transact significant volume" are "venues that have a meaningful role and impact on the equity market").

143 *See id.*

dealer operations other than ATSs, it] would issue a separate release discussing such a proposal and would take these comments into account."[144]

In considering expansion of Regulation SCI to broker-dealers or broker-dealer operations beyond SCI ATSs, the Commission has considered the extent to which current Commission and FINRA rules affect how broker-dealers design and review their systems for capacity, integrity, resiliency, availability, and/or security adequate to maintain operational capability and promote the maintenance of fair and orderly markets and compliance with federal securities laws and regulations, and whether additional technology oversight is appropriate for certain broker-dealers based on the magnitude of their activity in the markets today.[145] The Commission proposes to apply Regulation SCI to a limited number of the approximately 3,500 broker-dealers registered with the Commission. The proposed thresholds are designed to identify firms that, by virtue of their total assets or level of transaction activity over a period of time and on a consistent basis, play a significant role in the orderly functioning of U.S. securities markets. The thresholds are designed to identify firms that, if adversely affected by a technology event, could disrupt or impede orderly and efficient market operations more broadly.

#### ii. Current Regulatory Oversight of Broker-Dealer Systems Technology

There are a number of Commission and FINRA rules that affect how broker-dealers design and maintain their technology and promote business continuity and

---

144 SCI Adopting Release, *supra* note 1, at 72366.

145 As noted above, the concurrently issued Exchange Act Cybersecurity Proposal would establish minimum "cybersecurity rules" for all broker-dealers. That proposal does not, however, independently address weaknesses in broker-dealer operational capacity or resiliency not attributable to cybersecurity breaches.

regulatory compliance.[146] Although these rules may support the goal of more resilient broker-dealer systems, they are not designed to address the same concerns that Regulation SCI addresses and are not a substitute for Regulation SCI.[147]

As some commenters on the SCI Proposing Release stated, the Market Access Rule is relevant to certain broker-dealer systems. The Market Access Rule requires broker-dealers with market access to implement, on a market-wide basis, effective financial and regulatory risk management controls and supervisory procedures reasonably designed to limit financial exposure and ensure compliance with applicable regulatory requirements, and thus seeks to address, among other things, certain risks posed to the markets by broker-dealer systems.[148] Pursuant to the Market Access Rule, a broker or dealer with market access, or that provides a customer or any other person with access to a national securities exchange or ATS through use of its market participant identifier or otherwise, must establish, document, and maintain a system of risk management controls

---

146 17 CFR 240.3a1-1(a)(2) ("Rule 3a1-1(a)(2)"), exempts from the Exchange Act section 3(a)(1) definition of "exchange" an organization, association, or group of persons that complies with Regulation ATS. All such exempted ATSs must be a registered broker-dealer and become a member of an SRO, which typically is FINRA. Accordingly, FINRA rules applicable to broker-dealers apply to ATSs. A similar discussion of FINRA rules applicable to ATSs appears in the SCI Adopting Release, *supra* note 1, at 72263.

147 *See infra* notes 148-166 and accompanying text. *See also* SCI Adopting Release, *supra* note 1, at 72263 (n. 115 and accompanying text), 72365 (discussing comments received).

148 *See* Securities Exchange Act Release No. 63241 (Nov. 3, 2010), 75 FR 69792 (Nov. 15, 2010) ("Market Access Release"). Under 17 CFR 240.15c3-5(a)(1) ("Rule 15c3-5(a)(1)"), "market access" is defined to mean: (i) access to trading in securities on an exchange or ATS as a result of being a member or subscriber of the exchange or ATS, respectively; or (ii) access to trading in securities on an ATS provided by a broker-dealer operator of an ATS to a non-broker-dealer. *See* 17 CFR 240.15c3-5(a)(1). In adopting Rule 15c3-5(a)(1), the Commission stated that "the risks associated with market access…are present whenever a broker-dealer trades as a member of an exchange or subscriber to an ATS, whether for its own proprietary account or as agent for its customers, including traditional agency brokerage and through direct market access or sponsored access arrangements." *See* Market Access Release at 69798. As such, the Commission stated that "to effectively address these risks, Rule 15c3-5 must apply broadly to all access to trading on an Exchange or ATS." *Id.*

and supervisory procedures reasonably designed to manage the financial, regulatory, and other risks of this business activity.[149] The Market Access Rule specifies standards for financial and regulatory risk management controls and supervisory procedures.[150] It requires that the financial risk management controls and supervisory procedures must be reasonably designed to limit systematically the financial exposure of the broker or dealer that could arise from market access.[151] In addition, the Market Access Rule requires that regulatory risk management controls and supervisory procedures be reasonably designed to ensure compliance with all regulatory requirements.[152] As such, the focus of the Market Access Rule requires controls to prevent technology and other errors that can create some of the more significant risks to broker-dealers and the markets, namely those that arise when a broker-dealer enters orders into a national securities exchange or ATS, including when it provides sponsored or direct market access to customers or other persons, where the consequences of such an error can rapidly magnify and spread throughout the markets. Further, the Market Access Rule requires specific controls and procedures around a broker-dealer entering orders on a national securities exchange or ATS that Regulation SCI does not and would not prescribe.

In contrast, the policies and procedures required by Regulation SCI apply broadly to technology that supports trading, clearance and settlement, order routing, market data, market regulation, and market surveillance and, among other things, address their overall

---

149 *See* 17 CFR 240.15c3-5(b).

150 *See* 17 CFR 240.15c3-5(c).

151 *See* 17 CFR 240.15c3-5(c)(1).

152 *See* 17 CFR 240.15c3-5(c)(2). *See also* 17 CFR 240.15c3-5(a)(2) (defining "regulatory requirements" to mean all Federal securities laws, rules and regulations, and rules of self-regulatory organizations, that are applicable in connection with market access).

capacity, integrity, resilience, availability, and security independent of market access. Whereas the Market Access Rule prescribes specific controls and procedures around a broker-dealer entering orders on an exchange or ATS, it is not designed to ensure that the key technology pervasive and important to the functioning of the U.S. securities markets is robust, resilient, and secure.[153] Among other requirements, the policies and procedures requirements of Regulation SCI are designed to help ensure that the systems of SCI entities are adequate to maintain operational capability independent of any specific SCI event (*i.e.*, a systems issue such as a systems disruption, systems intrusion, or systems compliance issue). Further, the SCI review requirement obligates an SCI entity to assess the risks of its systems and effectiveness of its technology controls at least annually, identify weaknesses, and ensure compliance with the safeguards of Regulation SCI. The Market Access Rule and Regulation SCI, therefore, have different requirements and would operate in conjunction with each other to help ensure that SCI broker-dealer SCI systems, whether used for access to the national securities exchanges or ATSs or not, are robust, resilient, and secure.

Broker-dealers are also subject to the Commission's financial responsibility rules (17 CFR 240.15c3-1 ("Rule 15c3-1") and 17 CFR 240.15c3-3 ("Rule 15c3-3")) under the Exchange Act. Rule 15c3-1 requires broker-dealers to maintain minimum amounts of net capital, ensuring that the broker-dealer at all times has enough liquid assets to promptly satisfy all creditor claims if the broker-dealer were to go out of business.[154] Rule 15c3-3

---

153 *See also supra* note 141 and accompanying text.

154 *See* 17 CFR 240.15c3-1.

imposes requirements relating to safeguarding customer funds and securities.[155] These rules provide protections for broker-dealer counterparties and customers and can help to mitigate the risks to, and impact on, customers and other market participants by protecting them from the consequences of financial failure that may occur because of a systems issue at a broker-dealer, and thus have a different scope and purpose from Regulation SCI.[156]

Pursuant to 17 CFR 240.17a-3 ("Rule 17a-3" under the Exchange Act) and 17 CFR 240.17a-4 ("Rule 17a-4" under the Exchange Act), broker-dealers are required to make and keep current records detailing, among other things, securities transactions, money balances, and securities positions.[157] A systems issue at a broker-dealer would not excuse the broker-dealer for noncompliance with these requirements.[158] Further, a broker-dealer that fails to make and keep current the records required by Rule 17a-3 must give notice to the Commission of this fact on the same day and, thereafter, within 48 hours transmit a report to the Commission stating what the broker-dealer has done or is doing to

---

155 *See* 17 CFR 240.15c3-3.

156 Similarly, 17 CFR 248.30 ("Rule 30" of Regulation S-P), which requires registered brokers and dealers to have written policies and procedures that are reasonably designed to safeguard customer records and information—to insure their security and confidentiality, protect against threats or hazards to their security and integrity and protect against unauthorized access or use that could result in substantial harm or inconvenience to any customer—is not designed to help ensure operational capability of market related systems. In addition, 17 CFR 248.201 ("Regulation S-ID") requires financial institutions or creditors (defined to include registered broker-dealers) that have one or more covered accounts, as defined in 17 CFR 248.201(b)(3) (*e.g.*, brokerage account), to develop and implement a written identity theft prevention program to detect, prevent, and mitigate identity theft in connection with covered accounts that includes policies and procedures to identify and incorporate red flags into the program, detect and respond to red flags, and incorporate periodic updates to the program. This rule, however, is also not designed to ensure operational capability of market related systems.

157 *See* 17 CFR 240.17a-3; 17 CFR 240.17a-4.

158 *See, e.g.*, Securities Exchange Act Release No. 40162 (July 2, 1998), 63 FR 37668 (July 13, 1998) (stating that computer systems with "Year 2000 Problems" may be deemed not to have accurate and current records and be in violation of Rule 17a-3).

correct the situation.[159] Regulation SCI, however, more directly addresses mitigating the impact of technology failures with respect to SCI systems and indirect SCI systems (which include systems that are not used to make and keep current the records required by Rule 17a-3). Specifically, it requires notifications to the Commission for a different set of events—systems intrusions, systems compliance issues, and systems disruptions—than the notification requirements of 17 CFR 240.17a-11 ("Rule 17a-11"), and is therefore not duplicative of Rule 17a-11. In addition, it requires that, when an SCI event has occurred, an SCI entity must begin to take appropriate corrective action which must include, at a minimum, mitigating potential harm to investors and market integrity resulting from the SCI event and devoting adequate resources to remedy the SCI event as soon as reasonably practicable.

FINRA also has several rules that are similar to, but take a different approach from, Regulation SCI. For example, FINRA Rule 4370 requires that each broker-dealer create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption that are reasonably designed to enable them to meet their existing obligations to customers. The procedures must also address the broker-dealer's existing relationships with other broker-dealers and counterparties. A broker-dealer is required to update its plan in the event of any material change to the member's operations, structure, business, or location and must conduct an annual review of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location. The rule sets

---

[159] *See* 17 CFR 240.17a-11.

forth general minimum elements that a broker-dealer's business continuity plan must address.[160]

This rule is akin to Regulation SCI's Rule 1001(a)(2)(v) requiring policies and procedures for business continuity and disaster recovery plans.[161] However, unlike Regulation SCI, the FINRA rule does not include the requirement that the business continuity and disaster recovery plans be reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption, nor does it require the functional and performance testing and coordination of industry or sector-testing of such plans, which are instrumental in achieving the goals of Regulation SCI with respect to SCI entities.[162] In addition, FINRA Rule 4370 contains certain provisions that Regulation SCI does not.[163] For example, a broker-dealer must disclose to its customers through public disclosure statements how its business continuity plan addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope.[164] Accordingly, FINRA Rule 4370 and Regulation SCI would operate in conjunction with one another to help ensure that an SCI broker-dealer has business continuity and disaster recovery plans to achieve the goals of each rule.

---

160 Specifically, FINRA Rule 4370 requires that each plan must, at a minimum, address: data back-up and recovery; all mission critical systems; financial and operational assessments; alternate communications between customers and the member; alternate communications between the member and its employees; alternate physical location of employees; critical business constituent, bank, and counter-party impact; regulatory reporting; communications with regulators; and how the member will assure customers' prompt access to their funds and securities in the event that the member determines that it is unable to continue its business.

161 *See* SCI Adopting Release, *supra* note 1, at 72263-64.

162 *Id.*

163 *See supra* note 160.

164 *See* FINRA Rule 4370(e).

FINRA Rule 3110(b)(1) requires each broker-dealer to establish, maintain, and enforce written procedures to supervise the types of business in which it engages and to supervise the activities of registered representatives, registered principals, and other associated persons that are reasonably designed to achieve compliance with applicable securities laws and regulations.

This supervisory obligation extends to member firms' outsourcing of certain "covered activities"—activities or functions that, if performed directly by a member firm, would be required to be the subject of a supervisory system and written supervisory procedures pursuant to FINRA Rule 3110.[165] This rule is broadly similar to Rule 1001(b) of Regulation SCI regarding policies and procedures to ensure systems compliance. However, unlike Rule 1001(b), which focuses on ensuring that an entity's systems operate in compliance with the Exchange Act, the rules and regulations thereunder, and the entity's rules and governing documents, this FINRA rule does not specifically address compliance of broker-dealers' *systems*. Further, this provision does not cover more broadly policies and procedures akin to those in Rule 1001(a) of Regulation SCI regarding ensuring the SCI entity's operational capability. FINRA Rule 3110(b)(1) and Regulation SCI would operate in conjunction to help ensure that the SCI systems of SCI broker-dealers, including those operated by third parties, are robust, resilient, and operate as intended.

---

165 *See* FINRA, *Regulatory Notice 21-29: Vendor Management and Outsourcing* (Aug. 13, 2021), *available at* https://www.finra.org/sites/default/files/2021-08/Regulatory-Notice-21-29.pdf; FINRA, *Notice to Members 05-48: Outsourcing* (July 2005), *available at* https://www.finra.org/sites/default/files/NoticeDocument/p014735.pdf.

FINRA Rule 3130 requires a broker-dealer's chief compliance officer to certify annually that the member has in place processes to establish, maintain, review, test, and modify written policies and procedures reasonably designed to achieve compliance with applicable FINRA rules, MSRB rules, and federal securities laws and regulations. This rule is similar to Rule 1001(b) of Regulation SCI regarding policies and procedures to ensure systems compliance; however, like FINRA Rule 3130(b)(1), it does not specifically address compliance of broker-dealers' *systems*, and does not require similar policies and procedures to those in Rule 1001(a) of Regulation SCI regarding operational capability of SCI entities. Therefore, FINRA Rule 3130 and Regulation SCI would operate in conjunction with each other to help ensure compliance with applicable law.

FINRA Rule 4530 imposes a regime for reporting certain events to FINRA, including, among other things, compliance issues and other events where a broker-dealer has concluded, or should have reasonably concluded, that a violation of securities or other enumerated law, rule, or regulation of any domestic or foreign regulatory body or SRO has occurred. This requirement is similar to Regulation SCI's reporting requirements under Rule 1002 with respect to systems compliance issues; however, it does not cover reporting of systems disruptions and systems intrusions that did not also involve a violation of a securities law, rule, or regulation. Further, the FINRA reporting rule differs from the Commission notification requirements with respect to the scope, timing, content and required recipient of the reports. FINRA Rule 4530 addressing reporting of certain issues to FINRA is thus not duplicative of Regulation SCI, which, among other things, was designed to enhance direct Commission oversight of entities

designated as key entities because they play a significant role in the U.S. securities markets.

Additionally, while regulations and associated guidance applicable to bank holding companies promulgated by the Federal Reserve Board and other bank regulators address operational resilience, their direct application is to bank holding companies rather than broker-dealers registered with the Commission. For example, a 2020 interagency paper issued by the Federal Reserve Board, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation sets forth "sound practices" for the largest, most complex firms, including U.S. bank holding companies, to follow to strengthen their operational resilience. While this publication offers key strategies for covered entities to follow to remain resilient, many of which are similar to what Regulation SCI requires, they are not mandatory for registered broker-dealers.[166] Thus, although some Exchange Act and FINRA rules other than Regulation SCI support the goal of robust and resilient broker-dealer systems, the Commission believes that additional protections, reporting of systems problems, and direct Commission oversight of broker-dealer technology is appropriate for the largest broker-dealers.

---

166 *See* Federal Reserve Board, *SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience* (Nov. 2, 2020), ("Banking Interagency Paper"), *available at* https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm ("To help large and complex domestic firms address unforeseen challenges to their operational resilience, the sound practices are drawn from existing regulations, guidance, and statements as well as common industry standards that address operational risk management, business continuity management, third-party risk management, cybersecurity risk management, and recovery and resolution planning."). The paper applies to national banks, state member banks, state nonmember banks, savings associations, U.S. bank holding companies, and savings and loan holding companies that have average total consolidated assets greater than or equal to (a) $250 billion or (b) $100 billion and have $75 billion or more in average cross-jurisdictional activity, average weighted short-term wholesale funding, average nonbank assets, or average off-balance sheet exposure. As discussed below, the Commission's proposed approach to identifying SCI broker-dealers similarly takes into account the size of the firm, as measured by a total assets threshold and/or market activity thresholds.

### iii. Proposed Thresholds for an "SCI broker-dealer"

*Overview*

As proposed, Regulation SCI would apply to a limited number of broker-dealers that satisfy: (i) a total assets threshold, or (ii) one or more transaction activity thresholds.

The Commission preliminarily believes that a broker-dealer that meets the proposed thresholds for assets or transaction activity, whether operating in multiple markets or predominantly in a single market, that becomes unreliable or unavailable due to a systems issue, risks disrupting fair and orderly market functioning.

Current Regulation SCI applies to all national securities exchanges and certain significant-volume ATSs, all of which are highly dependent on sophisticated automated and interconnected systems. As electronic trading has grown, and continues to grow in some asset classes, many broker-dealers are similarly dependent on sophisticated and interconnected automated systems.[167] These broker-dealer systems contribute to the orderly functioning of U.S. securities markets, encompassing, for example, systems for trading and quoting, order handling, dissemination and processing of market data, and the process of clearance and settlement.

An "SCI broker-dealer" would be a broker or dealer registered with the Commission pursuant to section 15(b) of the Exchange Act which:

- In at least two of the four preceding calendar quarters, ending March 31, June 30, September 30, and December 31, reported to the Commission, on Form X-

---

[167] For example, *see* Algorithmic Trading Report, *supra* note 3 (discussing many uses of computer systems in contemporary markets, particularly with respect to the trading of equity and debt securities).

17A-5 (§ 249.617),[168] total assets in an amount that equals five percent (5%) or more of the total assets of all security brokers and dealers; or[169]

- During at least four of the preceding six calendar months:
    - With respect to transactions in NMS stocks, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the average daily dollar volume[170] reported by or pursuant to applicable effective transaction reporting plans, provided, however, that for purposes of calculating its activity in transactions effected otherwise than on a national securities exchange or on an alternative trading system, the broker-dealer shall exclude transactions for which it was not the executing party; or
    - With respect to transactions in exchange-listed options contracts, transacted average daily dollar volume in an amount that equals ten

---

168 Broker-dealers that file Form X-17A-5 on a monthly basis would use their total assets, as reported on Item 940 of Form X-17A-5, for the months ending Mar. 31, June 30, Sept. 30, and Dec. 31. Broker-dealers that file Form X-17A-5 on a quarterly basis would use their total assets, as reported on Item 940 of Form X-17A-5, for the quarters ending Mar. 31, June 30, Sept. 30, and Dec. 31.

169 *See* definition of SCI broker-dealer in proposed amended Rule 1000. The term "total assets of all security brokers and dealers" would, for purposes of this threshold, mean the total assets calculated and made publicly available by the Board of Governors of the Federal Reserve, or any subsequent provider of such information, for the associated preceding calendar quarter. *Id. See supra* note 127; *infra* text accompanying notes 181-185.

170 For June 2022, the average daily dollar volume in NMS stocks, as reported by applicable effective transaction reporting plans, was approximately $560 billion, with 10% of that reflecting approximately $56 billion.

percent (10%) or more of the average daily dollar volume[171] reported by an applicable effective national market system plan; or

- With respect to transactions in U.S. Treasury Securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume[172] made available by the self-regulatory organizations[173] to which such transactions are reported; or
- With respect to transactions in Agency Securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume[174] made available by the self-regulatory organizations[175] to which such transactions are reported.

An SCI broker-dealer would be required to comply with the requirements of Regulation SCI six months after the SCI broker-dealer satisfied either threshold for the first time.

---

171 For June 2022, the average daily dollar volume in exchange-listed options contracts, as reported by an applicable effective national market system plan, was approximately $23.8 billion, with 10% of that reflecting approximately $2.4 billion.

172 For June 2022, the average daily dollar volume in U.S Treasury Securities, according to FINRA TRACE data, was approximately $634.1 billion, with 10% of that reflecting approximately $63.4 billion.

173 Currently, there is one self-regulatory organization to which transactions in U.S Treasury Securities are reported (*i.e.,* FINRA).

174 For June 2022, the average daily dollar volume in Agency Securities, according to FINRA TRACE data was approximately $223 billion, with 10% of that reflecting approximately $22.3 billion.

175 Currently, there is one self-regulatory organization to which transactions in U.S Treasury Securities are reported (*i.e.,* FINRA) and one organization to which transactions in Agency securities are reported (*i.e.,* FINRA).

The proposed thresholds are designed to identify the largest U.S. broker-dealers. To assess which broker-dealers should be subject to Regulation SCI,[176] the Commission has taken into account the size of registered broker-dealers based on analyses of: (i) total assets reported on Form X-17A-5 (Financial and Operational Combined Uniform Single ("FOCUS") Report Part II, Item 940),[177] and (ii) transaction activity in certain asset classes.

*Proposed Total Assets Threshold*

A broker-dealer would be an SCI broker-dealer and included in the definition of SCI entity if, in at least two of the four preceding calendar quarters ending March 31, June 30, September 30, and December 31, it reported to the Commission on Form X-17A-5, FOCUS Report Part II, Item 940 total assets in an amount that equals five percent or more of the total assets of all security brokers and dealers. Congress and multiple regulators have used total assets as a factor in assessing whether an entity warrants heightened oversight. For example, under the Dodd-Frank Act, the Financial Stability Oversight Council ("FSOC") considers financial assets as one factor to determine whether a U.S. non-bank financial services company is supervised by the Federal Reserve Board and subject to enhanced prudential standards.[178] Furthermore, the Dodd-Frank Act requires the Federal Reserve Board to establish enhanced prudential standards for bank

---

176 *See supra* note 82 and accompanying text.

177 *See* Form X-17A-5, FOCUS Report, Part II, at 3, *available at* https://www.sec.gov/files/formx-17a-5_2_2.pdf (requiring broker-dealers to report their total assets in Item 940).

178 *See* Dodd-Frank Act section 113(a)(2), 12 U.S.C. 5323(a)(2).

holding companies over a certain threshold of total assets.[179] Additionally, the Federal Deposit Insurance Corporation ("FDIC") increases its Deposit Insurance Fund assessment for large and highly complex institutions as compared to small banks.[180]

Although a broker-dealer's total assets alone could be used as the proposed rule's measure of an entity's size and significance, to ensure that a total assets measure reflects significant activity in relative terms, the Commission proposes to scale each broker-dealer's total assets (the numerator) to a quarterly measure of "total assets of all security brokers and dealers," as calculated by the Federal Reserve Board (the denominator).[181] The firm's total assets filed on FOCUS reports (of which each firm has current and direct knowledge) would be divided by the broader measure of total assets for all securities brokers and dealers calculated and made publicly available by the Federal Reserve Board, or any subsequent provider of such information, for the purpose of comparing the size of a broker-dealer to the group of entities tracked by the Federal Reserve Board.[182] The Commission understands that the Federal Reserve Board publishes total assets for all security brokers and dealers approximately ten weeks after the end of the quarter (*e.g.*,

---

179 *See* Dodd-Frank Act section 165, 12 U.S.C. 5365(a)(1). *See also* Federal Reserve Board, Prudential Standards for Large Bank Holding Companies, Savings and Loan Holding Companies, and Foreign Banking Organizations, 84 FR 59032 (Nov. 1, 2019), and Federal Reserve Board, Changes to Applicability Thresholds for Regulatory Capital and Liquidity Requirements, 84 FR 59230 (Nov. 1, 2019). *See* SCI Adopting Release, *supra* note 1, at 72259, and also definition of "critical SCI systems" in 17 CFR 142.1000.

180 *See* FDIC, *Deposit Insurance Fund, Assessment Rates & Methodology* (last updated July 20, 2021), *available at* https://www.fdic.gov/resources/deposit-insurance/deposit-insurance-fund/dif-assessments.html.

181 *See supra* note 127. This figure has been calculated by the Federal Reserve Board and made available on the Federal Reserve Economic Data (FRED) website for many years. As stated above, the total assets figure calculated by the Federal Reserve Board is based on the information reported to the Commission by "security broker-dealers" on either the FOCUS report or the FOGS report. *See id.*

182 *Id.*

2022 third quarter results ((for quarter ending September 30, 2022)) were published on December 13, 2022). Therefore, the information for the preceding quarter should be available prior to the date on which the firm's FOCUS report is required to be filed with the Commission for the relevant quarter. To enable each firm to calculate whether it exceeds the threshold at the time it files its FOCUS report (which is due 17 days after the end of the quarter/month),[183] broker-dealers would compare their total assets to the previous quarter on or before the FOCUS report filing deadline. Accordingly, to assess whether it exceeds the threshold for a relevant calendar quarter, a broker-dealer would divide its total assets reported on Form X-17A-5, FOCUS Report Part II, Item 940 for that quarter by the total assets of all security brokers and dealers for the preceding quarter, as made available by the Federal Reserve.[184] Although it is possible that the total assets of all security brokers and dealers could increase or decrease sharply from one quarter to the next, the FRED data shows that this has occurred rarely and that the asset totals in the Federal Reserve Board's data generally do not change significantly from

---

183 Form X-17A-5 must be filed within 17 business days after the end of each calendar quarter, within 17 business days after the end of the fiscal year where that date is not the end of a calendar quarter, and/or monthly, in accordance with 17 CFR 240.17a-5, 240.17a-12, or 240.18a-7, as applicable. *See* Instructions to Form X-17A-5, FOCUS Report, Part II, at 2, *available at* https://www.sec.gov/files/formx-17a-5_22.pdf.

184 *See supra* note 127. For example, to assess whether it exceeds the threshold for the calendar quarter ending Dec. 31, a broker-dealer would divide its total assets reported Form X-17A-5, FOCUS Report Part II, Item 940 for the quarter ending Dec. 31, and divide that by the total assets of security brokers and dealers for the third quarter (ending Sept. 30) of the same year, as obtained from the Federal Reserve Board. If a broker-dealer reported $350 billion, $385 billion, $359 billion, and $386 billion in total assets on its FOCUS reports for Q4 2022, Q3 2022, Q2 2022, and Q1 2022, respectively, the broker-dealer would divide its total assets for each quarter by 5.07 trillion (for Q3 2022), $5.07 trillion (for Q2 2022), $5.23 trillion (for Q1 2022), and $4.96 trillion (for Q1 2021), respectively. *See infra* note 185. The broker-dealer's total assets as a percentage of the total assets of all security broker-dealers would be 6.9% for Q4 2022, 7.6% for Q3 2022. 6.9% for Q2 2022, and 7.8% for Q1 2022. In all four quarters, the broker-dealer would exceed the 5% threshold and therefore meet the definition of SCI broker-dealer.

quarter to quarter.[185] The Commission therefore believes that overall, the data made available by the Federal Reserve Board is an appropriate and consistent figure for use as a denominator in the proposed threshold.[186]

If a firm meets or exceeds the threshold in two of the four preceding calendar quarters, it would be required to comply with Regulation SCI beginning six months after the end of the quarter in which the SCI broker-dealer satisfied the proposed asset threshold for the first time. Based on data from recent quarters, at the proposed threshold, a broker-dealer registered with the Commission pursuant to section 15(b) of the Exchange Act and having total assets on its balance sheet in excess of approximately $250 billion in two of the preceding four calendar quarters would be an SCI broker-dealer for as long as it continued to satisfy the threshold.[187]

The Commission believes that the proposed threshold of five percent of total assets is a reasonable approach to identifying the largest broker-dealers. In addition to its

---

185 *See* Board of Governors of the Federal Reserve System (US), *Security Brokers and Dealers; Total Assets (Balance Sheet), Level [BOGZ1FL664090663Q]*, retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/BOGZ1FL664090663Q. The total assets data from the Federal Reserve shows a sharp drop at the time of the financial crisis, from Q3 2008 to Q4 2008. *See id.* More recent data show total assets for all security-broker dealers for purpose of the proposed denominator in recent quarters in trillion dollars as follows: Q3 2022: 5.07 trillion; Q2 2022: $5.07 trillion; Q1 2022: $5.23 trillion; Q4 2021: $4.96 trillion; Q3 2021: $5.05 trillion; Q2 2021: $4.94 trillion. *See id.*

186 The Federal Reserve Board data includes total assets reported on both FOCUS and FOGS forms. Its use would result in a conservative number of broker-dealers meeting the total assets threshold (*i.e.*, because elimination of FOGS data would reduce the size of the denominator). The Commission solicits comment below on whether another figure would be a more appropriate and useful measure for determining if a broker-dealer is in the top 5% of all broker-dealers in terms of its total assets, and if a percentage threshold is better measure than a dollar measure.

187 As a specific example, based on totals retrieved from FRED (*see supra* note 127) a broker-dealer assessing its total assets in Dec. 2022 would determine if that level exceeded 5% of total assets in two of the preceding four quarters (approximately $253 billion, $253 billion, $261 billion, and $248 billion, for Q3 of 2022, Q2 of 2022, Q1 of 2022, and Q4 of 2021, respectively). *See also* Banking Interagency Paper, *supra* note 166 (applicable to banking institutions having in excess of an average of $250 billion in total assets).

broad consistency with the approach taken by banking regulators,[188] this approach takes into consideration the multiple roles that the largest broker-dealers play in the U.S. securities markets. Not only do the largest broker-dealers generate liquidity in multiple types of securities, but many also operate multiple types of trading platforms.[189] Further, entities with assets at this level also take risk that they seek to hedge, in some cases using "central risk books" for that and other purposes, and engage in routing substantial order flow to other trading venues.[190] For these reasons, the Commission believes that systems issues at firms having assets at this level would have the potential to impact investors, the overall market, and the trading of individual securities, and that therefore their market technology should be subject to the requirements and safeguards of Regulation SCI. The threshold is designed to be appropriately high enough to ensure that only the largest broker-dealers are subject to the obligations, and associated burdens and costs, of Regulation SCI. It is also designed to be a relative measure that does not become outdated over time, as the size of the overall market expands or contracts.

---

188 *See, e.g.*, *supra* notes 166 and 187 (discussing Banking Interagency Paper).

189 For a broad discussion of these roles, *see, e.g.*, Rosenblatt Securities, *2022 US Equity Trading Venue Guide* (May 24, 2022) (discussing among other things the features of single-dealer platforms for equity securities that are operated by broker-dealers); *Regulation of NMS Stock Alternative Trading Systems*, Securities Exchange Act Release No. 83663 (July 18, 2018), 83 FR 38768 at 38770-72 (Aug. 7, 2018) (discussing among other things the operational complexity of multi-service broker-dealer with significant brokerage and dealing activity apart from operation of one or more ATSs).

190 *See, e.g.*, Rosenblatt Securities, *Central Risk Books: What the Buy Side Needs to Know* (Oct. 18, 2018) (stating that all of the biggest bank-affiliated broker-dealers have some form of central risk book and that the "critical mass of order flow or principal activity, spread across asset classes and regions" may not justify the operation of these books for smaller more focused firms). *See also* Algorithmic Trading Report, *supra* note 3, at 41-42 (describing central risk books as an important source of block liquidity). All of the firms that satisfy the proposed total assets threshold also satisfy at least one of the proposed trading activity thresholds. *See infra* text accompanying note 219.

As noted, the proposed total assets threshold for SCI broker-dealers would include a proposed time period measurement of "at least two of the four preceding calendar quarters." Requiring that the threshold is met in two out of the four preceding quarters would help mitigate the effect of a steep increase/decrease in total assets in any individual quarter.

Further, this measurement is designed to capture only the broker-dealers that are consistently at or above the proposed five percent threshold, and would not include a broker-dealer that may have had an anomalous quarterly increase, so that a short-term spike in total assets uncharacteristic of the broker-dealer's overall total asset history would not cause it to become subject to Regulation SCI. Although the Commission is also proposing a time period measurement of "at least four of the preceding six calendar months" for the trading activity thresholds discussed below (consistent with the time period measurement for SCI ATSs),[191] using a quarterly measure for the total asset threshold is appropriate because FOCUS reports are required at least quarterly for all broker-dealers and the proposed scaling measure is one that is updated quarterly. Based on its analysis of FOCUS reports during the period from Q4 2021 through Q3 2022, the Commission estimates that five entities would exceed the proposed threshold (with the fifth-ranked firm in each quarter reporting total assets in excess of $300 billion, and all firms ranging from approximately seven to 14 percent of the total assets reported by the Federal Reserve Board for the previous quarter), and further anticipates that this

---

[191] *See* Rule 1000 (definition of "SCI ATS") (providing a time period measurement of "at least four of the preceding six calendar months").

threshold would result in little, if any, variation in which firms exceed the threshold over the course of four calendar quarters.[192]

*Proposed Transaction Activity Threshold*

In the Commission's view, a broker-dealer's transaction activity is another reasonable measure for estimating the significance of a broker-dealer's role in contributing to fair and orderly markets. In several asset classes, the transaction activity of each of a relatively small number of broker-dealers constitutes a share of trading that could, if affected by a systems issue, negatively impact fair and orderly markets. For example, in NMS stocks, some broker-dealers constitute significant concentrations of on-exchange trading, and some broker-dealers execute off-exchange transactions at levels that rival or exceed the volume of trading on current SCI entities.[193] For listed options, which are required to execute on a national securities exchange, a small number of firms participate in a high proportion of trades.[194] Similarly, transaction reporting data for U.S. Treasury Securities and Agency Securities reveal that a handful of broker-dealers each represent a significant percentage of the average weekly (for U.S. Treasury Securities) or

---

192 As with other entities that are SCI entities because they satisfy a threshold (*e.g.*, SCI ATSs), an SCI broker-dealer would no longer be an SCI broker-dealer, and thus no longer be subject to Regulation SCI, in the quarter when it no longer satisfies the total assets test (i.e., it does not meet the threshold in two of the previous four quarters). This assumes the broker-dealer also does not meet or no longer satisfies the proposed transaction activity threshold.

193 For example, in Sept. 2022, one broker-dealer executed a greater proportion of shares in NMS stocks than all but two national securities exchanges. *See*, *e.g.*, FINRA, *OTC Transparency Data*, *available at* https://otctransparency.finra.org/otctransparency; CBOE, *Historical Market Volume Data*, *available at* https://www.cboe.com/us/equities/market_statistics/historical_market_volume/.

194 As discussed further below in this section, the Commission estimates that six firms would satisfy the 10% options transaction activity threshold.

daily (for Agency Securities) dollar volume reported by FINRA (currently the only SRO to which such transactions are reported).[195]

Accordingly, the Commission is proposing to include as an SCI entity any registered broker-dealer that, irrespective of the size of its balance sheet, consistently engages in transaction activity at a substantially high level in certain enumerated asset classes, scaled as a percentage of total average daily dollar volume over a specified time period.[196] If a significant systems issue at a broker-dealer that meets the proposed thresholds were to occur, the concern is that its effect would have widespread impact, for example, by impeding the ability of other market participants to trade securities in one or more of the identified asset classes, interrupting the price discovery process, or contributing to capacity issues at other broker-dealers. Further, if executions were delayed by a systems disruption in an SCI broker-dealer's trading, order routing, clearance and settlement, or market data system, due to the magnitude of the proposed covered transaction activity in which these firms consistently engage, the delay could have cascading effects disruptive to the broader market.[197]

---

195 As discussed further below in this section, the Commission estimates that four firms would satisfy the 10% U.S. Treasury Security transaction activity threshold, and six firms would satisfy the 10% Agency Security transaction activity threshold.

196 As discussed further below, the Commission proposes that average daily dollar volume be the denominator used as the scaling measure for each relevant asset class. *See infra* notes 211-217 and accompanying text (discussing entities that currently and may in the future receive and make available transaction reports, or aggregated volume statistics in NMS stocks, exchange-listed options, U.S. Treasury Securities, and Agency Securities).

197 For example, capacity constraints, whether due to risk management, or operational capability limitations of systems, could limit how much one broker-dealer could handle a sudden increase in order flow from a large broker-dealer. For context, based on analysis of data from the

The proposed transaction thresholds are broadly similar across different types of securities. However, because of differences in market structure, there are notable differences in the application of the thresholds across types of securities.

Regulation SCI currently applies to, among other entities, national securities exchanges for both listed equities and listed options, and to ATSs trading significant volume in NMS stocks. A national securities exchange and an ATS are a type of "trading center," as that term is defined in 17 CFR 242.600 through 242.614 ("Regulation NMS").[198] For purposes of counting transaction activity in NMS stocks, the proposed thresholds are anchored to broker-dealer activity conducted on or as a trading center. Therefore, the Commission is proposing, with respect to the transaction thresholds for NMS stocks, to include broker-dealer activity on national securities exchanges and NMS Stock ATSs, as well as broker-dealer activity as a trading center. Broker-dealer activity "as a trading center" refers in this context to trading activity in NMS stocks not effected on a national securities exchange or on an ATS, but by the broker-dealer, where the

---

Consolidated Audit Trail, in 2022, two large market makers in NMS stocks engaged in over-the counter transactions (all purchases and all sales effected otherwise than on a national securities exchange or ATS) having a total dollar volume of at least $37 billion on most trading days; with at least a quarter of trading days in 2022 having total dollar volume of $42.3 billion or more, and all trading days having an average total dollar volume of $37.3 billion. Counting volume across all venues (all purchases and all sales effected over-the counter, on a national securities exchange, or on ATS), these figures for the same two firms, respectively, are: at least $82.2 billion, ($67.6 marked as principal/riskless principal) on most trading days; at least $97.1 billion ($83.7 billion marked as principal/riskless principal) on at least a quarter of the trading days; and $83.5 billion ($69.4 billion marked as principal/riskless principal) as the average for all trading days.

198 Rule 600 of Regulation NMS defines the term trading center to mean: a national securities exchange or national securities association that operates an SRO trading facility, an alternative trading system, an exchange market maker, an OTC market maker, or any other broker or dealer that executes orders internally by trading as principal or crossing orders as agent. 17 CFR 242.600(b)(95).

broker-dealer is the executing party, either as principal or as agent.[199] A similar distinction is not made for exchange-listed options contracts because those transactions are executed on a national securities exchange.[200]

The "trading center" term in Regulation NMS applies only to NMS securities; however, there exist today electronic venues for fixed income securities that perform similar functions as trading centers and that are equally important to investors to execute trades in fixed income securities. Such electronic trading venues, particularly for U.S. Treasury Securities and Agency Securities (where electronic trading is prevalent[201]), have developed from a market structure in which electronic bilateral trading was and continues to be important. For this reason, the Commission is proposing to include under the SCI broker-dealer threshold all trades for U.S. Treasury Securities and Agency Securities in which a broker-dealer may participate.

As proposed, an "SCI broker-dealer" would include a broker-dealer that, during at least four of the preceding six calendar months: (i) with respect to transactions in NMS stocks, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the average daily dollar volume reported by or pursuant to applicable effective transaction reporting plans, provided, however, that for purposes of calculating its activity in transactions effected otherwise than on a national securities exchange or on an alternative trading system, the broker-dealer shall exclude transactions for which it was

---

199 *See* 17 CFR 242.600(a)(95), defining "trading center" to include, among other entities, "an OTC market maker, or any other broker or dealer that executes orders internally by trading as principal or crossing orders as agent."

200 In some cases, matching of orders for exchange-listed options occur on an ATS, with matches then routed to one or more national securities exchange for execution.

201 *See* Government Securities ATS Reproposal, *supra* note 84.

not the executing party; (ii) with respect to transactions in exchange-listed options contracts, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the average daily dollar volume reported by an applicable effective national market system plan; (iii) with respect to transactions in U.S. Treasury Securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume made available by the self-regulatory organizations to which such transactions are reported; or (iv) with respect to transactions in Agency securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume made available by the self-regulatory organizations to which such transactions are reported.[202]

The Commission proposes to add a definition of "U.S. Treasury Security" and "Agency Security" to clarify how the transaction activity threshold for these asset classes would operate.[203] A "U.S. Treasury Security" would mean a security issued by the U.S. Department of the Treasury. "Agency Security" would mean a debt security issued or guaranteed by a U.S. executive agency, as defined in 5 U.S.C. 105, or government-sponsored enterprise, as defined in 2 U.S.C. 622(8). These definitions are designed to

---

202 The proposed definition of SCI broker-dealer does not include a transaction activity threshold for equity securities that are not NMS stocks and for which transactions are reported to an SRO as a category in the proposed transaction activity threshold. The size of this market, as currently measured, is substantially smaller than the other asset classes enumerated. Based on its analysis of data from the Consolidated Audit Trail, between Oct. 2021 and Sept. 2022, for example, the average daily dollar volume for this market segment was approximately $2.6 billion. Nor do the proposed amendments to Regulation SCI include Fixed Income ATSs or broker-dealers that exceed a transaction activity threshold in corporate debt or municipal securities. *But see infra* section III.A.3 (requesting comment on the matter).

203 The Commission believes that the terms NMS stock and exchange-listed options are currently well understood. *See* Rule 600 of Regulation NMS (defining the terms NMS stock and NMS security and distinguishing NMS stocks from listed options on the basis of how transaction reports are made available).

provide the scope of securities an SCI broker-dealer must include when assessing whether it has satisfied the proposed transaction activity threshold. The proposed definitions are similar to and consistent with those in FINRA's rules,[204] to avoid confusion and facilitate the comparison between data used to create the numerator and denominator when assessing whether a broker-dealer surpassed the U.S. Treasury Security or Agency Security transaction thresholds.

As is the case currently for the thresholds applicable to SCI ATSs,[205] the proposed thresholds for SCI broker-dealers would include a proposed time period measurement of "at least four of the preceding six calendar months." Specifically, the proposed time measurement period is designed to capture broker-dealers that consistently meet the proposed thresholds and not capture broker-dealers with relatively low transaction activity that may have had an anomalous increase in trading on a given day or few days. In other words, a short-term spike in transaction activity uncharacteristic of a broker-dealer's overall activity should not cause it to become subject to Regulation SCI; using the proposed time period of at least four of the preceding six calendar months would help ensure this.

The proposed thresholds would generally take into account all of a broker-dealer's transactions.[206] The thresholds proposed are designed to identify firms whose transaction activity is of such a magnitude that a systems issue negatively impacting that

---

204 *See* FINRA Rules 6710(l) and 6710(p). FINRA Rule 6710 also establishes which securities are eligible for transaction reporting to the "Trade Reporting and Compliance Engine" (TRACE), which is the automated system developed by FINRA that, among other things, accommodates reporting and dissemination of transaction reports where applicable.

205 *See* Rule 1000 (definition of "SCI ATS").

206 As described further above and below, the proposed threshold for NMS stocks would operate slightly differently.

activity could contribute to a disruption in fair and orderly markets, and for which the application of Regulation SCI is therefore appropriate.

With respect to NMS stocks, only transactions which the broker-dealer (i) trades on a national securities exchange or an ATS, or (ii) executes off of a national securities exchange or an ATS would be counted. When a broker-dealer is the non-executing counterparty to an off-exchange, non-ATS transaction that transaction would not be counted for that broker-dealer.[207] The purpose of this approach is to count towards the threshold for NMS stocks broker-dealer activity on or as a trading center.

To assess whether it satisfies the proposed thresholds, a broker-dealer would need to determine its average daily dollar volume in an enumerated asset class each calendar month, and divide that figure by the total reported average daily dollar volume for that month. More specifically, its numerator would be the average daily dollar volume during the calendar month, taking into account all relevant purchase and sale transactions[208] in which the broker-dealer engaged during that calendar month, as determined by the broker-dealer from information in its books and records, as required to be kept pursuant

---

207 The volume for that trade, as reported through an effective transaction reporting plan, would still be included in the overall calculation of market volume used as the denominator in threshold calculations.

208 For NMS stocks, this would exclude those purchases or sales off-exchange and not effected through an ATS, in which the broker-dealer was not the executing party. As specific examples, when broker-dealer A routes a customer order to broker-dealer B for routing and execution, and broker-dealer B executes the customer order as principal or crosses it against another order it is holding, the volume for that order would contribute towards the threshold for broker-dealer B but not for broker-dealer A. Similarly, if broker-dealer A sends an order to the single-dealer platform operated by broker-dealer B, and broker-dealer B executes a trade against that order, the volume would contribute towards the threshold for broker-dealer B but not for broker-dealer A. For any asset class, the proposed definition of SCI broker-dealer would not exclude from a broker-dealer operator's transaction tally transactions executed on its own ATS. For example, if the broker-dealer operator trades as a participant on its ATS, or where a broker-dealer operator acts as a counterparty to every trade on its own ATS, its volume would be counted as trading activity of the broker-dealer.

to Exchange Act Rule 17a-3.[209] The denominator would be the total average daily dollar volume for each calendar month, as that total is determined from one or more sources that receive and make available transaction reports, or, as the case may be, aggregated price and volume statistics.

With respect to NMS stocks, information necessary to calculate the denominator currently is available from the plan processors (*i.e.,* the SIPs) of the CTA/CQ Plans and Nasdaq UTP Plan. These Plans are effective transaction reporting plans, and effective national market systems plans.[210] Following implementation of the Market Data Infrastructure rules, the information necessary to calculate the denominator would be available from a competing consolidator or may be self-determined by a self-aggregator that obtains the information pursuant to effective transaction reporting plans, as required by 17 CFR 242.601 ("Rule 601" of Regulation NMS) and 17 CFR 242.603(b) ("Rule 603(b)" of Regulation NMS).[211] For listed options, total average daily dollar volume may

---

209 *See* 17 CFR 240.17a-3(a)(6) (requiring a broker-dealer to keep a memorandum of each brokerage order given or received for the purchase or sale of a security, to include the price at which the order executed); 17 CFR 240.17a-3(a)(7) (requiring a memorandum of purchases and sales of a security for its own account, to include the price).

210 *See supra* note 20 and *infra* note 211. *See also infra* note 262 (stating that an ATS that trades NMS stocks is subject to Regulation SCI if its trading volume reaches: (i) 5% or more in any single NMS stock and 0.25% or more in all NMS stocks of the average daily dollar volume reported by applicable transaction reporting plans; or (ii) 1% or more in all NMS stocks of the average daily dollar volume reported by applicable transaction reporting plans).

211 With respect to NMS stocks, Rule 601 of Regulation NMS (17 CFR 242.601) requires national securities exchanges and national securities associations to report transactions and last sale data pursuant to an effective transaction reporting plan filed with the Commission in accordance with 17 CFR 242.608 ("Rule 608" of Regulation NMS). *See* 17 CFR 242.601. The national securities exchanges and FINRA comply with Rule 601 by satisfying the requirements of Rule 603(b) of Regulation NMS (which requires the national securities exchanges and FINRA to act jointly pursuant to one or more effective national market system plans, to disseminate consolidated

be determined from consolidated information made available by the plan processor of the OPRA Plan.[212]

With respect to U.S. Treasury Securities and Agency Securities, total average daily dollar volume may be determined from information made available by SROs to which transactions in U.S. Treasury Securities and Agency Securities are reported. Currently there is only one SRO to which this information is reported: FINRA.[213] In connection with its TRACE system, FINRA is currently the most complete source of

---

information, including transactions, in NMS stocks). Currently, transaction information is consolidated by the (exclusive) plan processor of each effective national market system plan (*i.e.*, the CTA/CQ Plan and Nasdaq UTP Plan for NMS stocks). *See* CTA Plan, *available at* https://www.ctaplan.com; Nasdaq UTP Plan, *available at* https://www.utpplan.com. After the implementation of the Market Data Infrastructure rules (*see* Market Data Infrastructure Adopting Release, *supra* note24) national securities exchanges and FINRA will be required to provide transaction reports to competing consolidators and/or self-aggregators pursuant to new effective national market system plans that satisfy the requirements of Rule 603(b). Pursuant to 17 CFR 242.600(a)(14) (Rule 600(a)(14) of Regulation NMS) the term "competing consolidator" means a securities information processor required to be registered pursuant to Rule 614 of Regulation NMS or a national securities exchange or national securities association that receives information with respect to quotations for and transactions in NMS stocks and generates a consolidated market data product for dissemination to any person. Pursuant to 17 CFR 242.600(a)(83) (Rule 600(a)(83) of Regulation NMS) the term "self-aggregator" means a broker, dealer, national securities exchange, national securities association, or investment adviser registered with the Commission that receives information with respect to quotations for and transactions in NMS stocks, including all data necessary to generate consolidated market data, and generates consolidated market data solely for internal use (with a proviso that a self-aggregator may make consolidated market data available to its affiliates that are registered with the Commission for their internal use). *See* Market Data Infrastructure Adopting Release, *supra* note 24 (providing a full discussion of these terms). Following implementation of the Market Data Infrastructure rules, a broker-dealer may obtain consolidated average daily dollar volume from its chosen competing consolidator, or independently calculate that figure itself, as a "self-aggregator."

212 *See* OPRA Plan, *available at* https://www.opraplan.com.

213 However, should a national securities exchange (an SRO) trade U.S. Treasury or Agency Securities in the future, if transaction reports are made available by that SRO, they would be relevant to determining consolidated average daily dollar volume.

aggregate volume in U.S. Treasury Securities and Agency Securities.[214] Specifically, FINRA Rule 6750(a) requires FINRA to disseminate information on Agency Securities, immediately upon receipt of the transaction report.[215] With respect to U.S. Treasury Securities, information in TRACE regarding individual transactions is for regulatory purposes only and is not disseminated publicly. However, pursuant to FINRA Rule 6750, on March 10, 2020, FINRA began posting on its website weekly, aggregate data on the trading volume of U.S. Treasury Securities reported to TRACE, and the Commission recently approved website posting of aggregate data more frequently (*i.e.,* daily).[216] Notwithstanding the transparency provided by FINRA/TRACE, aggregate trading volume in U.S. Treasury and Agency securities does not purport to reflect the whole of these markets, as aggregate volume statistics are limited to volume reported by TRACE reporters, including ATSs, registered-broker dealers that are members of FINRA, and

---

214 *See* FINRA, *Trade Reporting and Compliance Engine (TRACE)*, *available at* https://www.finra.org/filing-reporting/trace. FINRA Rule 6730(a)(1) requires FINRA members to report transactions in TRACE-Eligible Securities, which FINRA Rule 6710 defines to include U.S. Treasury Securities and Agency Securities. For each transaction in U.S. Treasury Securities and Agency Securities, a FINRA member would be required to report the CUSIP number or similar numeric identifier or FINRA symbol; size (volume) of the transaction; price of the transaction (or elements necessary to calculate price); symbol indicating whether transaction is a buy or sell; date of trade execution ("as/of" trades only); contra-party's identifier; capacity (principal or agent); time of execution; reporting side executing broker as "give-up" (if any); contra side introducing broker (in case of "give-up" trade); the commission (total dollar amount), if applicable; date of settlement; if the member is reporting a transaction that occurred on an ATS pursuant to FINRA Rule 6732, the ATS's separate Market Participant Identifier ("MPID"); and trade modifiers as required. For when-issued transactions in U.S. Treasury Securities, a FINRA member would be required to report the yield in lieu of price. *See* FINRA Rule 6730(c).

215 *See* FINRA Rule 6750(a).

216 *See* Securities Exchange Act Release No. 95438 (Aug. 5, 2022), 87 FR 49626 (Aug. 11, 2022) (Order Approving a Proposed Rule Change to Amend FINRA Rule 6750 Regarding the Publication of Aggregated Transaction Information on U.S. Treasury Securities). The implementation date for these TRACE enhancements for U.S. Treasury Securities was Feb. 13, 2023, at which point the weekly data reports were replaced with daily and monthly reports. Using daily reports of U.S. Treasury Security data, broker-dealers should have the information necessary to complete the calculations needed to assess if they satisfy the proposed threshold.

depository institutions meeting transaction volume thresholds in U.S. Treasury Securities, agency-issued debt and mortgage-backed securities.[217]

Counting all relevant purchases and sales from all broker-dealers may result in counting a transaction more than once across the market, and would sum to total volume across broker-dealers that exceeds what is reported pursuant to the relevant plans or SRO. Similarly, summing the percentages that result from dividing the total activity of each broker-dealer by the total volume reported by the relevant plans or SRO would result in a value greater than 100 percent.[218] Accordingly, the proposed ten percent (10%) transaction activity thresholds for measuring a broker-dealer's significance in the markets are not market share thresholds analogous to the current SCI ATS volume thresholds. However, because the types of transactions proposed to be counted are a measure of a broker-dealer's size and significance, it is particularly useful if that measure continues to reflect significant activity as the size of the overall market expands or contracts and

---

217 *See* Federal Reserve Board, Agency Information Collection Activities: Announcement of Board Approval Under Delegated Authority and Submission to OMB (Oct. 21, 2021) 86 FR 59716 (Oct. 28, 2021).

218 Transaction reporting systems generally report volume for trades, rather than volume for purchase and sales separately. Consequently, adding up the total purchase and sale activity for all broker-dealers will not equal the total volume reported through these systems. For example, a trade for 100 shares of an NMS stock between two broker-dealers on a national securities exchange would be reported by the effective transaction reporting plan as 100 shares, even though one broker-dealer bought 100 shares and another sold 100 shares. Similarly, because broker-dealers often trade with customers, doubling the transaction volume reported through these systems does not provide an accurate measure of total broker-dealer purchase and sale activity. After the implementation of the Market Data Infrastructure rules (*see* Market Data Infrastructure Adopting Release, *supra* note 24) national securities exchanges on which NMS stocks are traded and FINRA, each of which is required by Rule 601 of Regulation NMS to file a transaction reporting plan in accordance with Rule 608 of Regulation NMS, will be further required, pursuant to Rule 603(b) of Regulation NMS, to make available to all competing consolidators and self-aggregators its information with respect to quotations for and transactions in NMS stocks, including all data necessary to generate consolidated market data. Following implementation of the Market Data Infrastructure rules, a broker-dealer may determine average daily dollar volume from information provided by its chosen competing consolidator, or independently calculate that figure itself, as a "self-aggregator."

remains stable relative to a recognizable measure so that it does not become outdated over time. Therefore, the Commission proposes as a denominator a measure that would scale each broker-dealer's average daily dollar transaction volume to consolidated average daily dollar transaction volume, the latter being determinable from information reported by, or made available by or pursuant to, applicable effective transaction reporting or national market system plans or self-regulatory organizations, as described above.

Any broker-dealer that transacts, as proposed, ten percent (10%) or more of the average daily dollar volume in an enumerated asset class, during at least four of the preceding six calendar months would be an SCI broker-dealer. The proposed trading activity thresholds are designed to measure the size of a broker-dealer's footprint in the market in terms that provide a method for assessing the size of its footprint as the market grows (or shrinks). In this way, the proposed thresholds identify broker-dealers by their transaction activity as compared to a consistent measure of market volume, and give a sense of the size and significance of a broker-dealer activity in the markets in a manner that should not become outdated over time.

The Commission also believes that a threshold of ten percent (10%) or more in the identified asset classes is appropriately high enough to apply Regulation SCI only to the large broker-dealers on which the maintenance of fair and orderly markets depend. The Commission estimates that 17 entities would satisfy one or more of the proposed transaction activity thresholds (the same five entities identified by the total assets threshold plus 12 additional entities).[219] In sum, the Commission believes that the

---

[219] *See supra* text accompanying notes 189-190.

proposed total assets threshold and transaction activity thresholds are appropriate measures for identifying broker-dealers that would pose a substantial risk to the maintenance of fair and orderly markets in the event of a systems issue.

SCI broker-dealers would not have to comply with the requirements of Regulation SCI until six months after the end of the quarter in which the SCI broker-dealer satisfied the proposed asset threshold for the first time, or six months after the end of the month in which the SCI broker-dealer satisfied one of the proposed activity thresholds for the first time. The Commission believes this is an appropriate amount of time for firms to come into compliance with Regulation SCI.

#### iv. Proposed Revision to Definition of "SCI Systems" for Certain SCI Broker-Dealers; SCI Entities Trading Multiple Asset Classes, Which May Include Crypto Asset Securities

In conjunction with the proposed inclusion of SCI broker-dealers as SCI entities, the Commission proposes to limit the definition of "SCI systems" for an SCI broker-dealer that qualifies as an SCI entity only because it satisfies a transaction activity threshold. Specifically, the Commission is proposing to revise the definition of "SCI systems" to add a limitation that states, "*provided, however,* that with respect to an SCI broker-dealer that satisfies only the requirements of paragraph (2) of the definition of 'SCI broker-dealer,' such systems shall include only those systems with respect to the type of securities for which an SCI broker-dealer satisfies the requirements of paragraph (2) of the definition."

The current definition of "SCI systems" does not contain the limitation that is proposed for SCI broker-dealers. For example, an SCI ATS that exceeds the average daily dollar volume threshold for NMS stocks is subject to Regulation SCI requirements

for all of its SCI systems (*i.e.*, that meet the definition of SCI systems discussed in section II.B.1 above) and indirect SCI systems. Thus, to the extent that the SCI systems and indirect SCI systems of an SCI ATS (or any other SCI entity) relate to equity securities that are non-NMS stocks, exchange-listed options, debt securities, security-based swaps, or any other securities, including crypto asset securities, such systems are subject to the Regulation SCI requirements.[220]

As it considers the expansion of Regulation SCI to broker-dealers, many of which operate multiple business lines and transact in different types of securities, the Commission preliminarily believes that an SCI broker-dealer that qualifies as an SCI entity based only on a transaction activity threshold for a particular type of security should have its obligations limited to systems with respect to that type of security. If a broker-dealer meets only the transaction activity threshold for NMS stocks, for example, its systems that directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance for NMS stocks are those that raise the concerns Regulation SCI is meant to address. If the broker-dealer's activity with respect to other classes of securities is nominal, it is unlikely to pose risk to the maintenance of fair and orderly markets if the systems with respect to those types of securities were unavailable (assuming the systems for the distinct asset class are separate). If a system of the broker-dealer is used for more than one type of securities (*i.e.*, an asset class that triggered the threshold and an asset class that did not or is not subject to SCI thresholds),

---

220 *See supra* notes 37-38 and 36 and accompanying text (discussing the scope of the current definition of "SCI systems").

such system would still meet the definition of "SCI system."[221] Current SCI entities are and will continue to be, and proposed SCI entities other than SCI broker-dealers that satisfy a transaction activity threshold would be, required to assess whether the technology systems of, or operated by or on their behalf, with respect to any type of security (including crypto asset securities, discussed further below) are SCI systems covered by Regulation SCI because they directly support: (i) trading; (ii) clearance and settlement; (iii) order routing; (iv) market data; (v) market regulation; or (vi) market surveillance.

### v. Crypto Asset Securities

Public information about the size and characteristics of the crypto asset securities market is limited.[222] However, the Commission, currently understands that only a small

---

221 For example, if a broker-dealer operator of an SCI ATS uses an SCI system to trade both a type of security that triggered the SCI threshold and a type of security that did not trigger the threshold, that system will be an SCI system for both types of securities. A broker-dealer operator of such SCI ATS could wish to use the SCI system only for trading the type of security that triggered the SCI threshold and create a separate system only to trade the type of security that did not trigger the SCI threshold.

222 *See*, *e.g.*, Fin. Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation* 119 (2022) ("FSOC Report"), *available at* https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf ("The crypto-asset ecosystem is characterized by opacity that creates challenges for the assessment of financial stability risks."); U.S. Dep't of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* 12 (Sept. 2022) ("Crypto-Assets Treasury Report"), *available at* https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf (finding that data pertaining to "off-chain activity" is limited and subject to voluntary disclosure by trading platforms and protocols, with protocols either not complying with or not subject to obligations "to report accurate trade information periodically to regulators or to ensure the quality, consistency, and reliability of their public trade data"); Fin. Stability Bd., *Assessment of Risks to Financial Stability from Crypto-assets* 18-19 (Feb. 16, 2022) ("FSB Report"), *available at* https://www.fsb.org/wp-content/uploads/P160222.pdf (finding that the difficulty in aggregating and analyzing available data in the crypto asset space "limits the amount of insight that can be gained with regard to the [crypto asset] market structure and functioning," including who the market participants are and

portion of crypto asset security trading activity is occurring within Commission registered entities, and particularly, registered broker-dealers. This may be due in part to the fact that there are currently no special purpose broker-dealers authorized to maintain custody of crypto asset securities.[223] Without the ability to custody a customer's crypto-asset securities, a broker-dealer is limited in the amount of agency business in crypto-asset securities that it could do. Similarly, today, only a limited amount of crypto asset security volume occurs on ATSs operating pursuant to the Regulation ATS exemption.[224]

---

where the market's holdings are concentrated, which, among other things, limits regulators' ability to inform policy and supervision); Raphael Auer et al., *Banking in the Shadow of Bitcoin? The Institutional Adoption of Cryptocurrencies* 4, 9 (Bank for Int'l Settlements, Working Paper No. 1013, May 2022), *available at* https://www.bis.org/publ/work1013.pdf (stating that data gaps, which can be caused by limited disclosure requirements, risk undermining the ability for holistic oversight and regulation of cryptocurrencies); Int'l Monetary Fund, *The Crypto Ecosystem and Financial Stability Challenges, in Global Financial Stability Report* 41, 47 (Oct. 2021), *available at* https://www.imf.org/-/media/Files/Publications/GFSR/2021/October/English/ch2.ashx (finding that crypto asset service providers provide limited, fragmented, and, in some cases, unreliable data, as the information is provided voluntarily without standardization and, in some cases, with an incentive to manipulate the data provided).

223 For background on Rule 15c3-3 as it relates to digital asset securities, *see* Commission, *Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities* (July 8, 2019), *available at* https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities; FINRA, SEC Staff No-Action Letter, *ATS Role in the Settlement of Digital Asset Security Trades* (Sept. 25, 2020), *available at* https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf. To date, five offerings of crypto asset securities have been registered or qualified under the Securities Act of 1933, and five classes of crypto asset securities have been registered under the Exchange Act. The Commission issued a statement describing its position that, for a period of five years, special purpose broker-dealers operating under the circumstances set forth in the statement will not be subject to a Commission enforcement action on the basis that the broker-dealer deems itself to have obtained and maintained physical possession or control of customer fully paid and excess margin digital asset securities for purposes of 17 CFR 240.15c3-3(b)(1) ("Rule 15c3-3(b)(1)" under the Exchange Act). *See* Crypto Asset Securities Custody Release, *supra* note 37. To date, no such special purpose broker-dealer registration applications have been granted by FINRA.

224 ATSs that do not trade NMS stocks file with the Commission a Form ATS notice, which the Commission does not approve. Form ATS requires, among other things, that ATSs provide information about: classes of subscribers and differences in access to the services offered by the ATS to different groups or classes of subscribers; securities the ATS expects to trade; any entity

This may be due in part to the significant trading activity in crypto asset securities that may be in non-compliance with the federal securities laws.[225] Nonetheless, if an SCI entity (current or proposed) trades crypto asset securities, the systems used for trading crypto asset securities may currently and in the future be subject to the requirements of Regulation SCI.[226]

*SCI Broker-Dealer Activity in Crypto Asset Securities*

---

other than the ATS involved in its operations; the manner in which the system operates; how subscribers access the trading system; procedures governing entry of trading interest and execution; and trade reporting, clearance, and settlement of trades on the ATS. In addition, all ATSs must file quarterly reports on Form ATS-R with the Commission. Form ATS-R requires, among other things, volume information for specified categories of securities, a list of all securities traded in the ATS during the quarter, and a list of all subscribers that were participants. To the extent that an ATS trades crypto asset securities, the ATS must disclose information regarding its crypto asset securities activities as required by Form ATS and Form ATS-R. Form ATS and Form ATS-R are deemed confidential when filed with the Commission. Based on information provided on these forms, a limited number of ATSs have noticed on Form ATS their intention to trade certain crypto asset securities and a subset of those ATSs have reported transactions in crypto asset securities on their Form ATS-R. *See also supra* note 223, referencing, Commission, *Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities* (July 8, 2019), *available at* https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities; FINRA, SEC Staff No-Action Letter, *ATS Role in the Settlement of Digital Asset Security Trades* (Sept. 25, 2020), *available at* https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf.

225 *See also* FSOC Report, *supra* note 222, at 5, 87, 94, 97 (emphasizing the importance of the existing financial regulatory structure while stating that certain digital asset platforms may be listing securities while not in compliance with exchange, broker-dealer, or other registration requirements, which may impose additional risk on banks and investors and result in "serious consumer and investor protection issues"); Crypto-Assets Treasury Report, *supra* note 222, at 26, 29, 39, 40 (stating that issuers and platforms in the digital asset ecosystem may be acting in non-compliance with statutes and regulations governing traditional capital markets, with market participants that actively dispute the application of existing laws and regulations, creating risks to investors from non-compliance with, in particular, extensive disclosure requirements and market conduct standards); FSB Report, *supra* note 222, at 4, 8, 18 (stating that some trading activity in crypto assets may be failing to comply with applicable laws and regulations, while failing to provide basic investor protections due to their operation outside of or in non-compliance with regulatory frameworks, thereby failing to provide the "market integrity, investor protection or transparency seen in appropriately regulated and supervised financial markets").

226 *But see supra* section II.B.1 (discussing how current SCI entities that trade crypto asset securities must assess whether their systems for trading crypto asset securities are SCI systems). As a specific example, if an SCI SRO were to obtain Commission approval to add a crypto asset security trading facility, that facility would be part of an SCI SRO that is subject to Regulation SCI.

As discussed above, the Commission is proposing to include as SCI entities large broker-dealers: those that satisfy a total assets threshold or a transaction activity threshold. The total assets threshold applies to broker-dealers irrespective of asset classes in which they conduct significant transaction activity. In contrast, the proposed transaction activity threshold specifies four enumerated asset classes: NMS stocks, exchange-listed options, U.S. Treasury Securities, and Agency Securities.

The proposal would affect an SCI broker-dealer that engages in crypto asset security activity as follows: for purposes of assessing whether it meets a transaction activity threshold, a broker-dealer would need to consider if it trades crypto asset securities that are NMS stocks, exchange-listed options, U.S. Treasury Securities, or Agency securities, and if so, include those transactions in its transaction tally of NMS stocks, exchange-listed options, U.S. Treasury Securities, or Agency securities, to assess if it satisfies one or more of the proposed thresholds. In addition, as proposed, the SCI systems and indirect SCI systems pertaining to crypto asset securities that are NMS stocks, exchange-listed options, U.S. Treasury Securities, or Agency securities would be subject to Regulation SCI, including as it is proposed to be amended, as discussed in section III. C, with respect to the asset class for which the SCI broker-dealer satisfies the transaction activity threshold.

Furthermore, as proposed, an SCI broker-dealer that meets the proposed total assets threshold would need consider its crypto asset security activities and assess whether any systems pertaining to crypto asset securities meet the current definition of

SCI systems or indirect SCI systems. Any such systems would be subject to Regulation SCI, including as it is proposed to be amended, as discussed in section III.C.[227]

**vi. Request for Comment**

9. Should Regulation SCI apply to broker-dealers? If not, why not? If so, should Regulation SCI apply to all broker-dealers, or just a subset? Please explain. At what size or level of a broker-dealer's activity would market integrity or the protection of investors be affected if the broker-dealer were no longer able to operate due to a systems disruption, systems compliance issue, or a systems intrusion? Are broker-dealers subject to more market discipline than current SCI entities? Please explain. Conversely, does a lack of transparency regarding events like SCI events limit this market discipline? Why or why not?
10. Would it be more appropriate to define an SCI broker-dealer using an approach that identifies a broker-dealer by category, rather than by size? For example, what are commenters' views on the impact to overall market integrity or the protection of investors if an OTC market maker was no longer able to operate due to a systems disruption, systems compliance issue, or a systems intrusion? Or an exchange market maker? Or a clearing broker-dealer? What are commenters' views on the importance of different categories of broker-dealers to the stability of the overall U.S. securities

---

[227] Likewise, an ATS currently is an SCI ATS if it satisfies a trading volume threshold for NMS stocks or equity securities that are not NMS stocks. For purposes of assessing whether it meets an SCI ATS trading volume threshold, an ATS needs to consider if it trades crypto asset securities that are equity securities; and if it does trade such securities, those transactions need to be included in its transaction tally as (i) NMS stocks or (ii) equity securities that are not NMS stocks, as they case may be, in order to calculate the volume threshold. Additionally, the definition of SCI systems and indirect SCI systems do not contain an asset class limitation with respect to SCI SROs (or any other current SCI entity). *See supra* note 36 and accompanying text.

market infrastructure, in the context of requiring them to comply with Regulation SCI? What risks do the systems of broker-dealers pose to the U.S. securities markets?

11. If the Commission were to identify an SCI broker-dealer by category, rather than by size, which categories should be covered and how should they be defined? For example, if commenters believe that Regulation SCI should apply to significant "OTC market makers," how should they be defined? Is it sufficiently clear which entities are "OTC market makers," as that term is defined under the Exchange Act? If not, why not? If so, should a threshold be used to identify those that are the most significant? What should that threshold be and how should it be calculated?
12. Is the current broker-dealer regulatory regime, including the Market Access Rule and other Commission and FINRA rules, sufficient to reasonably ensure the operational capability of the technological systems of the proposed SCI broker-dealers?
13. As discussed above, an SCI broker-dealer would be a broker-dealer registered with the Commission pursuant to section 15(b) of the Exchange Act, which: (1) in at least two of the four preceding calendar quarters, ending March 31, June 30, September 30, and December 31, reported to the Commission on Form X-17A-5 total assets in an amount that equals five percent (5%) or more of the quarterly total assets level of all security brokers and dealers; or (2) during at least four of the preceding six calendar months: (i) with respect to transactions in NMS stocks, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the average daily dollar volume reported by or pursuant to applicable effective transaction reporting plans, provided, however, that for purposes of calculating its activity in transactions effected otherwise than on a national securities exchange or on an ATS,

the broker-dealer shall exclude transactions for which it was not the executing party; (ii) with respect to transactions in exchange-listed options contracts, transacted average daily dollar volume reported by an applicable effective national market system plan; (iii) with respect to transactions in U.S. Treasury Securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume made available by the self-regulatory organization to which such transactions are reported; or (iv) with respect to transactions in Agency Securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume made available by the self-regulatory organization to which such transactions are reported. The Commission solicits comment with respect to all aspects of the proposed definition, including those aspects identified in the succeeding questions.

14. Is the proposed total assets threshold an appropriate way to identify broker-dealers that would pose a substantial risk to the maintenance of fair and orderly markets in the event of a systems issue?

15. Should the proposed total assets threshold be scaled using the proposed sources as the denominator? Why or why not? Is use of data made available by the Federal Reserve Board appropriate as the denominator for the measure of all security broker-dealer total assets? If not, what metric, if any, would be appropriate for the Commission to use as the denominator? Should the denominator be different in the event that such data is no longer made available by the Federal Reserve Board? Recognizing that the proposed numeric thresholds ultimately represent a matter of judgment by the Commission as it proposes to apply Regulation SCI to the largest broker-dealers, the

Commission solicits comment on the proposed thresholds levels. Is the proposed five percent numeric threshold appropriate? Why or why not? Is the proposed two of the preceding four quarter methodology, with lookback to the previous quarter for the denominator appropriate? Why or why not?

16. Are the proposed transaction activity thresholds an appropriate way to identify broker-dealers that would pose a substantial risk to the maintenance of fair and orderly markets in the event of a systems issue?
17. With respect to the proposed transaction activity thresholds, are the asset classes identified appropriate? Are there asset classes that are included that should be excluded, or asset classes that are excluded that should be included? Which ones and why? For example, should U.S. Treasury Securities and Agency Securities be included? Why or why not? Should OTC equity securities be included? Or security-based swaps? Is the size of the market in each asset class relevant? Why or why not?
18. With respect to the proposed transaction activity thresholds, recognizing that the proposed numeric thresholds ultimately represent a matter of judgment by the Commission as it proposes to apply Regulation SCI to the largest broker-dealers, the Commission solicits comment on the proposed threshold levels. Are the 10 percent transaction activity threshold levels proposed appropriate? Would higher or lower thresholds be appropriate? Should thresholds vary based on asset class? Is there a different approach that would be more appropriate?
19. For purposes of the numerator in each transaction activity threshold, is use of average daily dollar volume of all purchase and sale transactions, as proposed appropriate? If not, why not? Is there an alternative measure of market activity that could be

consistently determined by broker-dealers, as well as the Commission, and that would identify large broker-dealer activity that, if disrupted, could disrupt market functioning more broadly? Would share volume be more appropriate for any of the proposed asset classes?

20. Is it clear what average daily dollar volume, as made available by or pursuant to applicable effective transaction reporting plans, would be following implementation of the Market Data Infrastructure rules? Why or why not?
21. Should the transaction activity thresholds denominator have a minimum, so that if the market for a particular product shrinks significantly, entities that have a significant portion of that small market would not be scoped into the test? For example, should an options trading activity threshold specify that the threshold is exceeded if average daily dollar volume equals the greater of ten percent (10%) or more of the average daily dollar volume reported by or pursuant to an applicable effective transaction reporting plan, applicable national market system plan, applicable SRO, or $x billion? Why or why not? What would be an appropriate minimum dollar threshold and why? Please be specific.
22. Is the four out of the preceding six-month measurement period an appropriate timeframe for the transaction activity thresholds? Why or why not? Is there a different timeframe or approach that would be more appropriate? Please explain.
23. Do commenters believe that six months after the end of the quarter in which the broker-dealer satisfies the total assets threshold and six months after the end of the month in which the broker-dealer satisfies the transaction activity threshold constitute an appropriate amount of time to allow them to come into compliance with the

requirements of Regulation SCI? Why or why not? Is there a different time period that would be more appropriate? Please explain.

24. What are the differences between the current practices of broker-dealers and the practices that would be necessary if the proposed changes to Regulation SCI are adopted? Please describe and be specific.
25. Should all of the current or newly proposed requirements set forth in Regulation SCI apply to SCI broker-dealers? If only a portion, please specify which portion(s) and explain why. If all, explain why.
26. Is it appropriate to limit the application of the definition of "SCI systems" for SCI broker-dealers that meet the definition of an SCI broker-dealer only because of a transaction activity threshold only to those systems related to the types of securities for which the entity has triggered the threshold, as the Commission is proposing? Why or why not?
27. Should the definition of SCI systems as it applies to SCI broker-dealers be modified further than as proposed? Is the limitation of the definition of SCI systems as proposed to apply to SCI broker-dealers (and not applicable to broker-dealers that satisfy the total assets threshold) appropriate? Should the Commission instead provide a unique definition of SCI systems and indirect SCI systems for broker-dealers? If so, what should it be and why? For example, in the context of broker-dealers, would systems that "directly support trading" be a category of systems that is overbroad, or too narrow? Why or why not? Please explain. Are there any types of systems of broker-dealers to which Regulation SCI would apply that should not be covered? Which ones and why? Are there any types of systems of broker-dealers that would

not be covered by the definitions of SCI systems and indirect SCI systems as proposed that should be covered? Which types and why? Please be specific.

28. Is it clear how Regulation SCI would apply to proposed new SCI entities that trade crypto asset securities? Why or why not? Please be specific.
29. Are any of the proposed amendments to Regulation SCI (as discussed in section III.C below) inappropriate for broker-dealers? If so, which ones? As discussed in section III.C.6 below, the Commission proposes to add language to Rule 1002(c) of Regulation SCI regarding dissemination of information about SCI events by an SCI broker-dealer to its "customers," as a broker-dealer does not have "members and participants." Should the Commission require an SCI broker-dealer to notify its customers of an SCI event in the same manner as other SCI entities? Why or why not? Should the term "customers" be defined? If so, how? Should Rule 1002(c) be specifically tailored to SCI broker-dealers in a way that differs from the current rule? If so, how? Please be specific. Is the proposed requirement that, pursuant to Rule 1002(b)(4)(ii)(B), notices to the Commission include a copy of the information disseminated to customers appropriate? Why or why not?
30. Do commenters believe that different or unique requirements should apply to an SCI broker-dealer or systems of broker-dealers? What should they be, and why?
31. What effect, if any, would there be of having the largest broker-dealers subject to Regulation SCI, while others are not? Should the Commission include additional broker-dealers as SCI entities, based on size or function? Why or why not? For example, should the largest carrying broker-dealers, based on a size threshold, be subject to Regulation SCI? If so, should the size threshold be based on total assets or

number of customer accounts, or some other metric? If application of all of Regulation SCI is not appropriate for these entities, should they be required to adopt and implement reasonably designed policies and procedures to address their ability to continue to process customer and account transactions in a timely manner during reasonably anticipated surges in demand?

32. Should the proposed thresholds take into account whether a broker-dealer is affiliated with another broker-dealer? For example, should the Commission aggregate the transaction activity of affiliated broker-dealers for purposes of determining whether the transaction activity threshold test has been satisfied and, if it has, apply Regulation SCI to each broker-dealer? Why or why not? Should it aggregate total assets of affiliated broker-dealers? Why or why not?
33. Is the proposed six-month period during which a broker-dealer that meets the threshold to become an SCI broker-dealer does not have to comply with Regulation SCI appropriate? Should the Commission adopt a different time period? If so, how long should the period be and why?
34. Are there characteristics specific to SCI broker-dealers that would make applying Regulation SCI, either broadly or by specific existing/proposed provision(s), unduly burdensome or inappropriate for SCI broker-dealers? How much time would an SCI broker-dealer reasonably need to come into compliance with Regulation as proposed?

#### c. Exempt Clearing Agencies (deletion of "subject to ARP")

The Commission proposes to include all "exempt clearing agencies" as SCI entities. This proposed approach would expand the scope of exempt clearing agencies covered by Regulation SCI, which currently covers certain exempt clearing agencies—

those that are "subject to ARP."[228] The technology systems that underpin operations of both registered clearing agencies and exempt clearing agencies are critical systems that drive the global financial markets. Further, the activities of exempt clearing agencies subject to ARP and those not subject to ARP are similar. For example, for covered clearing agencies in particular,[229] such systems include those that set and calculate margin obligations and other charges, perform netting and calculate payment obligations, facilitate the movement of funds and securities, or effectuate end-of-day settlement. Increasingly, the technology behind these systems are subject to both rapid innovation

---

228 *See* Rule 1000; SCI Adopting Release, *supra* note 1, at 72271 (an "exempt clearing agency subject to ARP" is an entity that has received from the Commission an exemption from registration as a clearing agency under section 17A of the Exchange Act, and whose exemption contains conditions that relate to the Commission's Automation Review Policies, or any Commission regulation that supersedes or replaces such policies (such as Regulation SCI)).

229 17 CFR 240.17Ad-22 ("Rule 17Ad-22" under the Exchange Act) provides for two categories of registered clearing agencies and contains a set of rules that apply to each category. The first category is covered clearing agencies, which are subject to 17 CFR 240.17Ad-22(e) (Rule 17Ad-22(e)), which includes requirements intended to address the activity and risks that their size, operation, and importance pose to the U.S. securities markets, the risks inherent in the products they clear, and the goals of both the Exchange Act and the Dodd-Frank Act. *See* Securities Exchange Act Release No. 78961 (Sept. 28, 2016), 81 FR 70786, 70793 (Oct. 13, 2016) ("CCA Standards Adopting Release"). Covered clearing agencies are registered clearing agencies that provide central counterparty ("CCP") or central securities depository ("CSD") services. *See* 17 CFR 240.17Ad-22(a)(5). A CCP is a type of registered clearing agency that acts as the buyer to every seller and the seller to every buyer, providing a trade guaranty with respect to transactions submitted for clearing by the CCP's participants. *See* 17 CFR 240.17Ad-22(a)(2); Securities Exchange Act Release No. 88616 (Apr. 9, 2020), 85 FR 28853, 28855 (May 14, 2020) ("CCA Definition Adopting Release"). A CCP may perform a variety of risk management functions to manage the market, credit, and liquidity risks associated with transactions submitted for clearing. If a CCP is unable to perform its risk management functions effectively, however, it can transmit risk throughout the financial system. A CSD is a type of registered clearing agency that acts as a depository for handling securities, whereby all securities of a particular class or series of any issuer deposited within the system are treated as fungible. Through use of a CSD, securities may be transferred, loaned, or pledged by bookkeeping entry without the physical delivery of certificates. A CSD also may permit or facilitate the settlement of securities transactions more generally. *See* 15 U.S.C. 78c(a)(23)(A); 17 CFR 240.17Ad-22(a)(3); CCA Definition Adopting Release, at 28856. If a CSD is unable to perform these functions, market participants may be unable to settle their transactions, transmitting risk through the financial system. Currently, all clearing agencies registered with the Commission that are actively providing clearance and settlement services are covered clearing agencies. They are The Depository Trust Company ("DTC"), FICC, NSCC, ICE Clear Credit ("ICC"), ICE Clear Europe ("ICEEU"), The Options Clearing Corporation ("OCC"), and LCH SA.

and interconnectedness.[230] For the exempt clearing agencies not subject to ARP, they also provide CSD functions for transactions in U.S. securities between U.S. and non-U.S. persons, using similar technologies.[231] More generally, all exempt clearing agencies offer services that centralize a variety of technology functions, increasing access to services that help improve the efficiency of the clearance and settlement process by, for example, standardizing and automating functions necessary to complete clearance and settlement.[232] Over time, the increasing availability of, and access to, such technologies has also increased the dependence that market participants have on such services, raising the potential that such services could become single points of failure for U.S. market participants.[233] Further, as the services that exempt clearing agencies provide have

---

230 The second category includes registered clearing agencies other than covered clearing agencies; such clearing agencies must comply with 17 CFR 240.17Ad-22(d) ("Rule 17Ad-22(d)"). *See* 17 CFR 240.17Ad-22(d). Rule 17Ad-22(d) establishes a regulatory regime to govern registered clearing agencies that do not provide CCP or CSD services. *See* CCA Standards Adopting Release, at 70793. Although subject to Rule 17Ad-22(d), the Boston Stock Exchange Clearing Corporation ("BSECC") and Stock Clearing Corporation of Philadelphia ("SCCP") are currently registered with the Commission as clearing agencies but conduct no clearance or settlement operations. *See* Securities Exchange Act Release No. 63629 (Jan. 3, 2011), 76 FR 1473, 1474 (Jan. 10, 2011) ("BSECC Notice"); Securities Exchange Act Release No. 63268 (Nov. 8, 2010), 75 FR 69730, 69731 (Nov. 15, 2010) ("SCCP Notice").

231 *See, e.g.*, Release No. 79577 (Dec. 16, 2016), 81 FR 93994 (Dec. 22, 2016) ("Euroclear Exemption"); Release No. 38328 (Feb. 24, 1997), 62 FR 9225 (Feb. 28, 1997) ("Clearstream Exemption"). To manage the potential risks associated with these functions, the Commission's exemptions impose volume limits on the amount of transactions in U.S. Government securities for which each entity may perform clearance and settlement.

232 *See, e.g.*, Euroclear Exemption, *supra* note 231 (adding services for collateral management); Release No. 44188 (Apr. 17, 2001), 66 FR 20494 (Apr. 23, 2001) (granting an exemption to provide a central matching service to Global Joint Venture Matching Services US LLC, now known as DTCC ITP Matching US LLC, to facilitate the settlement of transactions between broker-dealers and their institutional customers) ("ITPM Exemption").

233 *See* Securities Exchange Act Release No. 76514 (Nov. 25, 2015), 80 FR 75387, 75401 (Dec. 1, 2015) (granting an exemption to provide matching services to each of Bloomberg STP LLC and SS&C Technologies, Inc. and stating that "[o]n balance, the Commission believes that the

evolved over time, they have become increasingly reliant on the provision of new technologies to market participants, and so the Commission has increasingly focused its oversight of exempt clearing agencies on the ways that such services might introduce operational risk to U.S. market participants.[234] Therefore, the Commission proposes to expand the scope of SCI entities to cover all exempt clearing agencies. As a result, there would no longer be a difference in how exempt clearing agencies are addressed by Regulation SCI.

#### i. Current Regulatory Framework for Exempt Clearing Agencies

The registration and supervisory framework for clearing agencies under the Exchange Act provides the Commission with broad authority to provide exemptive relief from certain of the Commission's regulatory requirements under the Exchange Act. Specifically, section 17A(b)(1) of the Exchange Act provides the Commission with authority to exempt a clearing agency or any class of clearing agencies from any

---

redundancy created by more interfaces and linkages within the settlement infrastructure increases resiliency"); SEC Division of Trading and Markets and Office of Compliance Inspections and Examinations, *Staff Report on the Regulation of Clearing Agencies* (Oct. 1, 2020) ("Staff Report on Clearing Agencies"), *available at* https://www.sec.gov/files/regulation-clearing-agencies-100120.pdf (staff stating that "consolidation among providers of clearance and settlement services concentrates clearing activity in fewer providers and has increased the potential for providers to become single points of failure.").

234 For example, in 2016 the Commission approved modifications to the Euroclear Exemption that included, among other things, a new set of conditions for the reporting of service outages. *See* Euroclear Exemption, *supra* note 231, at 94003 (setting forth eight "Operational Risk Conditions Applicable to the Clearing Agency Activities").

provision of section 17A or the rules or regulations thereunder.[235] Such an exemption may be effected by rule or order, upon the Commission's own motion or upon application, either conditionally or unconditionally. The Commission's exercise of authority to grant exemptive relief must be consistent with the public interest, the protection of investors, and the purposes of section 17A, including the prompt and accurate clearance and settlement of securities transactions and the safeguarding of securities and funds.[236] The Commission has granted exemptions from clearing agency registration to three entities that provide matching services. These exempt clearing agencies are DTCC ITP Matching US, LCC (successor in name to Omgeo and Global Joint Venture Matching Services US, LLC), Bloomberg STP LLC ("BSTP"), and SS&C Technologies, Inc. ("SS&C").[237] In certain instances, non-U.S. clearing agencies also

---

235 The Commission has also provided temporary relief from registration to certain clearing agencies under section 36 of the Exchange Act. On July 1, 2011, the Commission published a conditional, temporary exemption from clearing agency registration for entities that perform certain post-trade processing services for security-based swap transactions. *See, e.g.*, Release No. 64796 (July 1, 2011), 76 FR 39963 (July 7, 2011) (providing an exemption from registration under section 17A(b) of the Exchange Act, and stating that "[t]he Commission is using its authority under section 36 of the Exchange Act to provide a conditional temporary exemption [from clearing agency registration], until the compliance date for the final rules relating to registration of clearing agencies that clear security-based swaps pursuant to sections 17A(i) and (j) of the Exchange Act, from the registration requirement in section 17A(b)(1) of the Exchange Act to any clearing agency that may be required to register with the Commission solely as a result of providing Collateral Management Services, Trade Matching Services, Tear Up and Compression Services, and/or substantially similar services for security-based swaps"). The order facilitated the Commission's identification of entities that operate in that area and that accordingly may fall within the clearing agency definition. Recently, the Commission indicated that the 2011 Temporary Exemption may no longer be necessary. *See* Securities Exchange Act Release No. 94615 (Apr. 6, 2022), 87 FR 28872, 28934 (May 11, 2022) (stating that the "Commission preliminarily believes that, if it adopts a framework for the registration of [security-based swap execution facilities ("SBSEFs")], the 2011 Temporary Exemption would no longer be necessary because entities carrying out the functions of SBSEFs would be able to register with the Commission as such, thereby falling within the exemption from the definition of 'clearing agency' in existing [17 CFR 240.17Ad-24 (Rule 17Ad–24)]").

236 *See* 15 U.S.C. 78q-1(b)(1).

237 *See* exemption, *supra* note 233 (granting an exemption to provide matching services to each of BSTP and SS&C).

have received exemptions from registration as a clearing agency. These exempt clearing agencies include Euroclear Bank SA/NV (successor in name to Morgan Guaranty Trust Company of NY)[238] and Clearstream Banking, S.A. (successor in name to Cedel Bank, société anonyme, Luxembourg).[239] Each has an exemption to provide clearance and settlement for U.S. Government and agency securities for U.S. participants, subject to limitations on the volume of transactions set forth in their exemptions. The Euroclear Exemption also provides an exemption from registration to provide collateral management services for transactions in U.S. equity securities between U.S. persons and non-U.S. persons.

As previously discussed, each of these exempt clearing agencies makes available to market participants an increasingly wide array of technology services that help centralize and automate the clearance and settlement of securities transactions for market participants. This increasing reliance on new technologies has focused the Commission's attention on the potential for such services to introduce operational risk or introduce single points of failure into the national system for clearance and settlement. Given this important role of exempt clearing agencies in helping to ensure the functioning, resilience, and stability of U.S. securities markets, and their growing technological innovations and interconnectedness, the Commission proposes to expand the scope of "SCI entity" to cover all exempt clearing agencies, rather than only those "subject to ARP" to help ensure that the risks associated with the greater dispersal, sophistication,

---

238 *See* Euroclear Exemption, *supra* note 231.

239 *See* Clearstream Exemption, *supra* note 231.

and interconnection of such technologies are appropriately mitigated.[240] In this regard, pursuant to the terms and conditions of the clearing agency exemptive orders, the Commission may modify by order the terms, scope, or conditions if the Commission determines that such modification is necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of the Exchange Act.[241]

**ii. Request for Comment**

35. Is expanding the scope of "SCI entity" to cover all exempt clearing agencies, not just those exempt clearing agencies subject to ARP, appropriate? Why or why not? Please be specific and provide examples, if possible, to illustrate your points.
36. Should all or some aspects of Regulation SCI apply to all exempt clearing agencies? Why or why not? If only a portion, please specify which portion(s) and explain why. If all, explain why.
37. Would the Regulation SCI proposed requirements, together with the conditions under which the exempt clearing agency is subject in the Commission exemptive order, be

---

240 *See supra* note 228. Pursuant to the Commission's statement on CCPs in the European Union ("EU") authorized under the European Markets Infrastructure Regulation ("EMIR"), an EU CCP may request an exemption from the Commission where it has determined that the application of SEC requirements would impose unnecessary, duplicative, or inconsistent requirements in light of EMIR requirements to which it is subject. *See Statement on Central Counterparties Authorized under the European Markets Infrastructure Regulation Seeking to Register as a Clearing Agency or to Request Exemptions from Certain Requirements Under the Securities Exchange Act of 1934*, Securities Exchange Act Release No. 90492 (Nov. 23, 2020), 85 FR 76635, 76639 (Nov. 30, 2020), *available at* https://www.govinfo.gov/content/pkg/FR-2020-11-30/pdf/FR-2020-11-30.pdf (stating that in seeking an exemption, an EU CCP could provide "a self-assessment. . . [to] explain how the EU CCP's compliance with EMIR corresponds to the requirements in the Exchange Act and applicable SEC rules thereunder, such as Rule 17Ad-22 and Regulation SCI").

241 *See* ITPM Exemption, *supra* note 231; Euroclear Exemption, *supra* note 231; Clearstream Exemption, *supra* note 231.

sufficient to address operational risk concerns posed by exempt clearing agencies? Why or why not? Please be specific and respond with examples, if possible.

38. Given the proposed new requirements of Regulation SCI, should exempt clearing agencies be subject to a revised Commission exemptive order? Why or why not?
39. In support of the public interest and the protection of investors, the Commission is proposing to amend the clearing agency exemptive orders to replace all operational risk conditions with a condition that each exempt clearing agency must comply with Regulation SCI requirements. Should the ordering language provide that the exempt clearing agency must comply with all requirements in Regulation SCI? If so, explain why. If not, explain why not.
40. Should proposed Regulation SCI distinguish among different types of exempt clearing agencies such that some requirements of Regulation SCI might be appropriate for some exempt clearing agencies, but not others? Why or why not? If so, what are those distinctions and what are those requirements? Please be specific and provide examples, if possible.
41. To what extent do exempt clearing agencies rely on third-party providers to provide systems that support their clearance and settlement functions? Do such third-party providers introduce operational or other risks that would be subject to the requirements of Regulation SCI? Are there any circumstances in which the use of a third-party provider would prevent compliance with Regulation SCI? Why or why not? Please be specific and provide examples, if possible.
42. For EU CCPs authorized under EMIR, the Commission stated that exemptive relief may be considered under section 17A(b)(1) of the Exchange Act in scenarios where

SEC requirements are unnecessary, duplicative, or inconsistent relative to EMIR requirements. The Commission recognizes that the EU and other jurisdictions may have requirements similar those being proposed in Regulation SCI. Should the Commission provide foreign CCPs with exemptive relief from newly proposed Regulation SCI? Why or why not? In the context of exemptive requests for newly proposed Regulation SCI, what factors should the Commission take into account in assessing whether SEC requirements may be "unnecessary, duplicative, or inconsistent" relative to home jurisdiction requirements for foreign CCPs, including EU CCPs authorized under EMIR? Please be specific and provide examples, if possible.

#### 3. General Request for Comment on Proposed Expansion of SCI Entities

43. The Commission requests comment generally on the proposed expansion of the definition of SCI entity. Are there are other entities that should be included as SCI entities? If so, which entities and why? Further, are there any entities, which if included as SCI entities, would have critical SCI systems? Please explain.

### B. Request for Comment Regarding Significant-Volume Fixed Income ATSs and Broker-Dealers Using Electronic or Automated Systems for Trading of Corporate Debt Securities or Municipal Securities

#### 1. Discussion

As stated above, the Commission did not include Fixed Income ATSs as SCI entities when it adopted Regulation SCI based on consideration of comments regarding the risk profile of these ATSs at that time.[242] In light of the evolution of technology since

---

[242] *See supra* text accompanying note 79.

then, and specifically, the technology for trading corporate debt and municipal securities, the Commission requests comment on whether significant-volume ATSs and/or broker-dealers with significant transaction activity in corporate debt or municipal securities should be subject to Regulation SCI.[243]

Currently, an ATS is subject to Rule 301(b)(6) of Regulation ATS if its trading volume reaches "20 percent or more of the average daily volume traded in the United States" in either corporate debt or municipal securities.[244] Among other things, Rule 301(b)(6) requires such a significant-volume Fixed Income ATS to notify the Commission staff of material systems outages and significant systems changes and to establish adequate contingency and disaster recovery plans.[245] The requirements of Rule

---

243 For purposes of this release, the term Fixed Income ATSs refers only to ATSs trading corporate debt and municipal securities and excludes Government Securities ATSs, which are the subject of a separate proposal. *See supra* notes 84-85 and accompanying text.

244 *See* 17 CFR 242.301(b)(6). Until Regulation SCI was adopted, Rule 301(b)(6) applied to an ATS trading NMS stocks, equity securities that are not NMS stocks, corporate debt securities, or municipal securities exceeding a 20% volume threshold. Since the adoption of Regulation SCI, Rule 301(b)(6) has applied only to ATSs trading corporate debt securities or municipal securities exceeding a 20% volume threshold. Rule 301(b)(6) currently does not specify whether the thresholds refer to share, dollar, or transaction volume. In the Government Securities ATS Reproposal, the Commission has proposed to specify that these thresholds refer to "average daily dollar volume." *See* Government Securities ATS Reproposal, *supra* note 84, at 15572.

245 More specifically, with regard to systems that support order entry, order routing, order execution, transaction reporting, and trade comparison, Rule 301(b)(6)(ii) of Regulation ATS requires significant-volume ATSs to: establish reasonable current and future capacity estimates; conduct periodic capacity stress tests of critical systems to determine their ability to accurately, timely and efficiently process transactions; develop and implement reasonable procedures to review and keep current system development and testing methodology; review system and data center vulnerability to threats; establish adequate contingency and disaster recovery plans; perform annual independent reviews of systems to ensure compliance with the above listed requirements and perform review by senior management of reports containing the recommendations and conclusions of the independent review; and promptly notify the Commission of material systems outages and significant systems changes. *See* 17 CFR 242.301(b)(6)(ii). As discussed in the SCI Adopting Release, the application of Rule 301(b)(6) to Fixed Income ATSs is in addition to various Exchange Act and FINRA rules applicable to broker-dealers operating ATSs. *See* SCI Adopting Release, *supra* note 1, at 72263. *See also supra* notes 146-166 and accompanying text (providing an updated discussion of various Exchange Act, FINRA, and certain other regulations applicable to broker-dealers, including those operating ATSs).

301(b)(6) applicable to significant-volume Fixed Income ATSs, which date to 1998 and have not been updated since that time, are less rigorous than the requirements of Regulation SCI.[246] The Commission explained in the SCI Adopting Release that it adopted Regulation SCI to expand upon, update, and modernize the requirements of Rule 301(b)(6) for those ATSs trading NMS stocks and equity securities that are not NMS stocks that it had identified as playing a significant role in the U.S. securities markets.[247] Regulation SCI did this by, for example, moving from the Commission's 1980s and 90s-era technology precepts to a framework that speaks to a broader set of systems that are subject to an overarching standard: that they be subject to policies and procedures reasonably designed to maintain operational capability and promote the maintenance of fair and orderly markets. Regulation SCI also requires tested business continuity and disaster recovery plans that include geographic diversity to achieve specified recovery time objectives. In addition, Regulation SCI requires notice and dissemination of information regarding a wider range of systems problems (*i.e.*, SCI events) to the Commission and affected market participants, and also requires that corrective action be taken with respect to such problems.[248]

When proposing Regulation SCI in 2013, the Commission sought to include as SCI entities those ATSs that are reliant on automated systems and represent a significant

---

246 *See* Securities Exchange Act Release No. 40760 (Dec. 8, 1998), 63 FR 70844, (Dec. 22, 1998) ("Regulation ATS Adopting Release").

247 *See* SCI Adopting Release, *supra* note 1, at 72264.

248 As discussed further below, the Commission is now proposing updates to Regulation SCI that are designed to take account of new and emerging technology challenges. If adopted, these changes to Regulation SCI will render Rule 301(b)(6) even more outdated by comparison. Below the Commission solicits comment on whether, in lieu of applying Regulation SCI to these entities, Rule 301(b)(6) should be updated instead.

pool of liquidity in certain asset classes.[249] Regarding Fixed Income ATSs, the Commission proposed to include those exceeding five percent or more of either average daily dollar volume or average daily transaction volume traded in the United States, but it did not adopt that proposal.[250] Instead, for ATSs trading corporate debt or municipal securities exceeding a 20 percent "average daily volume" threshold, it left in place the older, more limited technology regulations in Rule 301(b)(6) of Regulation ATS.[251] In support of that determination, the Commission distinguished the equity markets from the corporate debt and municipal securities markets, stating that the latter markets generally relied much less on automation and electronic trading than markets that trade NMS stocks or equity securities that are not NMS stocks, and also tended to be less liquid than the equity markets, with slower execution times and less complex routing strategies.[252]

Due to changes in the market and updates to technology, the Commission again requests comment on applying Regulation SCI to significant-volume Fixed Income ATSs, and further requests comment regarding broker-dealers trading significant volume

---

249 *See* SCI Proposing Release, *supra* note 14, at 18094-96.

250 *See* SCI Proposing Release, *supra* note 14, at 18093, 18095. At adoption, the Commission included only ATSs that trade NMS stocks and equity securities that are not NMS stocks exceeding a specified volume threshold. Rule 1000 of Regulation SCI defines SCI ATS to mean an ATS, which, during at least four of the preceding six calendar months, had: (1) With respect to NMS stocks: (i) 5% or more in any single NMS stock, and 0.25% or more in all NMS stocks, of the average daily dollar volume reported by an effective transaction reporting plan, or (ii) 1% or more, in all NMS stocks, of the average daily dollar volume reported by an effective transaction reporting plan; or (2) with respect to equity securities that are not NMS stocks and for which transactions are reported to an SRO, 5% or more of the average daily dollar volume as calculated by the SRO to which such transactions are reported. *See* 17 CFR 242.1000. Rule 1000 also states that an ATS that meets one of these thresholds is not required to comply with Regulation SCI until six months after satisfying the threshold for the first time. *See id.*

251 *See* SCI Adopting Release, *supra* note 1, at 72270.

252 *See id*. The Commission also acknowledged comments stating that lowering the 20% threshold in Rule 301(b)(6) could have the unintended effect of discouraging technology evolution in these markets. *Id.*

in corporate debt or municipal securities.[253] In particular, the Commission is soliciting comment on whether the distinctions drawn by the Commission in its original adoption of Regulation SCI, between equities markets on the one hand, and the corporate debt and municipal securities markets on the other, based on differences in their reliance on automation and electronic trading strategies have diminished such that Fixed Income ATSs or broker-dealers with significant activity in corporate debt and municipal securities should be subject to increased technology oversight pursuant to Regulation SCI.

As noted above, the Commission proposed and then recently re-proposed to extend Regulation SCI to ATSs that trade U.S. Treasury Securities or Agency Securities (*i.e.*, Government Securities ATSs) exceeding a five percent dollar volume threshold in at least four out of the preceding six months, citing the increased reliance on technology in the government securities markets in recent years and the resulting operational similarities and technological vulnerabilities and risks of such ATSs to existing SCI entities.[254] In the Government Securities ATS Reproposal, the Commission discussed ways in which the government securities markets have become increasingly dependent on electronic trading in recent years.[255] The Commission solicits comment on whether

---

253 *See* SCI Adopting Release, *supra* note 1, at 72409 (stating, "[A]s the Commission monitors the evolution of automation in this market, the Commission may reconsider the benefits and costs of extending the requirements of Regulation SCI to fixed-income ATSs in the future.").

254 *See* Government Securities ATS Proposing Release, *supra* note 84, at 87152-54. *See also* Government Securities ATS Reproposal, *supra* note 84, at 15527-29. Specifically, in the Government Securities ATS Reproposal, the Commission discussed how advances in technology have resulted in the increased use of systems that use protocols and non-firm trading interest to bring together buyers and sellers of securities and how these systems functioned as market places similar to market places provided by registered exchanges and ATSs. *See* Government Securities ATS Reproposal, *supra* note 84, at 15497-98.

255 *See* Government Securities ATS Reproposal, *supra* note 84, at 15526.

trading in corporate debt securities or municipal securities by ATSs and/or broker-dealers has evolved similarly.

The growth in electronic trading in the corporate debt and municipal securities markets in recent years appears to be substantial,[256] and accelerating.[257] Although traditional methods of bilateral corporate bond trading conducted through either dealer-to-dealer or dealer-to-customer negotiations (often using telephone calls) remain important (with an estimated 71.4 percent of trading in corporate bonds facilitated via

---

256 *See* Government Securities ATS Reproposal, *supra* note 84, at 15528 at n. 389, 15606, and 15609. *See also SIFMA Insights: Electronic Trading Market Structure Primer*, *supra* note 3 (outlining and comparing electronification trends in different markets); SIFMA, *SIFMA Insights: US Fixed Income Market Structure Primer* (July 2018), *available at* https://www.sifma.org/wp-content/uploads/2018/07/SIFMA-Insights-FIMS-Primer_FINAL.pdf (discussing several different types of fixed-income markets, noting that the historically quote-driven voice broker market structure has moved to accommodate limit order book protocols in the intradealer markets and request-for-quote ("RFQ") protocols in the dealer-to-client markets; and assessing that "Current growth [in the dealer-to-client markets] is enabling the total growth in overall electronification percentages: UST 70%, Agency 50%, Repos 50%, IG Corporates 40% and HY Corporates 25%").

257 *See* Annabel Smith, *Pandemic sees electronic fixed income trading skyrocket in 2021*, the Trade (Mar. 3, 2021), *available at* https://www.thetradenews.com/pandemic-sees-electronic-fixed-income-trading-skyrocket-in-2021/; Municipal Securities Rulemaking Board, *Characteristics of Municipal Securities Trading on Alternative Trading Systems and Broker's Broker Platforms* (Aug. 2021), *available at* https://msrb.org/MarketTopics/-/media/27E4F111D18246C6B9DA849082230CD0.ashx (discussing volume on ATSs and broker's broker platforms from 2016-2021).

bilateral voice trading during the first half of 2021),[258] more recent data suggest that dependencies on electronic protocols have increased in the last year alone.[259]

In the municipal securities markets, a majority (56.4%) of all inter-dealer trades and 26% of inter-dealer par value traded were executed on ATSs during the period from

---

258 *See* Government Securities ATS Reproposal, *supra* note 84, at 15606-07. Market observers also note increased use of electronic trading in the growth of all-to-all trading and portfolio trading. *See* Greenwich Associates, *All-to-All Trading Takes Hold in Corporate Bonds* (Q2 2021), *available at* https://content.marketaxess.com/sites/default/files/2021-04/All-to-All-Trading-Takes-Hold-in-Corporate-Bonds.pdf#:~:text=In%20all-%20to-all%20markets%2C%20where%20asset%20managers%20provide,of%20the%20corporate%20bond%20market%E2%80%99s%20growth%20and%20evolution (stating that all-to-all trading, which allows asset managers to provide liquidity to dealers and each other and for dealers to trade with one another electronically, has increased from 8% of investment grade volume in 2019 to 12% of investment grade volume in 2020); *see also Li Renn Tsai*, *Understanding Portfolio Trading*, Tradeweb (Sept. 6, 2022), *available at* https://www.tradeweb.com/newsroom/media-center/in-the-news/understanding-portfolio-trading/#:~:text=Portfolio%20Trading%20is%20a%20solution%20that%20gives%20asset,savings%2C%20mitigate%20operational%20risk%2C%20and%20reduce%20market%20slippage (discussing that portfolio trading, a process similar to program trading for equities which allows asset managers to buy/sell a basket of bonds to trade together as a single package, increased from 2% of total corporate bond trades in Jan. 2020 to 5% in Sept. 2021); Kate Marino, *Algorithms have arrived in the bond market*, Axios (Sept. 3, 2021), *available at* https://www.axios.com/2021/09/03/bond-market-trading-algorithms (discussing the increase in portfolio trading in the bond market).

259 *See Jack Pitcher*, *Record E-Trading Brings More Liquidity to Corporate Bond Market*, Bloomberg (Oct. 31, 2022), *available at* https://www.bloomberg.com/news/articles/2022-10-31/electronic-credit-trading-surges-to-record-boosting-liquidity (citing a Sept. 2022 Coalition Greenwich report stating that "Investment-grade electronic trading accounted for 42% of volume in September, up 9 percentage points from the same month last year, and high yield was 34%, up 10 percentage points" and about one third of trading volume on junk bonds was through online trading in Sept. 2022, up from about a quarter of trading volume in the same period last year); *but see* Maureen O'Hara and Xing Alex Zhou, *The electronic evolution of corporate bond dealers*, Journal of Financial Economics (Jan. 5, 2021), *available at* https://www.sciencedirect.com/science/article/pii/S0304405X21000015 (discussing that any eventual domination of electronic bond trading may *ultimately* be limited because of the particular nature of bond trading, which includes bond illiquidity, the inability for larger trades to be broken into smaller trade sizes that can trade electronically, dealer unwillingness to trade more information-sensitive high-yield bonds electronically, and the lack of new dealers in bond market structure).

August 2016 through April 2021."[260] Moreover, as recently reported by the MSRB, the number of transactions with a dealer on an ATS more than tripled from 2015 to 2021; the average daily number of municipal securities trades increased more than 550% from 2015 to 2022 and also increased more than 75% in 2022; and the average daily par amount traded increased more than 400% since 2015 and more than doubled in 2022 compared to 2021.[261]

While technological developments provide many benefits to the U.S. securities markets and investors, they also increase the risk of operational problems that have the potential to cause a widespread impact on the securities markets and market participants. The trend in electronic trading in these markets and recent data on the volume of Fixed Income ATSs suggest that there is likely to be one or more Fixed Income ATSs (or broker-dealers) that both rely on electronic trading technology and represent or generate significant sources of liquidity in these asset classes. In light of these developments, the Commission believes that it is appropriate to request comment on whether ATSs and broker-dealers that trade significant volume in corporate debt securities or municipal

---

260 *See* Simon Z. Wu, Characteristics of Municipal Securities Trading on Alternative Trading Systems and Broker's Broker Platforms, Municipal Securities Rulemaking Board (Aug. 2021), available at https://www.msrb.org/sites/default/files/MSRB-Trading-on-Alternative-Trading-Systems.pdf. *See also* Government Securities ATS Reproposal, *supra* note 84, at 15609 (discussing use of electronic trading protocols in the municipal securities markets, and noting that "one MSRB report found that technological advancements in this market and the movement away from voice trading and towards electronic trading have helped reduce transaction costs for dealer-customer trades by 51 percent between 2005 and 2018").

261 *See* John Bagley and Marcelo Vieira, *Customer Trading with Alternative Trading Systems*, Municipal Securities Rulemaking Board (Aug. 2022), *available at* https://www.msrb.org/sites/default/files/2022-08/MSRB-Customer-Trading-with-Alternative-Trading-Systems.pdf.

securities should also be subject to some or all of the requirements of Regulation SCI, and if so, what an appropriate threshold would be.[262]

### 2. Request for Comment

The Commission is requesting comment on whether to apply Regulation SCI to Fixed Income ATSs on the basis of volume, or to broker-dealers that trade corporate debt or municipal securities on or above a trading activity threshold. Specifically:

44. Should significant volume ATSs and/or broker-dealers with significant transaction activity in corporate debt or municipal securities be subject, in whole or in part, to Regulation SCI?[263]
45. Do commenters agree that the corporate debt and municipal securities markets have become increasingly electronic in recent years? Why or why not? Please provide data to support your views. If electronic trading in the corporate debt and municipal securities markets has increased, are these markets sufficiently different or unique to warrant an approach to technology oversight that differs from the approach taken in Regulation SCI? Why or why not?

---

262 An ATS that trades NMS stocks is subject to Regulation SCI if its trading volume reaches: (i) 5% or more in any single NMS stock and 0.25% or more in all NMS stocks of the average daily dollar volume reported by applicable transaction reporting plans; or (ii) 1% or more in all NMS stocks of the average daily dollar volume reported by applicable transaction reporting plans. An ATS that trades equity securities that are not NMS stocks is subject to Regulation SCI if its trading volume is 5% or more of the average daily dollar volume (across all equity securities that are not NMS stocks) as calculated by the SRO to which such transactions are reported. As stated in the SCI Adopting Release, the higher threshold for equity securities that are not NMS stocks versus NMS stocks was selected taking into account the lower degree of automation, electronic trading, and interconnectedness in the market for equity securities that are not NMS stocks and assessment that those ATSs would present lower risk to the market in the event of a systems issue, but not necessarily no risk. *See* SCI Adopting Release, *supra* note 1, at 72269. As stated above, a 5% average daily dollar volume threshold is proposed for Government Securities ATSs (*i.e.*, ATSs that that trade Agency Securities and/or U.S. Treasury Securities), where electronic trading is prevalent.

263 The Commission notes that ATSs may also trade crypto asset securities. *See* section II.A.3.b.v. (discussing obligations of ATSs trading crypto asset securities).

46. What are the risks associated with systems issues at Fixed Income ATSs or broker-dealers that trade corporate debt or municipal securities today? What impact would a systems issue at a Fixed Income ATS or such broker-dealer have on the trading of corporate debt or municipal securities and the maintenance of fair and orderly markets?
47. Do electronic systems used to trade corporate debt or municipal securities markets today have linkages to any trading venues, including to U.S. Treasury markets? Are these linkages developing or likely to develop? If not, are there interconnections with third-party or other types of systems? How do any interconnections impact the risk of an SCI event at a Fixed Income ATS or broker-dealer that trades corporate debt or municipal securities on the market and/or market participants?
48. If commenters believe that Regulation SCI should apply, in whole or in part, to Fixed Income ATSs or broker-dealers that trade corporate debt or municipal securities, should there be a volume threshold? For example, should the definition of SCI ATS include those ATSs which, during at least four of the preceding six calendar months had: (1) with respect to municipal securities, five percent or more of the average daily dollar volume traded in the United States, as provided by the self-regulatory organization to which such transactions are reported; or (2) with respect to corporate debt securities, five percent or more of the average daily dollar volume traded in the United States as provided by the self-regulatory organization to which such transactions are reported? Similarly, should the definition of SCI-broker-dealer include a similar threshold to that proposed for registered broker-dealers trading Treasury or Agency securities (during at least four of the preceding six calendar

months reported to the self-regulatory organization(s) to which such transactions are reported, average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume as made available by the self-regulatory organization to which such transactions are reported)?

49. Is basing a threshold on a percentage of average daily dollar volume appropriate? Should there be an alternative threshold based on average daily share volume? Or par value? Or transaction volume?

50. Would commenters have a different view on what an appropriate threshold would be for Fixed Income ATSs if additional entities become Fixed Income ATSs as a result of adoption of the amendments to Rule 3b-16(a) that the Commission has proposed in the Government Securities ATS Reproposal?

51. If the Commission proposes to apply Regulation SCI to Fixed Income ATSs, should it propose a similar approach for broker-dealers that trade corporate debt or municipal securities? Why or why not?

52. Would four out of the preceding six months be an appropriate period to measure the volume thresholds for corporate debt and municipal securities for purposes of Regulation SCI? Why or why not? Would Fixed Income ATSs or broker-dealers that trade corporate debt or municipal securities have available appropriate data with which to determine whether a proposed threshold has been met? If not, what data or information is missing? Does the answer depend on whether the Government Securities ATS Reproposal (proposing to expand the definition of exchange in Rule 3b-16(a)) is adopted as proposed?

53. Should any or all Fixed Income ATSs that meet a volume threshold be subject to Rule 301(b)(6) of Regulation ATS instead of Regulation SCI (*i.e.*, should Rule 301(b)(6) be retained)? Why or why not? Alternatively, should any or all Fixed Income ATSs or broker-dealers that trade corporate debt or municipal securities be subject to only certain provisions of Regulation SCI? Which ones and why? Please explain. Alternatively, should Rule 301(b)(6) of Regulation ATS be updated to be more similar to Regulation SCI in certain respects? If so, how?

54. If commenters believe Rule 301(b)(6) should continue to apply to Fixed Income ATSs, is the 20 percent average daily volume threshold an appropriate threshold? Should it be amended to specify what the 20 percent average daily volume refers to (*e.g.*, share? dollar? par? transaction?)? Should the Commission amend Rule 301(b)(6) to subject all Fixed Income ATSs, or certain Fixed Income ATSs, to the requirements of the rule if the Fixed Income ATS reaches a 5 percent, 10 percent, 15 percent or another volume threshold? If so, please explain why such a threshold would be appropriate. Alternatively, should Rule 301(b)(6) be superseded and replaced by Regulation SCI?

55. Are there characteristics specific to the corporate debt and municipal securities markets that would make applying Regulation SCI broadly or any specific provision of Regulation SCI to Fixed Income ATSs or broker-dealers that trade corporate debt or municipal securities unduly burdensome or inappropriate? Please explain. For example, if an ATS that fits the description of a Communication Protocol System (as described in the Government Securities ATS Proposal) were to be become an SCI ATS, would there be certain features or functions of that system that would not meet

the definition of SCI systems, but that should be subject to Regulation SCI as SCI systems? Would there be any features or functions of that system that would meet the definition of SCI systems, but that should not be subject to Regulation SCI? Commenters that recommend that the Commission propose that ATSs and/or broker-dealers with significant transaction activity in corporate debt or municipal securities be subject to Regulation SCI are requested to specifically address the expected benefits and costs of their recommendations, above the current baseline of Rule 301(b)(6) of Regulation ATS, and the expected effects of their recommendations on efficiency, competition, and capital formation.

### C. Strengthening Obligations of SCI Entities

In adopting Regulation SCI, the Commission recognized that technology, standards, and threats would continue to evolve and that the regulation would need to be flexible so as to develop alongside such changes. Thus, 17 CFR 242.1001(a)(1) ("Rule 1001(a)(1)" of Regulation SCI) requires that each SCI entity have "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."[264] While Rule 1001(a)(2) itemizes certain minimum requirements such policies and procedures must include, they are generally broad areas that must be covered (*e.g.*, requiring capacity planning estimates, stress tests, systems development and testing programs, reviews and testing for threats, business continuity and disaster recovery plans, standards with respect to market data,

---

[264] *See* 17 CFR 242.1001(a)(1).

and monitoring for potential SCI events), Rule 1001(a) does not prescribe in detail how they should be addressed.[265]

Since the adoption and implementation of Regulation SCI, technology and the ways SCI entities employ such technology have continued to evolve, as have the potential vulnerabilities of, and threats posed to, SCI entities. In addition, the Commission and its staff have gained valuable experience and insights with respect to technology issues surrounding SCI entities and their systems. Given the important role SCI entities play in our markets, it is appropriate to strengthen the requirements Regulation SCI imposes on SCI entities to help ensure that their SCI systems and indirect SCI systems continue to remain robust, resilient, and secure.

### 1. Systems Classification and Lifecycle Management

#### a. Discussion

The terms "SCI systems," "indirect SCI systems," and "critical SCI systems" are foundational definitions within Regulation SCI. These terms map out the scope of Regulation SCI's applicability to an SCI entity. If an SCI entity does not classify its systems pursuant to these defined terms, it cannot fully understand how it should apply Regulation SCI's requirements and where its obligations under the regulation start and end. Specifically, "SCI systems" is defined to mean "all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance." The definition of "SCI systems" does not scope in every system of an SCI entity; rather, it is limited to those

---

[265] *Id*.

functions the Commission believed were of particular significance for the purposes of Regulation SCI, namely systems that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance. "Indirect SCI systems" come into play with respect to security standards and systems intrusions and include "any systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems." Importantly, both definitions include systems operated by an SCI entity as well as systems operated by third parties on behalf of a given SCI entity.

Except as discussed above,[266] the proposed rule amendments would not change the definition of SCI systems, indirect SCI systems, or critical SCI systems. However, the Commission is proposing to modify certain existing, and add a number of additional, requirements to the policies and procedures required of SCI entities with respect to their SCI systems (and indirect SCI systems or critical SCI systems, as the case may be), under Rule 1001(a), as discussed in further detail below.

One of the first steps many SCI entities take to comply with Regulation SCI is developing a classification of their systems in accordance with these definitions; *i.e.*, a documented inventory of the specific systems of the SCI entity that fall within each type of systems (*i.e.*, SCI system, indirect SCI system, and critical SCI system). However, not all SCI entities maintain such a list. A foundational and essential step for an SCI entity to be able to meet its obligations under Regulation SCI is to be able to identify clearly the systems that are subject to obligations under Regulation SCI. Therefore, the Commission

---

266 *See supra* section III.A.2.b.iv (discussing the proposed limitation to the definition of SCI systems for certain SCI broker-dealers).

is proposing a new provision to ensure that SCI entities develop and maintain a written inventory of their systems and classification. Specifically, new paragraph (a)(2)(viii) in Rule 1001 would require each SCI entity to include in their policies and procedures the maintenance of a written inventory and classification of all of its SCI systems, critical SCI systems, and indirect SCI systems.

In addition, 17 CFR 242.1001(a)(2)(viii) ("proposed Rule 1001(a)(2)(viii)") would require that the SCI entity's policies and procedures include a program with respect to the lifecycle management of such systems, including the acquisition, integration, support, refresh, and disposal of such systems, as applicable. This provision would require SCI entities to consider how a system subject to Regulation SCI moves through its lifecycle, from initial acquisition to eventual disposal. The purpose of this provision is to help ensure that an SCI entity is able to identify risks an SCI system may face during its various lifecycle phases. Importantly, SCI entities would need to address the refresh of such systems in their lifecycle management program. Generally, systems that are properly refreshed and updated include up-to-date software and security patches. In addition, the lifecycle management program required in their policies and procedures must address disposal of such systems. Disposal generally should include sanitization of end-of-life systems to help ensure that systems that are no longer intended as SCI systems or indirect SCI systems do not contain sensitive information (*e.g.*, relating to the operations or security of the SCI entity or its systems architecture) that might be

unintentionally revealed if such end-of-life systems fall into the wrong hands.[267] Thus, this generally would require SCI entities to pinpoint precisely when a given system "becomes" an SCI system (or an indirect SCI system), as well as the point at which it is officially "no longer" an SCI system (or an indirect SCI system).

#### b. Request for Comment

56. Do commenters agree with the proposed requirement in proposed Rule 1001(a)(2)(viii) to require SCI entities to include in their policies and procedures the maintenance of a written inventory and classification of all of its SCI systems, critical SCI systems, and indirect SCI systems? Why or why not?
57. Do commenters believe that Regulation SCI should require that SCI entities have a program with respect to the lifecycle management of such systems, including the acquisition, integration, support, refresh, and disposal of such systems, as applicable? Why or why not? Do SCI entities currently maintain such lifecycle management programs? Are there other aspects of lifecycle management that commenters believe should be included in the proposed requirement? If so, please describe.

### 2. Third-Party Provider Management

#### a. Third-Party Provider Management Issues

When it adopted Regulation SCI, the Commission recognized that an SCI entity may choose to use third parties to assist it in running its SCI systems and indirect SCI systems. The Commission took into account such scenarios by including the phrase "or

---

[267] For example, such policies generally should not simply require mere disposal of end-of-life SCI systems but should ensure their effective disposal such that sensitive information (including software, configuration info, middleware, etc.) that could compromise the security of an SCI entity's data and network is not inadvertently revealed.

operated by *or on behalf of*"[268] in key definitions such as "SCI systems," "critical SCI systems," and "indirect SCI systems." The inclusion of the phrase "or on behalf of" was intended to make clear that outsourced systems are not excluded and that any such systems were within the scope of Regulation SCI, even when operated not by the SCI entity itself but rather by a third party. In the SCI Adopting Release, the Commission made clear that it was the responsibility of the SCI entity to manage its relationships with such third parties through due diligence, contract terms, and monitoring of third-party performance.[269] In addition, as the Commission stated when adopting Regulation SCI, "[i]f an SCI entity is uncertain of its ability to manage a third-party relationship…to satisfy the requirements of Regulation SCI, then it would need to reassess its decision to outsource the applicable system to such third party. (footnotes omitted)"[270]

An SCI entity may decide to outsource certain functionality to, or utilize the support or services of, a third-party provider (which would include both affiliated providers as well as vendors unaffiliated with the SCI entity) for a variety of reasons. In selecting a third-party provider to operate an SCI system on its behalf, an SCI entity may be attracted to the potential benefits that it may believe the third-party provider would bring, which could range from cost efficiencies and increased automation to particular expertise the vendor may provide in areas such as security and data latency. Third-party providers may also provide services that an SCI entity may not currently have in-house,

---

268 Emphasis added.

269 *See* SCI Adopting Release, *supra* note 1, at 72276.

270 *Id.*

such as a particular type of software required to run or monitor a given SCI system, or a data or pricing feed.

The Commission believes that the use of third-party providers by SCI entities can be appropriate and even advantageous and preferable in certain instances, given the benefits they may provide when employed appropriately. However, as the Commission discussed in the SCI Adopting Release, when utilizing a third-party provider, an SCI entity is "responsible for having in place processes and requirements to ensure that it is able to satisfy the requirements of Regulation SCI for systems operated on behalf the SCI entity by a third party."[271] Thus, an SCI entity generally should be aware of the potential costs and risks posed by this choice including, for example: cybersecurity risks (*e.g.*, a compromise in a third-party provider's systems impacting the systems of the SCI entity); operational risks (*e.g.*, a disruption or shutdown of a third-party provider's service, or a bankruptcy or cessation of operation of a third-party provider, negatively impacting or disrupting the operation of an SCI system); reputational risks (*e.g.*, a faulty or incorrect input from a third-party provider causing an SCI entity's output to be incorrect); and legal and regulatory risks (*e.g.*, a third-party provider's lack of responsiveness or unwillingness to provide the SCI entity necessary information or detail results in an SCI entity missing a reporting or compliance deadline, such as a deadline for reporting an SCI event or taking corrective action on an SCI event). With the continued and increasing use of third-party providers by SCI entities and, in some cases, with third-party providers playing increasingly important and even critical roles in ensuring the reliable, resilient, and secure operation of SCI systems and indirect SCI systems, the Commission believes that it is

---

[271] *See* SCI Adopting Release, *supra* note 1, at 72276.

appropriate to strengthen Regulation SCI's requirements with respect to SCI entities' use of third-party providers and the management of such relationships, as described in detail below.[272]

In recent years, many types of businesses have turned to cloud service providers ("CSPs") to take advantage of their services.[273] Today, CSPs can provide a range of support to a wide variety of businesses, with deployment models ranging from public cloud, private cloud, hybrid cloud, and multi-cloud, and service models including Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS"), and Software as a Service ("SaaS").[274] SCI entities are also engaging with CSPs to assist in operating their SCI systems and some utilize, or have announced their intention to utilize, CSPs for all or nearly all of their applicable systems,[275] others have begun moving towards employing

---

272 *See infra* sections III.C.2.b. through d (discussing the proposed rule changes with respect to third-party management programs, third-party providers for critical SCI systems, and third-party provider participation in BC/DR testing).

273 *See, e.g.*, Angus Loten, CIOs Accelerate Pre-Pandemic Cloud Push Wall St. J. (Apr. 26, 2021).

274 Additional information relating to the services provided by CSPs is widely available online from CSPs as well as firms that provide consulting services for potential clients of CSPs. FINRA, *Cloud Computing in the Securities Industry* 3-4 (Aug. 2021), *available at* https://www.finra.org/sites/default/files/2021-08/2021-cloud-computing-in-the-securities-industry.pdf (providing a summary description of these services). For a discussion of considerations and risks relevant to the use of cloud service providers by entities in the financial services sector, *see* the Financial Services Sector's Adoption of Cloud Services, U.S. Dept. of the Treasury (issued February 8, 2023), available at: https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

275 *See, e.g.*, FINRA, *Podcast: How the Cloud has Revolutionized FINRA Technology* (July 30, 2018), *available at* www.finra.org/media-center/finra-unscripted/how-cloud-has-revolutionized-finra-technology; Securities Exchange Act Release No. 93433 (Oct. 27, 2021), 86 FR 60503 (Nov. 2, 2021) (SR-OCC-2021-802) (Notice of Filing and Extension of Review Period of Advance Notice Relating to OCC's Adoption of Cloud Infrastructure for New Clearing, Risk Management, and Data Management Applications). *See also*, Huw Jones, *Microsoft invests $2 billion in London Stock Exchange*, Reuters (Dec. 12, 2022).

CSPs at a more deliberate pace,[276] and others continue to explore and consider whether or not to use such services. A decision to move their systems from an "on-premises,"[277] internally run data center to "the cloud" is a significant one, often with potential benefits that may include cost efficiencies, automation, increased security, and resiliency, and entities may also take advantage of such an opportunity to reengineer or otherwise update their systems and applications to run even more efficiently than before.

In deciding whether to utilize a CSP, an SCI entity generally should take into account the various factors it would as with any other third-party providers.[278] However, given the degree to which CSP services may be integral to the operation of SCI systems, SCI entities generally should examine closely any potential relationship and utilization of CSP services. Importantly, regardless of the CSP and service model an SCI entity may be considering, it is the SCI entity's responsibility to ensure that it can and does comply with Regulation SCI. For example, in describing the services they provide, CSP marketing materials typically describe their service models as "shared responsibilities" between the

---

276 *See, e.g.*, Nasdaq, *Press Release: Nasdaq and AWS Partner to Transform Capital Markets* (Nov. 30, 2021), *available at* www.nasdaq.com/press-release/nasdaq-and-aws-partner-to-transform-capital-markets-2021-12-01; Nasdaq, *Press Release: Nasdaq Completes Migration of the First U.S. Options Market to AWS* (Dec. 5, 2022), *available at* https://www.nasdaq.com/press-release/nasdaq-completes-migration-of-the-first-u.s.-options-market-to-aws-2022-12-05.

277 In using the term "on-premises," the Commission means that the data center's hardware (*e.g.*, the servers, switches, and other physical machines) is generally under the control of and operated by the SCI entity, even if the data center is physically located in a facility operated by a third party and for which such third party provides or arranges for certain services including, but not limited to, power, water, and physical security.

278 *See* SCI Adopting Release, *supra* note 1, at 72275-76. In this section, the Commission discusses many issues that may be relevant for SCI entities to consider in relation to their use of third-party vendors generally, and with respect to cloud service providers specifically. These issues include those that the Commission and its staff have encountered with respect to SCI entities since the adoption and implementation of Regulation SCI; however, this is not meant to be a comprehensive list of all potential issues and considerations, and the Commission welcomes comment on other applicable issues and considerations that commenters believe are relevant for SCI entities with respect to third-party providers.

CSP and client. With respect to an SCI entity's obligations under Regulation SCI, however, the SCI entity bears responsibility for compliance with the requirements of Regulation SCI, including for SCI systems operated on its behalf by third-party providers. As with other third-party providers that operate SCI systems on behalf of an SCI entity, if an SCI entity is uncertain of its ability to manage a CSP relationship (whether through appropriate due diligence, contract terms, monitoring, or other methods) to satisfy the requirements of Regulation SCI, the SCI entity would need to reassess its decision to outsource the applicable system to such CSP. As with any third-party provider, the SCI entity generally should not rely solely on the reputation of or attestations from a given CSP. In addition, an SCI entity that utilizes a CSP should not view the usage of a CSP from the perspective of being able to turn over its Regulation SCI-related responsibilities to the CSP; instead, an SCI entity generally should ensure that its own personnel have the requisite skills to properly manage and oversee such a relationship, and understand the issues – including technical ones – that may arise from the utilization of a CSP and are relevant to ensure its compliance with Regulation SCI.[279]

Rule 1001(a)(2)(v) of Regulation SCI requires that an SCI entity's policies and procedures include 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.[280] When the Commission adopted this provision it did not specifically discuss

---

[279] *See* SCI Adopting Release, *supra* note 1, at 72276.

[280] *See* SCI Adopting Release, *supra* note 1, at 72295. *See also infra* section III.C.2.c, including notes 292-294 and accompanying text (discussing the proposed modifications to Rule 1001(a)(2)(v)).

its application to CSPs. Whereas "on-premises" systems are installed and run at a site under the control of an SCI entity, the systems of an SCI entity that reside "in the public cloud" may not be tied to any specific geographic location. However, SCI entities must ensure that their SCI systems, whether "on-premises" or "in the public cloud," comply with the requirement in Regulation SCI to have 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. These provisions of Regulation SCI exist to help limit the downtime caused by wide-scale disruptions. Thus, for example, in determining whether any SCI-related systems "in the public cloud" can meet this requirement, SCI entities generally should understand where its systems will reside (*i.e.*, the locations of the CSP data center site(s) that may be used), and should consider whether those sites provide sufficient geographical diversity and operational resiliency to achieve the resumption requirements of Rule 1001(a)(2)(v).[281]

As discussed in section III.C.2.b.2 below, the Commission's proposal includes a requirement that every SCI entity undertake a risk-based assessment of the criticality of each of its third-party providers, including analyses of third-party provider concentration, of key dependencies if the third-party provider's functionality, support, or service were to become unavailable or materially impaired, and of any potential security, including cybersecurity, risks posed. This third-party provider assessment may be particularly relevant with respect to CSPs utilized by SCI entities, and an SCI entity may want to take

---

[281] While CSPs may use slightly different nomenclature, typically, a CSP's region contains multiple availability zones, and an availability zone contains multiple data centers.

into consideration the degree to which it may be "locked-in" to any given CSP it is considering engaging. As with any third-party provider, it could consider its exit strategies with respect to any potential CSP it might choose and may consider architectural decisions that would enable a quick re-deployment to another CSP if needed. Even when tools, such as containerization,[282] exist that are designed to automate and simplify the deployment of systems to CSPs, and which appear at first glance to allow for greater portability among CSPs, SCI entities may want to consider any lock-in effects that utilizing CSP-specific tools might have. In addition, it may be useful for SCI entities to consider the relative benefits and costs of potential alternatives that could reduce dependence on any single CSP. In cases where the use of CSPs is being considered for both primary and backup systems, an SCI entity, taking into account the nature of its systems, may want to consider whether it is appropriate to utilize different CSPs, for such systems, as well as whether an "on-premises" backup may be appropriate. Similarly, SCI entities should generally engage their CSPs to ensure that they can meet the business continuity and disaster recovery requirements of Regulation SCI, which may not apply to the vast majority of a CSP's other clients.

More broadly, an SCI entity should ensure that it is able to meet its regulatory obligations under Regulation SCI, including the notice and dissemination requirements of Rule 1002. When there is a systems issue (including, for example, an outage or a cybersecurity event) at a CSP, a wide swath of CSP clients may be affected. SCI entities

---

[282] Containerization allows developers to deploy applications more quickly by bundling an application with its required frameworks, configuration files, and libraries such that it may be run in different computing environments. Container orchestrators allow for automated deployment of identical applications across different environments, and simplify the process for management, scaling, and networking of containers.

have regulatory requirements under Regulation SCI that other CSP clients may not have, and an SCI entity must have information regarding such issues within the time requirements of Regulation SCI to comply with its notice and dissemination requirements.[283]

An SCI entity should also be cognizant of its data security and recordkeeping obligations under Regulation SCI,[284] and generally should consider how the CSP and its employees or contractors would secure confidential information, how and where it would retain information (including all records required to be kept under Regulation SCI), how the information would be accessed by the personnel of the SCI entity, or others, such as those conducting SCI reviews and Commission staff, as well as ensure that such information access will be provided in a manner that provides for its compliance with the requirements of Regulation SCI.

While the discussion above is focused on CSPs, they are only one of many types of third-party providers an SCI entity may utilize. The discussion above is not an exhaustive list of issues SCI entities generally should consider with respect to utilizing CSPs; in addition, while the discussion provides some illustrative examples of areas of potential concern in an SCI entity's relationship with a CSP, similar issues may be applicable to the relationships between SCI entities and other types of third parties. In

---

283 *See, e.g.*, Rule 1002 (relating to an SCI entity's obligations with respect to SCI events). *See also* Rule 1001(c) (which include requirements that an SCI entity's policies and procedures include escalation procedures to quickly inform responsible SCI personnel of potential SCI events).

284 *See* 17 CFR 242.1001(a)(2)(iv) ("Rule 1001(a)(2)(iv)") (relating to, among other things, vulnerabilities pertaining to internal threats) and Rule 1005 (relating to recordkeeping requirements related to compliance with Regulation SCI). *See also infra* section III.C.3.a (discussing newly proposed 17 CFR 242.1001(a)(2)(x) ("proposed Rule 1001(a)(2)(x)"), relating to unauthorized access to systems and information).

addition, some third-party providers may provide key functionality that may not have been widely utilized by SCI entities when Regulation SCI was adopted,[285] and the Commission anticipates that third-party providers will likely arise to provide other types of functionality, service, or support to SCI entities that are not contemplated yet today. All the same, the Commission believes that any third-party provider that an SCI entity uses with respect to its SCI systems and indirect SCI systems should be managed appropriately by the SCI entity to help ensure that such utilization of the third-party provider is consistent with the SCI entity's obligations under Regulation SCI.

As discussed above, when the Commission adopted Regulation SCI in 2014, it had accounted for the possibility that an SCI entity might utilize third-party providers to operate its SCI systems or indirect SCI systems by incorporating the phrase "on behalf of" in certain key definitions of Regulation SCI.[286] In addition, "outsourcing" is one of the "domains" identified by the Commission and its staff.[287] Based on the experience of Commission staff, all SCI entities that utilize third-party providers have some level of third-party provider oversight in place. However, given the growing role they are playing with respect to SCI systems and indirect SCI systems, and because the myriad of issues that may arise with respect to third-party providers (including, but not limited to oversight, access, speed of information flow, security and unauthorized access, loss of expertise internally, and lock-in) may become even more amplified when taking into

---

285 One example of this are the services of shadow infrastructure providers, such as edge cloud computing, content delivery networks, and DNS providers.

286 *See supra* notes 268-270 and accompanying text (discussing "on behalf of").

287 *See* SCI Adopting Release, *supra* note 1, at 72302. *See also Staff Guidance on Current SCI Industry Standards* 5, 8 (Nov. 19, 2014), *available at* https://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf.

account the regulatory obligations of SCI entities, the Commission believes that it is appropriate to delineate more clearly requirements with respect to the oversight and management of third-party providers, and thus is proposing to revise Regulation SCI to include additional requirements relating to third-party providers.[288]

**b. Third-Party Provider Management Program**

The Commission is proposing new 17 CFR 242.1001(a)(2)(ix) ("proposed Rule 1001(a)(2)(ix)") regarding third-party provider management. While some SCI entities may already have a formal vendor management program, the Commission is proposing to require that SCI entities have a third-party provider management program that includes certain elements. Specifically, proposed Rule 1001(a)(2)(ix) would require each SCI entity to include in its policies and procedures required under Rule 1001(a)(1) a program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for its SCI systems and, for purposes of security standards, indirect SCI systems. The Commission is proposing this new provision to help ensure

---

288 The Commission proposed the Clearing Agency Governance rules in Aug. 2022, which contains, among other proposed requirements, proposed new 17 CFR 240.17Ad-25(i) ("Rule 17Ad-25(i)"). *See Clearing Agency Governance and Conflicts of Interest*, Securities Exchange Act Release No. 95431 (Aug. 8, 2022), 87 FR 51812 (Aug. 23, 2022) (proposing policy and procedure requirements for clearing agency board of directors to oversee relationships with service providers for critical services to, among other things, confirm and document that risks related to relationships with service providers for critical services are managed in a manner consistent with its risk management framework, and review senior management's monitoring of relationships with service providers for critical services, and to review and approve plans for entering into third-party relationships where the engagement entails being a service provider for critical services to the registered clearing agency). Registered clearing agencies that would be subject to proposed Rule 17Ad-25(i), if adopted, would also be subject to Regulation SCI, as proposed to be amended. However, the scope of proposed Rule 17Ad-25(i) is meant to address not only service providers providing technology or systems-based services, but also service providers that would include the clearing agency's parent company under contract to staff the registered clearing agency, as well as service providers that are investment advisers under contract to help facilitate the closing out of a defaulting participant's portfolio. *See id.* at 51836. Commenters are encouraged to review the Clearing Agency Governance proposed rules to determine whether they might affect their comments on this proposal.

that an SCI entity that elects to utilize a third-party provider will be able to meet its obligations under Regulation SCI.

**i. Third-Party Provider Contract Review**

First, the program would be required to include initial and periodic review of contracts with such third-party providers for consistency with the SCI entity's obligations under Regulation SCI. The Commission believes that it is critical that each SCI entity carefully analyze and understand the impact any third-party providers it chooses to utilize may have on its ability to satisfy its obligations under Regulation SCI. As discussed above,[289] the Commission recognizes that many SCI entities may seek to and, in practice, do outsource certain of its SCI-related functionality, support, or service to third parties. As key entities in our securities markets, SCI entities have regulatory obligations that are not placed upon non-SCI entities, and third-party providers SCI entities may utilize may not be familiar with the requirements of Regulation SCI. As the Commission stated in adopting Regulation SCI, if an SCI entity determines to utilize a third party for an applicable system, "it is responsible for having in place processes and requirements to ensure that it is able to satisfy the applicable requirements of Regulation SCI for such system."[290] And, if an SCI entity is uncertain of its ability to manage a third-party relationship (including through contract terms, among other methods) to satisfy the requirements of Regulation SCI, "then it would need to reassess its decision to outsource the applicable system to such third party."[291] Thus, it is incumbent on SCI entities to

---

289 *See supra* section III.C.2.a.

290 *See* SCI Adopting Release, *supra* note 1, at 72276.

291 *See id*.

review their relationships with such third-party providers to ensure that the SCI entities are able to satisfy their obligations under Regulation SCI. In addition, consistent with the current requirement that an SCI entity periodically review the effectiveness of its policies and procedures, this provision would require an SCI entity to review contracts with such third-party providers periodically for consistency with the SCI entity's obligations under Regulation SCI.

A foundational part of this review is to ensure that any contracts that the SCI entity has with such third-party providers are consistent with the requirements of Regulation SCI. These documents govern the obligations and expectations as between an SCI entity and a third-party provider it utilizes, and the SCI entity is responsible for assessing if these agreements allow it to comply with the requirements of Regulation SCI. For example, an SCI entity generally should consider whether or not it is appropriate to rely on a third-party provider's standard contract or standard service level agreement ("SLA"), particularly if such contract or SLA has not been drafted with Regulation SCI's requirements in mind. For example, regardless of whether an SCI entity is negotiating with the dominant provider in the field, has made its best efforts in negotiating contract or SLA terms, or has extracted what it believes to be "the best terms" it (or any client of the third party) could get, if the SCI entity determines that any term in such agreements are inconsistent with such SCI entity's obligations under Regulation SCI, the SCI entity should reassess whether such outsourcing arrangement is appropriate and will allow it to meet its obligations under Regulation SCI. In addition, in some cases, particularly where the third-party provider would play a significant role in the operation of an SCI entity's SCI systems or indirect SCI systems, or provide functionality, support, or service to such

systems without which there would be a meaningful impact, an SCI entity and its third-party provider may find it useful to negotiate an addendum to any standard contract to separate and highlight the contractual understanding of the parties with respect to SCI-related obligations.

While each contract's specific terms and circumstances will likely differ, there are several considerations that SCI entities generally should take into consideration when entering into such a contract. For example, SCI entities generally should consider whether a contract raises doubt on its consistency with the SCI entity's obligations under Regulation SCI (*e.g.*, the contract terms are vague regarding the third-party provider's obligations to the SCI entity to enable the SCI entity to meets its SCI obligations). Generally, contractual terms should not be silent or lack substance on key aspects of Regulation SCI that would need the third-party provider's cooperation (*e.g.*, SCI event notifications and information dissemination, and business continuity and disaster recovery for an SCI entity seeking to move its SCI systems to a cloud service provider). Nor should they undermine the ability of the SCI entity to oversee and manage the third party (*e.g.*, by limiting the SCI entity's personnel ability to assess whether systems operated by a third-party provider on behalf of the SCI entity satisfy the requirements of Regulation SCI). The SCI entity may want to consider and, if appropriate, negotiate provisions that provide priority to the SCI entity's systems, such as for failover and/or business continuity and disaster recovery ("BC/DR") scenarios, if needed to meet the SCI entity's obligations under Regulation SCI. In addition, an SCI entity generally should review the contract for provisions that, by their terms, are inconsistent with Regulation SCI or would otherwise fail to satisfy the requirements of Regulation SCI (*e.g.*,

restricting information flow to the SCI entity and/or Commission and its staff pursuant to a non-disclosure agreement in a manner inconsistent with the requirements of Regulation SCI; specifying response times that are inconsistent with (*i.e.*, slower than) those required by Regulation SCI with respect to notifications regarding SCI events under Rule 1002). The Commission also believes that, to the extent possible, SCI entities may want to avoid defining terms in a contract with a third-party provider differently from how they are used in Regulation SCI, as this may introduce confusion as to the scope and applicability of Regulation SCI. In addition, although it is a term that may be common in many commercial contracts, provisions that provide the third-party provider with the contractual right to be able to make decisions that would negatively impact an SCI entity's obligations in its "commercially reasonable discretion" should be carefully considered, as what may be considered "commercially reasonable" for many entities that are not subject to Regulation SCI may not be appropriate for an SCI entity and its SCI systems and indirect SCI systems when taking into consideration the regulatory obligations of Regulation SCI.

**ii. Risk-Based Assessment of Third-Party Providers**

The Commission is also proposing in proposed Rule 1001(a)(2)(ix) to require each SCI entity to undertake a risk-based assessment of each third-party provider's criticality to the SCI entity, including analyses of third-party provider concentration, of key dependencies if the third-party provider's functionality, support, or service were to become unavailable or materially impaired, and of any potential security, including cybersecurity, risks posed. The Commission believes that specifically requiring each SCI entity to undertake a risk-based assessment of each of its third-party providers' criticality to the SCI entity will help them more fully understand the risks and vulnerabilities of

utilizing each third-party provider, and provide the opportunity for the SCI entity to better prepare in advance for contingencies should the provider's functionality, support, or service become unavailable or materially impaired. In performing this risk-based assessment, SCI entities would be required to consider third-party provider concentration, which would help ensure that they properly account and prepare contingencies or alternatives for an overreliance on a given third-party provider by the SCI entity or by its industry. In addition, each SCI entity would be required to assess any potential security, including cybersecurity, risks posed by its third-party provider, to help ensure that the SCI entity does not only take into consideration the benefits it believes a third-party provider can provide it, but the security risks involved in utilizing a given provider as well.

**c. Third-Party Providers for Critical SCI Systems**

The newly proposed provisions of proposed Rule 1001(a)(2)(ix) discussed above would apply to all SCI entities for all of their SCI systems. However, given the essential nature of critical SCI systems,[292] the Commission believes that it is appropriate to require SCI entities to have even more robust policies and procedures with respect to any third-party provider that supports such systems. In adopting Regulation SCI, the Commission stated that critical SCI systems are those SCI systems "whose functions are critical to the operation of the markets, including those systems that represent potential single points of

---

292 Critical SCI systems include systems that directly support functionality relating to: (i) clearance and settlement systems of clearing agencies; (ii) openings, reopenings, and closings on the primary listing market; (iii) trading halts; (iv) initial public offerings; (v) the provision of market data by a plan processor; or (vi) exclusively listed securities. In addition, the definition of critical SCI systems includes a catchall provision for systems that provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.

failure in the securities markets [and]…are those that, if they were to experience systems issues, the Commission believes would be most likely to have a widespread and significant impact on the securities market."[293] Therefore, the Commission is proposing to revise Rule 1001(a)(2)(v), which relates to the business continuity and disaster recovery plans of SCI entities. Currently, Rule 1001(a)(2)(v) requires their policies and procedures to include 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. To help ensure that SCI entities are appropriately prepared for any contingency relating to a third-party provider with respect to critical SCI systems, the Commission is proposing to revise Rule 1001(a)(2)(v) to also require the BC/DR plans of SCI entities to be reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity without which there would be a material impact on any of its critical SCI systems.

As discussed above, the Commission is proposing under proposed Rule 1001(a)(2)(ix) to require each SCI entity to conduct a risk-based assessment of the criticality of each of its third-party providers to the SCI entity. With respect to an SCI entity's critical SCI systems, the Commission believes the revised provisions of Rule 1001(a)(2)(v) are appropriate to ensure that an SCI entity has considered and addressed in its BC/DR plans how it would deal with a situation in which a third-party provider that provides any functionality, support, or service for any of its critical SCI systems has an

---

[293] *See* SCI Adopting Release, *supra* note 1, at 72277.

issue that would materially impact any such system. For example, such BC/DR plans generally should not only take into account and address temporary losses of functionality, support, or service – such as a momentary outage that causes a feed to be interrupted or extended cybersecurity event on the third-party provider – but also consider more extended outage scenarios, including if the third-party provider goes into bankruptcy or dissolves, or if it breaches its contract and decides to suddenly, unilaterally, and/or permanently cease to provide the SCI entity's critical SCI systems with functionality, support, or service.[294] In determining how to satisfy the requirement that policies and procedures be reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity without which there would be a material impact on any of its critical SCI systems, an SCI entity could consider if use of a CSP for its critical SCI systems also warrants maintaining an "on-premises" backup data center or other contingency plan which could be employed in the event of the scenarios noted above.

**d. Third-Party Provider Participation in BC/DR Testing**

With respect to an SCI entity's business continuity and disaster recovery plans, including its backup systems, Rule 1004 of Regulation SCI requires SCI entities to,: (a) establish standards for the designation of those members or participants that the SCI entity reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of such plans; (b) designate members or participants pursuant to such standards and require participation by

---

294 While such scenarios may appear to be improbable, given the criticality of the critical SCI systems to the SCI entity and U.S. securities markets, SCI entities should have plans in place to account for such scenarios, however remote.

such designated members or participants in scheduled functional and performance testing of the operation of such plans, in the manner and frequency specified by the SCI entity, provided that such frequency shall not be less than once every 12 months; and (c) coordinate the testing of such plans on an industry- or sector-wide basis with other SCI entities.[295]

Because the Commission believes that some third-party providers may be of such importance to the operations of an SCI entity, the Commission is proposing to include certain third-party providers in the BC/DR testing requirements of Rule 1004. In the same way SCI entities currently are required to establish standards for and require participation by their members or participants in the annual industry-wide testing required of all SCI entities, the Commission is adding third-party providers as another category of entities. Thus, pursuant to revised paragraph (a) of Rule 1004, an SCI entity would be required also to establish standards for the designation of third-party providers (in addition to members or participants) that it determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of the SCI entity's BC/DR plans. In addition, paragraph (b) of Rule 1004 would require each SCI entity to designate such third-party providers (in addition to members or participants) pursuant to such standards and require their participation in the scheduled functional and performance testing of the operation of such BC/DR plans, which would occur not less than once every 12 months and which would be coordinated with other SCI entities on an industry- or sector-wide basis.

---

[295] *See* 17 CFR 242.1004. *See also* SCI Adopting Release, *supra* note 1, at 72347-55 (providing a more detailed discussion of the BC/DR testing requirements under Rule 1004).

As discussed above, SCI entities often employ a wide array of third-party providers which perform a multitude of different functions, support, or services for them. While many of these third-party providers may provide relatively minor functions, support, or services for an SCI entity, there may be one or more third-party providers of such significance to the operations of an SCI entity that, without the functions, support, or services of such provider(s), the maintenance of fair and orderly markets in the event of the activation of the SCI entity's BC/DR plans would not be possible. For example, the Commission believes it likely that, for an SCI entity that utilizes a cloud service provider for all, or nearly all, of its operations, such CSP would be of such importance to the operations of the SCI entity and the maintenance of fair and orderly markets in the event of the activation of the SCI entity's BC/DR plans that it would be required to participate in the BC/DR testing required by Rule 1004.[296]

**e. Third-Party Providers of Certain Registered Clearing Agencies**

The Commission may examine the provision of services by third-party providers of certain registered clearing agencies. The Financial Stability Oversight Council ("FSOC") has designated certain financial market utilities ("FMUs")[297] as systemically

---

[296] Contractual arrangements with applicable third-party providers that require such providers to engage in BC/DR testing could help ensure implementation of this requirement. *See also* SCI Adopting Release, *supra* note 1, at 72350 (discussing how contractual arrangements by SCI entities that are not SROs would enable such SCI entities to implement the BC/DR testing requirement for their members or participants).

[297] *See* 12 U.S.C. 5462(6). The definition of "financial market utility" in section 803(6) of the Clearing Supervision Act contains a number of exclusions that include, but are not limited to, certain designated contract markets, registered futures associations, swap data repositories, swap execution facilities, national securities exchanges, national securities associations, alternative trading systems, security-based swap data repositories, security-based swap execution facilities, brokers, dealers, transfer agents, investment companies, and futures commission merchants. *See* 12 U.S.C. 5462(6)(B).

important or likely to become systemically important financial market utilities ("SIFMUs").[298] The Payment, Clearing, and Settlement Supervision Act of 2010 ("Clearing Supervision Act"), enacted in Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank Act"), provides for the enhanced regulation of certain FMUs.[299] FMUs include clearing agencies that manage or operate a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the FMU.[300] For SIFMUs, the Clearing Supervision Act provides for enhanced coordination between the Commission and Federal Reserve Board by allowing for regular on-site examinations and information sharing,[301] and further provides that the Commission and CFTC shall coordinate with the Federal

---

298 *See* 12 U.S.C. 5463. An FMU is systemically important if the failure of or a disruption to the functioning of such FMU could create or increase the risk of significant liquidity or credit problems spreading among financial institutions or markets and thereby threaten the stability of the U.S. financial system. *See* 12 U.S.C. 5462(9). On July 18, 2012, the FSOC designated as systemically important the following then-registered clearing agencies: CME Group ("CME"), DTC, FICC, ICC, NSCC, and OCC. The Commission is the supervisory agency for DTC, FICC, NSCC, and OCC, and the CFTC is the supervisory agency for CME and ICE. The Commission jointly regulates ICC and OCC with the CFTC. The Commission also jointly regulates ICE Clear Europe ("ICEEU"), which has not been designated as systemically important by FSOC, with the CFTC and Bank of England. The Commission also jointly regulated CME with the CFTC until 2015, when the Commission published an order approving CME's request to withdraw from registration as a clearing agency. *See* Securities Exchange Act Release No. 76678 (Dec. 17, 2015), 80 FR 79983 (Dec. 23, 2015).

299 The objectives and principles for the risk management standards prescribed under the Clearing Supervision Act shall be to (i) promote robust risk management; (ii) promote safety and soundness; (iii) reduce systemic risks; and (iv) support the stability of the broader financial system. Further, the Clearing Supervision Act states that the standards may address areas such as risk management policies and procedures; margin and collateral requirements; participant or counterparty default policies and procedures; the ability to complete timely clearing and settlement of financial transactions; capital and financial resources requirements for designated FMUs; and other areas that are necessary to achieve the objectives and principles described above. *See* 12 U.S.C. 5464(b), (c).

300 *See* 12 U.S.C. 5462(6).

301 *See* 12 U.S.C. 5466.

Reserve Board to develop risk management supervision programs for SIFMUs jointly.[302] In addition, section 807 of the Clearing Supervision Act provides that "[w]henever a service integral to the operation of a designated financial market utility is performed for the designated financial market utility by another entity, whether an affiliate or non-affiliate and whether on or off the premises of the designated financial market utility, the Supervisory Agency may examine whether the provision of that service is in compliance with applicable law, rules, orders, and standards to the same extent as if the designated financial market utility were performing the service on its own premises."[303] Given the importance of the provision of services by SIFMUs to the U.S. financial system and global financial stability, SIFMU third-party providers may be integral to the operation of the SIFMU and thus be examined by the Commission.

**f. Request for Comment**

58. Do SCI entities employ third-party providers to operate SCI systems or indirect SCI systems on their behalf? If so, what types of systems are most frequently operated by third parties?
59. Please describe SCI entities' use of third-party providers generally, even if they do not operate SCI systems or indirect SCI systems on behalf of an SCI entity. What types of functionality, support, or service do such entities provide to SCI entities? Please describe.

---

302 *See* 12 U.S.C. 5472; *see also* Federal Reserve Board, et al., *Risk Management Supervision of Designated Clearing Entities* (July 2011), *available at* https://www.federalreserve.gov/publications/other-reports/files/risk-management-supervision-report-201107.pdf (describing the joint supervisory framework of the Commission, CFTC, and Federal Reserve Board).

303 12 U.S.C. 5466.

60. The Commission requests commenters' views on significant issues that they believe SCI entities should take into account with respect to their use of third-party providers and the requirements of Regulation SCI. Are there common or important issues that commenters believe the Commission should focus on in addition to those discussed above? If so, please describe.
61. Do commenters believe it is appropriate to require, as in proposed Rule 1001(a)(2)(ix), that each SCI entity have a program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for its SCI systems and, for purposes of security standards, indirect SCI systems? Do commenters believe that such a program should require an initial and periodic review of contracts with such providers for consistency with the SCI entity's obligations under Regulation SCI? Why or why not?
62. Do commenters believe that it is appropriate to require each SCI entity to include a risk-based assessment of each third-party provider's criticality to the SCI entity, including analyses of third-party provider concentration, of key dependencies if the third-party provider's functionality, support, or service were to become unavailable or materially impaired, and of any potential security, including cybersecurity, risks posed? Why or why not?
63. Are there any third-party providers, or types of third-party providers, that commenters believe an SCI entity or SCI entities rely on in a manner that creates, from the commenters' point of view, undue concentration risk? If so, please describe.
64. Are there other aspects of third-party provider management that commenters believe should be included in the proposed rule provision? If so, please describe.

65. Do commenters agree with the proposed revisions to Rule 1001(a)(2)(v) to require the BC/DR plans of SCI entities to be reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity without which there would be a material impact on any of its critical SCI systems? Why or why not? Do commenters believe that any such providers exist today for the critical SCI systems of SCI entities? If so, please describe. Should the Commission require third-party provider diversity for critical systems of an SCI entity, for example, requiring an SCI entity that utilizes a third-party provider for its critical SCI systems to use a different party (*i.e.*, another third-party provider or operate the critical SCI system itself) for its backup for such systems? Why or why not?

66. Do commenters agree with the proposed revisions to Rule 1004 to require that SCI entities establish standards and designate third-party providers that must participate in BC/DR testing in the annual industry-wide BC/DR testing required by Rule 1004? Why or why not?

### 3. Security

The Commission recognized the importance of security for the technology systems of SCI entities and included various requirements and provisions in Regulation SCI relating to the security of an SCI entity's SCI systems. For example, the rules provide that minimum policies and procedures must provide for, among other things, regular reviews and testing of systems, including backup systems, to identify vulnerabilities from internal and external threats.[304] In addition, penetration testing is

[304] *See* 17 CFR 242.1001(a)(2)(iv).

required as part of the SCI review.[305] Recognizing that SCI systems may be vulnerable if other types of systems are not physically or logically separated (or "walled off"), Regulation SCI also specifies that "indirect systems" – defined as systems that if breached, are reasonably likely to pose a security threat to SCI systems – are also subject to the provisions of Regulation SCI relating to security standards and systems intrusions.[306] Thus, the application of Regulation SCI to indirect SCI systems could encourage SCI entities to establish effective controls that result in the core SCI systems being logically or physically separated from other systems that could provide vulnerable entry points into SCI systems, thereby removing these non-SCI systems from the scope of indirect SCI systems.[307]

Regulation SCI also includes "systems intrusions"[308] as one of three types of SCI events for which SCI entities are required to take corrective action, provide notification to the Commission, and disseminate information to their members and participants.[309] Since the adoption of Regulation SCI in 2014, cybersecurity has continued to be a significant concern for SCI entities and non-SCI entities alike. Various studies and surveys have noted significant increases in cybersecurity events[310] across all types of companies in

---

305 *See* 17 CFR 242.1003(b)(1)(i).

306 *See* 17 CFR 242.1000.

307 *See* SCI Adopting Release, *supra* note 1, at 72287-89 (discussing systems intrusions).

308 A "systems intrusion" is defined as "any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity." *See* 17 CFR 242.1000.

309 *See* 17 CFR 242.1002.

310 Cybersecurity events can span a wide variety of types of threats. For example, FINRA summarized common cybersecurity threats faced by broker-dealers to include phishing, imposter websites, malware, ransomware, distributed denial-of-service attacks, and vendor breaches, among others. *See* FINRA, *Common Cybersecurity Threats*, *available at* www.finra.org/rules-guidance/guidance/common-cybersecurity-threats.

recent years.[311] Among these are targeted ransomware attacks that lock access to a victim's data unless a ransom is paid, and have included certain high-profile incidents involving the local government of a major U.S. city[312] as well as one of the largest oil pipelines in the United States.[313] Cybersecurity events have also included hacks that have had widespread impacts across many industries and types of entities.[314] Financial sector entities have been vulnerable to cybersecurity events as well, including the Society for Worldwide Interbank Financial Telecommunication ("SWIFT"), an international cooperative of financial institutions that provides safe and secure financial transactions for its members, which was the target of a series of cybersecurity events in 2015 and 2016, including one incident in which $81 million was stolen.[315]

---

311 *See, e.g.*, Financial Services Information Sharing and Analysis Center, *Navigating Cyber 2022* (Mar. 2022), *available at* www.fsisac.com/navigatingcyber2022-report (detailing cyber threats that emerged in 2021 and predictions for 2022); Bree Fowler, *Number and cost of cyberattacks continue to grow, new survey says*, CNET (Jan. 21, 2022), *available at* https://www.cnet.com/news/privacy/cyberattacks-continue-to-increase-new-survey-says (citing, among other things, Anomali's poll of cybersecurity decision makers that 87% of their companies had experienced a cyberattack in the past three years that resulted in damage, disruption, or data breach); Accenture, *Triple digit increase in cyberattacks: What next?* (Aug. 4, 2021), *available at* www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks; Chris Morris, *Cyberattacks and ransomware hit a new record in 2021, says report*, Fast Company (Jan. 25, 2022), *available at* https://www.fastcompany.com/90715622/cyberattacks-ransomware-data-breach-new-record-2021 (citing report by Identity Theft Resource Center stating that the number of security compromises was up more than 68% in 2021).

312 *See, e.g.*, Stephen Deere, *Cost of City of Atlanta's cyber attack: $2.7 million – and rising*, The Atlanta Journal-Constitution (Apr. 12, 2018), *available at* https://www.ajc.com/news/cost-city-atlanta-cyber-attack-million-and-rising/nABZ3K1AXQYvY0vxqfO1FI/ (describing the costs relating to a five-day ransomware attack on the City of Atlanta in Mar. 2018).

313 *See, e.g.*, Clare Duffy, *Colonial Pipeline attack: A 'wake up call' about the threat of ransomware*, CNN Business (May 16, 2021), *available at* https://www.cnn.com/2021/05/16/tech/colonial-ransomware-darkside-what-to-know/index.html (describing the ransomware attack on a pipeline and concerns regarding the potential for similar attacks on critical US infrastructure).

314 *See, e.g.*, David Uberti, et al., *The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw*, Wall Street Journal (Dec. 21, 2021), *available at* https://www.wsj.com/articles/what-is-the-log4j-vulnerability-11639446180 (discussing the Log4j hack).

315 *See, e.g.*, Kim Zetter, *That Insane, $81M Bangladesh Bank Heist? Here's What We Know*, WIRED (May 17, 2016), *available at* https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.

Given the continued and increasing risks associated with cybersecurity for SCI entities, the Commission believes it is appropriate to enhance the cybersecurity provisions of Regulation SCI to help ensure that SCI systems and indirect SCI systems of the most important entities in our securities markets remain secure.

**a. Unauthorized Access to Systems and Information**

While Rule 1001(a)(1) already requires an SCI entity to have policies and procedures reasonably designed to ensure that its SCI systems and indirect SCI systems have levels of security adequate to maintain operational capabilities and promote the maintenance of fair and orderly markets, and Rule 1001(a)(4) specifies that policies and procedures will be deemed reasonable if consistent with current SCI industry standards, Rule 1001(a)(2) is not specific in terms of the need for an SCI entity to have access controls designed to protect both the security of the systems and the information residing therein. Limiting access to SCI systems and indirect SCI systems and the information residing therein to authorized purposes and users is particularly important given that these systems include the core technology of key U.S. securities markets entities, and would help ensure that such systems and information remain safeguarded and protected from unauthorized uses. Proposed Rule 1001(a)(2)(x) would specify that the Rule 1001(a)(1) policies and procedures of SCI entities include a program to prevent the unauthorized access to such systems and information residing therein. An SCI entity's policies and procedures generally should specify appropriate access controls to ensure that its applicable systems and information is protected. Such policies and controls generally should be designed to prevent both unauthorized external intruders as well as unauthorized internal personnel from access to these systems and information. For example, this would also include personnel that may be inappropriately accessing certain

systems and/or information residing on such systems, though they may have authorized access to other systems, portions of systems, or certain information residing in such systems at the SCI entity. Thus, for example, the procedures and access controls at the SCI entity generally should provide for an appropriate patch management cycle for systems software, to ensure that known software vulnerabilities are identified and patches are deployed and validated in a timely manner. The procedures and access controls generally should also be calibrated sufficiently to account for such different levels of access for each person granted access to any part of the SCI entity's systems or information. In addition, this requirement would make clear that an SCI entity's policies and procedures are required to address not only protection of its technology systems, but also of the information residing on such systems.

In developing and implementing such policies and procedures, SCI entities generally should develop a clear understanding of the need for access to systems and data, including identifying which users should have access to sensitive systems or data. In general, such policies and procedures should include: requiring standards of behavior for individuals authorized to access SCI systems and indirect SCI systems and information residing therein, such as an acceptable use policy; identifying and authenticating individual users; establishing procedures for timing distribution, replacement, and revocation of passwords or methods of authentication; restricting access to specific SCI systems or components thereof or information residing therein only to individuals requiring access to such systems or information as is necessary for them to perform their responsibilities or functions for the SCI entity; and securing remote access technologies

used to interface with SCI systems.[316] Access to systems and data can be controlled through a variety of means, including but not limited to the issuance of user credentials, digital rights management with respect to proprietary hardware and copyrighted software, authentication methods including multifactor authentication as appropriate, tiered access to sensitive information and network resources, and security and access measures that are regularly monitored not only to provide access to authorized users, but also to remove access for users that are no longer authorized (*e.g.*, due to termination of employment).[317] As with other policies and procedures required under Rule 1001, SCI entities may, if they choose, look to SCI industry standards in developing their policies and procedures to prevent unauthorized access to information and systems.[318]

**b. Penetration Testing**

Penetration tests can help entities understand how effective their security policies and controls are in the face of attempted and successful systems intrusions, and assist in revealing the potential threats and vulnerabilities to the entity's network and controls that might be exploited by malicious attackers to disrupt the operation of their systems, result in stolen confidential information, and damage their reputations. When the Commission adopted Regulation SCI in 2014, it required that SCI entities conduct penetration testing as part of its SCI review[319] but, because of the costs associated with penetration testing at

---

316 *See* Exchange Act Cybersecurity Proposal, *supra* note 10.

317 *See* Exchange Act Cybersecurity Proposal, *supra* note 10 (similarly discussing examples of access controls).

318 *See* Rule 1001(a)(4) of Regulation SCI (defining current SCI industry standards), which is discussed further in *infra* section III.C.5.

319 Specifically, paragraph (b)(1) of Rule 1003 currently requires that "[p]enetration test reviews of the network, firewalls, and production systems shall be conducted at a frequency of not less than once every three years…". Rule 1003(b)(1).

the time, only required that such tests be conducted once every three years.[320] In the time since the adoption of Regulation SCI, cybersecurity has become an even greater and more pervasive concern for all types of businesses, including SCI entities. At the same time, best practices of businesses with respect to penetration testing have evolved such that such tests occur on a much more frequent basis, as businesses confront the threat of cybersecurity events on a wider scale.[321]

Given this, the Commission is proposing to increase the frequency of penetration testing by SCI entities such that they are conducted at least annually, rather than once every three years. The Commission believes that such tests are a critical component of ensuring the cybersecurity health of an SCI entity's technology systems and that such a frequency would help to ensure that robust measures are in place to protect an SCI entity's systems from cybersecurity events. In addition, the proposed annual frequency would only be a minimum frequency and SCI entities may choose to adopt even more frequent penetration tests if they feel it appropriate to do so.[322]

In addition, the Commission is proposing to require that the conduct of such penetration testing include testing by the SCI entity of any vulnerabilities of its SCI

---

320 *See* SCI Adopting Release, *supra* note 1, at 72344.

321 *See, e.g.*, Fortra, *2022 Penetration Testing Report* 14 (July 7, 2022), *available at* https://static.fortra.com/core-security/pdfs/guides/cs-2022-pen-testing-report.pdf (stating that 42% of respondents conducted penetration testing one or two times a year, and 45% of respondents conducted penetration testing at a more frequent pace); PCI Security Standards Council, *Information Supplement: Penetration Testing Guidance* 6 (Sept. 2017), *available at* https://listings.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf ("at least annually and upon significant changes").

322 As discussed further below, as part of the proposed revisions to the SCI review requirement, the Commission is also moving rule provisions relating to the substantive requirements of the SCI review to Rule 1000 under the definition of "SCI review," while timing requirements relating to the SCI review and the report of the SCI review would be contained in Rule 1003(b). Thus, although currently the requirement relating to penetration test reviews is in Rule 1003, it is now proposed to be in Rule 1000.

entity's SCI systems and indirect SCI systems identified pursuant to § 242.1001(a)(2)(iv). Currently, the requirement in Rule 1003 with respect to penetration testing does not include this phrase. However, Rule 1001(a)(2)(iv) requires an SCI entity's policies and procedures to include, among other things, "regular reviews and testing…to identify vulnerabilities pertaining to internal and external threats…" The new language with respect to penetration testing (which is proposed to be located in the definition of SCI review in Rule 1000) would require SCI entities to include testing of the vulnerabilities identified pursuant to its regular review and testing requirement in designing its penetration testing. Thus, rather than, for example, running a static annual test against a portion of its SCI systems, this proposed language would require an SCI entity's penetration testing program to include any identified relevant threats and then conduct penetration testing accordingly, which should help ensure the security and resiliency of SCI systems.

**c. Systems Intrusions**

Rule 1000 of Regulation SCI defines a "systems intrusion" as any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity. Systems intrusions are one of three types of SCI events that each SCI entity must monitor for and, when they occur, subject to certain exceptions, an SCI entity must: take corrective action;[323] immediately notify the Commission and maintain certain records with respect to the event;[324] and promptly disseminate information about the event to applicable members

---

[323] *See* 17 CFR 242.1002(a).

[324] *See* 17 CFR 242.1002(b) (setting forth the notification and follow-up reporting that is required for a systems intrusion that is not de minimis).

and participants of each SCI entity.[325] As discussed in the SCI Adopting Release,[326] the definition of systems intrusion has several important characteristics to it, two of which are relevant to the changes proposed. First, because the term "entry" is used in the current definition, the term systems intrusions only applies to "successful" intrusions, thus excluding attempted (*i.e.*, unsuccessful) intrusions. In addition, the term "entry into" implies that the intrusion is limited to events that result in an intruder entering into the SCI entity's SCI systems or indirect SCI systems, and thus does not include any types of attacks on systems outside of the SCI entity's SCI systems or indirect SCI systems that nonetheless impacts such systems.

As discussed above, cybersecurity has become ever more increasingly important for all types of entities, and the same is true for SCI entities. The Commission believes that it is appropriate to expand the definition of systems intrusion to include two additional types of cybersecurity events. The first additional type of systems intrusion would include certain types of incidents that are currently considered to be cybersecurity events that are not included in the current definition, as discussed below. In addition, the revised definition would ensure that the Commission and its staff are made aware when an SCI entity is the subject of a significant cybersecurity threat, including those that may be ultimately unsuccessful, which would provide important information regarding threats that may be posed to other entities in the securities markets, including other SCI entities. By requiring SCI entities to submit SCI filings for these new types of systems intrusions, the Commission believes that the revised definition of systems intrusion would provide

---

325 *See* 17 CFR 242.1002(c).

326 *See* SCI Adopting Release, *supra* note 1, at 72288.

the Commission and its staff more complete information to assess the security status of the SCI entity, and also assess the impact or potential impact that unauthorized activity could have on the security of the SCI entity's affected systems as well on other SCI entities and market participants.

The proposed definition would have three prongs, the first of which would contain the current requirement that defines any "unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity" as a systems intrusion, and would continue to include a wide range of cybersecurity events. As stated in the SCI Adopting Release, the current definition describes "any unauthorized" entry or "breach" into SCI systems or indirect SCI systems, and includes unauthorized access, whether intentional or inadvertent, by employees or agents of the SCI entity that resulted from weaknesses in the SCI entity's access controls and/or procedures.[327] For example, data breaches are included under the first prong, as are instances in which an employee of an SCI entity accessed an SCI system without proper authorization. It also includes instances in which an employee, such as a systems administrator, was authorized to access a system, but where the employee improperly accessed confidential information within such system. Similarly, an instance in which members of an SCI entity were properly accessing a system but were inadvertently exposed to the confidential information of other members would also likewise fall within this prong.[328]

The new second prong would expand the definition of systems intrusion to include any cybersecurity event that disrupts, or significantly degrades, the normal

---

327 *See* SCI Adopting Release, *supra* note 1, at 72887-89 (providing a more detailed discussion of the current definition of systems intrusions).

328 *See id.* (providing a more detailed discussion of the current definition of systems intrusions).

operation of an SCI system. This prong is intended to include cybersecurity events on the SCI entity's SCI systems or indirect SCI systems that cause disruption to such systems, regardless of whether the event resulted in an entry into or access to them. For example, in distributed denial-of-service attacks, the attacker, often using malware-infected machines, typically seeks to overwhelm or drain the resources of the target with illegitimate requests to prevent the target's systems from providing services to those seeking to access or use them. Unlike cybersecurity events that would qualify under the current definition of systems intrusions (*i.e.*, the first prong of the proposed definition), the objective of these attacks is often simply to disrupt or disable the target's operations, rendering them unable to run efficiently, or run at all. For example, given the essential role hypervisors play in supporting cloud computing, an attack on a CSP's hypervisor, which enables the sharing of physical compute and memory resources across multiple virtual machines, could also significantly disrupt or even disable, albeit indirectly, the SCI systems of an SCI entity that is utilizing such CSP, and thus constitute a systems intrusion under the proposed second prong. Likewise, these systems intrusions could include certain command and control attacks where a malicious actor is able to infiltrate a system to install malware to enable it to send commands to infected devices remotely. Similarly, supply chain attacks that enter a SCI entity's systems through an apparently authorized means, such as through regular maintenance software updates that – unbeknownst to the software provider and the recipient – contain malicious code and could also be systems intrusions under this proposal.[329] Because such cybersecurity events can cause serious harm and disruption to an SCI entity's operations, the

---

[329] *See supra* note 314 and accompanying text (discussing the Log4j hack).

Commission believes that the definition of systems intrusion should be broadened to include cybersecurity events that may not entail actually entering or accessing the SCI entity's SCI systems or indirect SCI systems, but still cause disruption or significant degradation. For this second prong, the Commission believes it is appropriate to utilize language similar to that used in the definition of systems disruption (*i.e.*, "disrupts, or significantly degrades, the normal operation of an SCI system").[330] Similar to a systems disruption that occurs within the SCI systems or indirect SCI systems, if a cybersecurity event disrupts, or significantly degrades, an SCI entity's normal operations,[331] it would constitute a systems intrusion under the proposed revised definition, and the obligations and reporting requirements of Rule 1002 would apply.[332]

The third prong would include any significant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria. In contrast to the types of systems intrusions that are part of the first prong of the proposed definition, the third prong is intended to capture unsuccessful, but significant, attempts to enter an SCI entity's SCI systems or indirect SCI systems. The Commission recognizes that it would be inefficient, inappropriate, and undesirable (for both SCI entities as well as the Commission and its

---

330 The Commission believes that the term "cybersecurity event," as used here, would generally be understood to mean "an unauthorized activity that disrupts or significantly degrades the normal operation of an SCI system."

331 *See* SCI Adopting Release, *supra* note 1, at 72284 ("SCI entities would likely find it helpful to establish parameters that can aid them and their staff in determining what constitutes the 'normal operation' of each of its SCI systems and when such 'normal operation' has been disrupted or significantly degraded because those parameters have been exceeded." (footnotes omitted)).

332 Such events may, in some cases, first appear to an SCI entity to be a "systems disruption" but, upon further investigation and understanding of the true cause of the SCI event, may turn out to be both a "systems intrusion" as well as a "systems disruption." In such cases, the applicable SCI entity should mark the SCI event as both types on its submissions to the Commission on Form SCI.

staff) to require that all attempted entries be considered systems intrusions. Rather, the Commission is seeking to include only attempts that an SCI entity believes to be significant attempts to its systems, even if successfully prevented.

The term "significant attempted unauthorized entry" would not be defined in the rule. Rather, the proposed rule would require each SCI entity to establish reasonable written criteria for it to use to determine whether a significant attempted unauthorized entry has occurred, because the Commission believes that each SCI entity should be granted some degree of discretion and flexibility in determining what constitutes a significant attempted unauthorized entry for its purposes, given that SCI entities differ in nature, size, technology, business model, and other aspects of their businesses.[333] However, the Commission believes that certain characteristics of attempted unauthorized entries would generally weigh in favor of such attempted unauthorized entries being considered significant and constituting systems intrusions that should be considered SCI events subject to the requirements of Regulation SCI, including: when an SCI entity becomes aware of reconnaissance that may be leveraged by a threat actor; a targeted campaign that is customized to the SCI entity's system;[334] an attempted cybersecurity

---

333 Under 17 CFR 242.1003(a)(1) ("Rule 1003(a)(1)"), each SCI entity is similarly required to establish reasonable written criteria for identifying a material change to its SCI systems for quarterly reporting to the Commission. *See also* SCI Adopting Release, *supra* note 1, at 72341-42 (discussing the definition of material systems change).

334 A wide variety of entities engage in web scanning, which may be in a targeted manner (*e.g.*, looking at certain IP address ranges) or broadly across the internet. Often, such scanning may be for non-malicious purposes such as, for example, indexing website content (for search engines) or mapping networks. Others may engage in such scanning to identify vulnerable systems or websites, which could be to inform vulnerability management identification and remediation efforts or identify opportunities for exploitation. Because of the wide range of possible uses of scanning and the nature of scanning tools' interactions with systems, such scanning activity alone is not necessarily indicative of malicious intent or even a vulnerable system capable of being exploited. However, evidence of further, follow-on activity indicative of a precursor to unauthorized entry may be a factor that an SCI entity should consider in weighing whether a significant attempted unauthorized entry has occurred.

event that required the SCI entity's personnel to triage, even if it was ultimately determined to have no impact; an attempted attack from a known sophisticated advanced threat actor; the depth of the breach in terms of proximity to SCI systems and critical SCI systems; and a cybersecurity event that, if successful, had meaningful potential to result in widespread damage and/or loss of confidential data or information.

As with all SCI events, SCI entities would be required under 17 CFR 242.1002(a) ("Rule 1002(a)") to take corrective action with respect to any events that were determined to be systems intrusions under the proposed revised definition. In addition, the Commission is proposing to make a revision to the Commission reporting requirements relating to systems intrusions under Rule 1002(b) such that all systems intrusions would be required to be immediately reported to the Commission pursuant to the requirements of Rule 1002(b). Currently, paragraph (b)(5) of Rule 1002 states that the Commission notification requirements under paragraphs (b)(1) through (4) do not apply to any SCI event that has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants ("de minimis SCI events").[335] Instead, SCI entities are currently required to make, keep and preserve records relating to all such SCI events, and provide a quarterly report of de minimis systems intrusions and systems disruptions pursuant to Rule 1002(b)(5).[336] The Commission is proposing to eliminate the de minimis exception's applicability to systems intrusions, thus requiring all systems intrusions, whether de minimis or non-de minimis, to be reported pursuant to the requirements of 17 CFR 242.1002(b)(1) through (4) ("Rule

---

335 Rule 1002(b)(5).

336 *Id.*

1002(b)(1) through (4)").[337] By their very nature, systems intrusions may be difficult to identify, and assessing the impact of any systems intrusion is often complex and could potentially require a lengthy investigation before any conclusions may be reached with any degree of certainty. Because of this, the Commission recognizes that it may be difficult for SCI entities to make a clear determination in a timely manner of whether a systems intrusion is de minimis. At the same time, the Commission believes that it is important for the Commission and its staff to receive notification of systems intrusions to be aware of potential and actual security threats to individual SCI entities, particularly given that such threats may extend to other market participants in the securities markets, including other SCI entities. Thus, the Commission believes it is appropriate to eliminate systems intrusions from the types of SCI events that may make use of the exception for de minimis SCI events and be quarterly reported, and instead require that each systems intrusion be reported under the framework in Rule 1002(b)(1) through (4).[338]

Rule 1002(c) sets forth the requirements with respect to disseminating information regarding SCI events to applicable members or participants of SCI entities,

---

337 To conform to the proposed elimination of de minimis systems intrusions from the quarterly report, Rule 1002(b)(5)(i) would be amended by replacing the phrase "all such SCI events" with the phrase "all such systems disruptions or systems compliance issues," and Rule 1002(b)(5)(ii) would be amended to no longer include references to systems intrusions and instead read: "Submit to the Commission a report, within 30 calendar days after the end of each calendar quarter, containing a summary description of such systems disruptions, including the SCI systems affected by such systems disruptions during the applicable calendar quarter."

338 The Commission notes that systems intrusions, as currently defined in Rule 1000 of Regulation SCI, have been relatively infrequent as compared to other types of SCI events, and thus the burden of this proposed change in reporting for systems intrusions under the current definition (which is the first prong of the proposed revised definition of systems intrusions) should be relatively low for SCI entities. For example, in the three-year period from 2019 to 2021, systems intrusions only accounted for 27 of the 10,501 SCI events in total (including both de minimis and non-de minimis SCI events). The Commission requests comment below regarding the frequency of systems intrusions as defined by the second and third prongs of the proposed revised definition of systems intrusion.

and the Commission believes that it would be appropriate that information about systems intrusions under the proposed second prong of the systems intrusion definition (a "cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system") be disseminated pursuant to Rule 1002(c)'s requirements. However, importantly, in contrast to the more detailed information dissemination requirements for SCI entities in paragraph (c)(1) of Rule 1002 for systems disruptions and systems compliance issues, in recognition of the more sensitive nature of systems intrusions (disclosure of which may alert threat actors of an existing or potential weakness in an SCI entity's systems, or alert them of an ongoing investigation of a systems intrusion), the Commission's information dissemination requirements for systems intrusions contained in paragraph (c)(2) of Rule 1002 only requires SCI entities to provide a "summary description" for such events.[339] In addition, paragraph (c)(2) also permits an SCI entity to delay disclosure of a systems intrusion in cases where the SCI entity "determines that dissemination of such information would likely compromise the security of the SCI entity's SCI systems or indirect SCI systems, or an investigation of the systems intrusion, and documents the reasons for such determination."[340]

With respect to information dissemination to an SCI entity's members or participants, however, the Commission believes that information regarding significant attempted unauthorized entries should not be required to be disseminated to an SCI entity's members or participants, as any benefits associated with disseminating

---

339 The information dissemination requirements described here for systems intrusions differ from the analogous requirements for the other two types of SCI events (systems disruptions and systems compliance issues), which require SCI entities to also, among other things, further provide a more detailed description of such SCI events when known. *See* 17 CFR 242.1002(c)(1).

340 *See* 17 CFR 242.1002(c)(2) ("Rule 1002(c)(2)").

information about unsuccessful attempted unauthorized entries to members or participants of an SCI entity would likely not be justified due to distractions that such information would bring, particularly since the SCI entity's security controls were able, in fact, to repel the cybersecurity event. In addition, disseminating information regarding unsuccessful intrusions could result in the threat actors being unnecessarily alerted that they have been detected, which could make it more difficult to identify the attackers and halt their efforts on an ongoing, more permanent basis. Thus, the Commission is proposing to new 17 CFR 242.1002(c)(4)(iii) ("proposed Rule 1002(c)(4)(iii)") which would exclude systems intrusions that are significant attempted unauthorized entries into the SCI systems or indirect SCI systems of an SCI entity from the information dissemination requirements of 17 CFR 242.1002(c)(1) through (3) ("Rule 1002(c)(1) through (3)").

**d. Request for Comment**

67. Do commenters agree that cybersecurity is an area that the Commission should enhance as part of Regulation SCI? Is it necessary to help ensure that SCI entities maintain a robust technology infrastructure for the SCI systems and indirect SCI systems? Why or why not?
68. Do commenters agree with the proposed addition of Rule 1001(a)(2)(x), to enumerate that the policies and procedures of SCI entities shall include a program to prevent the unauthorized access to SCI systems and, for purposes of security standards, indirect SCI systems, and information residing therein? Why or why not?
69. Do commenters agree that SCI entities should be required to have an increased frequency of penetration test reviews? Why or why not? Do commenters feel that the requirement to have such tests at least annually is appropriate? How frequently do

SCI entities conduct penetration testing today? Do commenters agree with the proposed requirement that the penetration testing include testing of any identified vulnerabilities? Why or why not?

70. Do commenters believe that it is appropriate to modify the definition of systems intrusion as proposed in Rule 1000? Do commenters believe that it would be useful (for example, for SCI entities and the Commission and its staff) to include other types of scenarios in the definition of systems intrusion? If so, which scenarios should be included and why? If not, why not?

71. Do commenters agree with the proposed revisions to the definition of systems intrusions to include the second prong, (*i.e.*, for any cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system)? Why or why not? Could such events put the security or operational capability of an SCI system at risk? How frequently do commenters believe systems intrusions, as defined by the proposed second prong, occur at SCI entities? The Commission does not define the term "cybersecurity event" in the proposed rule text but, as noted, believes it would generally be understood to mean "an unauthorized activity that disrupts or significantly degrades the normal operation of an SCI system." Do commenters agree? Do commenters believe it is necessary to provide a definition of the term "cybersecurity event" in the proposed rule text? If so, do commenters agree with the meaning above? If not, how should it be defined? Please be specific.

72. Do commenters believe that significant attempted unauthorized entries into the SCI systems or indirect SCI systems of an SCI entity should be included in the definition of systems intrusions, as under the proposed third prong? Why or why not? Do

commenters believe that the Commission should define the term "significant attempted unauthorized entry," or do commenters believe it is appropriate to require an SCI entity to establish reasonable written criteria to make such determinations to provide SCI entities some degree of discretion and flexibility in determining what constitutes a significant attempted unauthorized entry for its purposes, given differences as between SCI? What types of criteria or scenarios do commenters believe should constitute a significant attempted unauthorized entry? Please describe and be specific. How frequently do commenters believe systems intrusions, as defined by the proposed third prong, occur at SCI entities?

73. Do commenters agree with the proposed removal of systems intrusions from the types of de minimis SCI events permitted to be reported quarterly under Rule 1002(b)(5)? Why or why not? Should there be a requirement that SCI events that are systems intrusions, as proposed to be defined, be reported to senior management of an SCI entity? Why or why not?

74. Do commenters agree with proposed addition of Rule 1002(c)(4)(iii), which would exclude systems intrusions that are significant attempted unauthorized entries from the information dissemination requirements of Rule 1002(c)(1) through (3)? Why or why not?

#### 4. SCI Review

##### a. Discussion

Rule 1000 currently defines the SCI review to be a review, following established procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems, and which review contains: (a) a risk assessment with respect to such systems of an SCI entity; and

(b) an assessment of internal control design and effectiveness of its SCI systems and indirect SCI systems to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards. Paragraph (b)(1) of Rule 1003 requires each SCI entity to conduct an SCI review of the SCI entity's compliance with Regulation SCI not less than once each calendar year; however, penetration test reviews of the network, firewalls, and production systems may be conducted at a frequency of not less than once every three years, and assessments of SCI systems directly supporting market regulation or market surveillance may be conducted at a frequency based upon the risk assessment conducted as part of the SCI review, but in no case less than once every three years. Paragraph (b)(2) of Rule 1003 requires SCI entities to submit a report of the SCI review to senior management of the SCI entity for review no more than 30 calendar days after completion of such SCI review, and paragraph (b)(3) requires SCI entities to submit to the Commission, and to the board of directors of the SCI entity or the equivalent of such board, a report of the SCI review, together with any response by senior management, within 60 calendar days after its submission to senior management of the SCI entity.

The SCI review is an important part of Regulation SCI because it is a periodic evaluation by objective personnel of an SCI entity's compliance with SCI and helps the SCI entity to identify weaknesses and vulnerabilities in its systems and controls. In addition, because of Rule 1003(b)'s reporting requirements, the SCI review and the report of the SCI review helps to ensure that the senior management and board of the SCI entity are involved in and aware of the SCI entity's compliance with the regulation. Finally, the report provides the Commission and its staff insight into the SCI entity's compliance with

Regulation SCI as well and assists the staff in determining how to follow up with the SCI entity in reviewing and addressing any identified weaknesses and vulnerabilities.

The SCI review is currently required to be conducted by "objective personnel," and the Commission believes that this requirement continues to be appropriate. Thus, as the Commission discussed in the SCI Adopting Release, SCI reviews may be performed by personnel of the SCI entity (such as internal audit function) or an external firm, provided that such personnel are, in fact, objective and, as required by rule, have the appropriate experience to conduct reviews of SCI systems and indirect SCI systems.[341]

As described below, the Commission is proposing a number of revisions to the requirements relating to SCI reviews and for the reports SCI entities submit (both to their board of directors as well as to the Commission).[342] The definition of SCI review in Rule 1000 is proposed to be amended to contain the substantive requirements for an SCI review, which would be required to be "a review, following established and documented procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems…" The revised definition of SCI review in Rule 1000 would go on to detail what an SCI review would

---

341 *See* SCI Adopting Release, *supra* note 1, at 72343. The Commission continues to believe that persons who were not involved in the process for development, testing, and implementation of the systems being reviewed would generally be in a better position to identify weaknesses and deficiencies that were not identified in the development, testing, and implementation stages. Thus, any personnel with conflicts of interest that have not been adequately mitigated to allow for objectivity should be excluded from serving in this role, and a person or persons conducting an SCI review should not have a conflict of interest that interferes with their ability to exercise judgment, express opinions, and present recommendations with impartiality. *See id.*

342 Rule 1000 (definition of SCI review) and Rule 1003(b) both currently contain requirements relating to SCI reviews. As described in this section, the Commission is proposing to focus the definition of SCI review in Rule 1000 on requirements relating to the SCI review itself, whereas Rule 1003(b)'s proposed language would be focused on the required contents of the report of the SCI review, as well as the timelines for when the SCI review is required to be conducted and when the report of the SCI review is required to be provided to senior management and the Commission.

be required to include and would require the use of appropriate risk management methodology. Specifically, paragraph (1) of the definition would require, with respect to each SCI system and indirect SCI system of the SCI entity, three assessments to be performed by objective personnel conducting the SCI review. The first required assessment would be of the risks related to the capacity, integrity, resiliency, availability, and security. The second assessment would be of internal control design and operating effectiveness to include logical and physical security controls, development processes, systems capacity and availability, information technology service continuity, and information technology governance, consistent with industry standards. The third assessment would be of third-party provider management risks and controls. As discussed above, the Commission is also proposing to update the requirement for penetration testing, from the current requirement of at least once every three years to at least annually.[343] Finally, the definition of SCI review in Rule 1000 would provide that assessments of SCI systems directly supporting market regulation or market surveillance would be required to be conducted at a frequency based upon the risk assessment conducted as part of the SCI review, but in no case less than once every three years.

It has been the experience of the Commission and its staff that the SCI reviews and their reports of such SCI reviews vary among SCI entities in content and detail. To help ensure that every SCI review and report of such reviews contain the assessments and related information the Commission and its staff believes is necessary for an SCI entity to be able to assess its compliance with Regulation SCI, the Commission proposes adding certain additional requirements and details with respect to each SCI review and the report

---

[343] *See supra* section III.C.3.b (discussing the frequency of required penetration test reviews).

of the SCI review that are submitted to the SCI entity's board and to the Commission. In the lead-in provision for the definition, the words "and documented" are proposed to be added to ensure that SCI entities and the objective personnel conducting SCI reviews document the work that is done during the SCI review. Documentation is necessary as evidence that the requirements relating to the SCI review are being complied with, and would help ensure that policies and procedures are followed. Documentation is also critical to any follow-on reviews of the work that may be required, such as follow-up on the work of the SCI review by SCI entity personnel (including by its senior management or board of directors) or by the Commission or its staff. In addition, such documentation would facilitate follow-up required to address deficiencies and weaknesses that may be identified during the SCI review, such as through mitigation and remediation plans.

The proposed definition of SCI review would also require that the SCI review use "appropriate risk management methodology." The objective personnel conducting the SCI review would be required to establish, document, and utilize a given risk methodology in conducting the SCI review that is appropriate for the SCI entity being reviewed. The Commission is not specifying a particular methodology that a given SCI entity and its objective personnel must use, but rather is providing the flexibility to such objective personnel to determine the risk management methodology that should be utilized, so long as it is appropriate given the SCI entity's characteristics and risks.

The requirements of the SCI review would apply to each individual SCI system and indirect SCI system, and would require that the SCI review include three specific assessments to be performed by objective personnel. This language is intended to require that each of these assessments be performed by objective personnel –either by those

conducting the SCI review or others that those conducting the SCI review engage for such purposes– rather than utilizing, for example, enterprise or IT risk assessments as the basis for the SCI review after deeming them "reasonable." The proposed requirement would not specify a particular control framework to be applied for such assessments, but rather would provide flexibility to those conducting the SCI review to choose the methodology they believe to be most appropriate given the particular characteristics and risks of the SCI entity's systems being assessed, and undertake the assessments themselves, or oversee and direct other objective personnel on how the assessments should be performed. The Commission considers the SCI reviews to be an important window into the strength of the technological infrastructure of SCI entities, and whether the controls implemented by the SCI entity are appropriate and employed properly. In addition, the Commission requires that objective personnel be used to help ensure the impartiality of the review and that the reviewers examine what they believe to be most appropriate for such a review.[344] The Commission believes that, by requiring that these assessments be performed by objective personnel, these assessments and tests will be able to provide the SCI entity, its senior management, its board of directors, and the Commission, an appropriately impartial and accurate assessment of the risks associated with the SCI entity's SCI systems and indirect SCI systems.

In the definition of SCI review in Rule 1000, the phrase "a risk assessment with respect to such systems of an SCI entity" would be replaced with an assessment of "the risks related to the capacity, integrity, resiliency, availability, and security" of each such system. The Commission believes that the additional detail in the proposed language

---

[344] *See supra* note 341 and accompanying text (discussing "objective personnel").

would tie the required risk assessment more closely with the key principles of Regulation SCI (found in Rule 1001(a)(1)) relating to the "capacity, integrity, resiliency, availability and security" of each SCI entity's systems, while maintaining the focus of the assessment on the overall risks associated with such systems.

Further, in the definition of SCI review he phrase "internal control design and effectiveness" would be revised to read "internal control design and operating effectiveness" to clarify that the associated assessment must examine how well the internal controls performed in actual operations, *i.e.*, in practice. Thus, this assessment would look not only at how the controls worked in theory (*i.e.*, as designed), but also in practice (*i.e.*, in operations).[345] In addition, the definition of SCI review in Rule 1000 would expand on the list of controls to be assessed, adding "systems capacity and availability" and "information technology service continuity" to the current list of "logical and physical security controls, development processes, and information technology governance." The Commission believes that systems capacity and availability and information technology service continuity are important areas for SCI entities to consider when conducting their SCI reviews, and is proposing to include them on the list of controls reviewed by objective personnel performing the SCI reviews to ensure that these additional areas of controls are assessed during each SCI review. As stated above,

---

345 *See, e.g.*, Sunil Bakshi, *Tips for Effective Control Design*, ISACA (Feb. 9, 2022), *available at* https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-6/tips-for-effective-control-design; PCAOB, *AS2201: An Audit of Internal Controls Over Financial Reporting That is Integrated with An Audit of Financial Statements*, *available at* https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201; and AICPA, AU-C Section 94), *An Audit of Internal Controls Over Financial Reporting That is Integrated With an Audit of Financial Statements*, *available at* https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/au-c-00940.pdf.

the foundational principles of Regulation SCI are set forth in Rule 1001 and require in part that each SCI entity establish, maintain, and enforce written policies and procedures reasonably designed to ensure that their SCI systems and, for purposes of security standards, indirect SCI 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.[346] The proposed addition of "systems capacity and availability" relates to this requirement with respect to "capacity" and "availability," and "information technology service continuity" relates to this requirement with respect to "resiliency" and "availability," and would require that objective personnel consider whether an SCI entity's internal controls have been designed and implemented in a manner to achieve these objectives of Regulation SCI, rather than only those currently enumerated regarding security, development processes, and governance.

New paragraph (1)(C) of the definition of SCI review in Rule 1000 would require an assessment of third-party provider management risks and controls with respect to each of its SCI systems and indirect SCI systems. As discussed in detail above,[347] third-party provider management is an important part of managing the risks posed when an SCI entity uses a third-party for functionality, support, or services.

Importantly, the proposed amended definition of SCI review under Rule 1000 uses the phrase "with respect to each" when referencing SCI systems and indirect SCI systems. This wording clarifies that the associated assessments are required to be made for each applicable system for each SCI review (*i.e.*, every year). Thus, the Commission

---

346 *See supra* note 39 and accompanying text.

347 *See supra* section III.C.2.

believes it to be appropriate to conduct these assessments for each and every SCI system or, as applicable, indirect SCI system annually, rather than, for example, rotating control testing across several years such that not all systems and/or relevant controls are tested each year. However, in adopting Regulation SCI, the Commission determined to allow assessments of SCI systems directly supporting market regulation or market surveillance to be conducted, based upon a risk-assessment, at least once every three years, rather than annually, and the Commission is not amending this provision.[348]

Proposed paragraph (2) would contain the requirement that penetration test reviews be performed by objective personnel, conducted at least once each year. As discussed above, the revised requirements relating to SCI reviews would change the frequency of required penetration testing provision (currently located in Rule 1003(b)(1) but proposed to be relocated to the definition of "SCI review" in Rule 1000) from "not less than once every three years" to at least annually with each SCI review, and require that they include testing of any identified vulnerabilities of its SCI systems and indirect SCI systems.[349] In addition, the language relating to the frequency of assessments of SCI systems directly supporting market regulation or market surveillance, proposed to be in paragraph (3), would remain unchanged.[350]

---

348 *See* 17 CFR 242.1003(b)(1)(ii).

349 *See supra* section III.C.3.b. and proposed paragraph (2) of the definition of SCI review in Rule 1000, (relating to cybersecurity revisions, including penetration testing). Of course, while SCI entities would be required to conduct penetration test reviews at least annually as part of the SCI review, nothing in the proposed rule would prevent them from conducting penetration testing more frequently if warranted.

350 As noted above, while the substance of the provision relating to the frequency of assessments of SCI systems directly supporting market regulation or market surveillance would remain unchanged, the provision would be moved from current Rule 1003(b)(1)(ii) to proposed paragraph (3) of the definition of SCI review in Rule 1000.

Proposed Rule 1003(b) would continue to include requirements relating to the timeframes for conducting the SCI review (unchanged at "not less than once each calendar year")[351] and submitting reports of the SCI review to senior management (unchanged at "no more than 30 calendar days after completion of such SCI review")[352] and the Commission (unchanged at "within 60 calendar days after its submission to senior management").[353] However, proposed Rule 1003(b)(1) would add the phrase "for each calendar year during which it was an SCI entity for any part of such calendar year" to clarify that, if an SCI entity is an SCI entity for any part of the calendar year, it must conduct the SCI review and submit the associated report of the SCI review to the SCI entity's senior management and board, as well as to the Commission. Thus, an SCI review would be required for a new SCI entity, even in its first year as an SCI entity and even if its starting date as an SCI entity were not until late in the year. Similarly, if an SCI entity ceased to be an SCI entity during the middle of a calendar year (*e.g.*, an SCI ATS that falls out of the SCI ATS thresholds in July of a given year), it would still be required to submit an SCI review for that portion of the calendar year during which it was an SCI entity. The Commission believes this is appropriate, as the SCI review and the report of the SCI review contain, among other things, assessments of the SCI entity's compliance with the requirements of Regulation SCI which help to confirm, through objective personnel, that the capacity, integrity, resiliency, availability and security

---

351 *See* proposed Rule 1003(b)(1).

352 *See* proposed Rule 1003(b)(2).

353 *See* proposed Rule 1003(b)(3).

requirements of Regulation SCI have been met by the entity for the period during which it was an SCI entity.

Rule 1003(b) would also add additional detail on what the report of the SCI review is required to contain. Currently, the rule does not provide any specific requirements with respect to the contents of the report of the SCI review. In the experience of Commission staff, this has resulted in a wide range in the types and quality of SCI reports the Commission receives from SCI entities. In reviewing the reports, the Commission staff has found certain information particularly important in assessing the SCI review, and as a result the Commission is now revising the rule to require this information to be included in all reports on SCI reviews. Rule 1003(b)(2) would be revised to require the report of the SCI review to include: (i) the dates the SCI review was conducted and the date of completion; (ii) the entity or business unit of the SCI entity performing the review; (iii) a list of the controls reviewed and a description of each such control; (iv) the findings of the SCI review with respect to each SCI system and indirect SCI system, which must include, at a minimum, assessments of: the risks related to the capacity, integrity, resiliency, availability, and security; internal control design and operating effectiveness; and vendor management risks and controls; (v) a summary, including the scope of testing and resulting action plan, of each penetration test review conducted as part of the SCI review; and (vi) a description of each deficiency and weakness identified by the SCI review.

Items (i) and (ii) contain basic administrative information (relating to dates and the entity/unit conducting the SCI review) about the SCI review to identify the period over which the SCI review was conducted and the entity/unit responsible for such review

that Commission staff may contact for any questions regarding the SCI review or the report of the SCI review. Item (iii), relating to controls reviewed as part of the SCI review, would assist Commission staff in understanding the scope of the review and, if applicable, also allow staff to identify and request additional information regarding any of the controls listed or any controls it believed to be missing. Item (iv) would contain the substantive findings of the SCI review and relate to the three assessments that are required to be part of the SCI review under paragraph (1) of the definition of SCI review in Rule 1000. Similarly, item (v) relates to paragraph (2) of the definition of SCI review relating to penetration test reviews and would require an SCI entity to provide a summary of each penetration test review conducted as part of the SCI review.[354] Item (v) also would require that the summary include the scope of testing and the resulting action plan. Item (vi) would require a description of each deficiency and weakness identified during the SCI review, including through the assessments and any testing conducted as part of the SCI review. This information is proposed to be included in the report of the SCI review to provide the senior management and board of the SCI entity, as well as the Commission and its staff, with information on the SCI review, including any deficiencies and weaknesses identified by the objective personnel that conducted the SCI review.

The Commission believes that requiring this minimum set of requirements for the report of the SCI review, as described above, would help ensure that SCI entities and the

---

354 The Commission notes that the proposed requirement under item (vi) would specify that a summary of each penetration test review be included but does not call for the penetration test review itself be included. The Commission believes that a summary that includes the scope of testing and action plan of the penetration test would provide Commission staff with sufficient initial information to obtain a broad understanding of what was tested and any vulnerabilities it identified and that Commission staff could, in any case, if it believed it appropriate, request that the SCI entity provide it with a copy of the penetration test review.

objective personnel that conduct the SCI review include in the report of the SCI review the key pieces of information relating to the SCI review (*i.e.*, information relating to the controls reviewed; substantive findings from the assessments conducted as part of the SCI review; summaries of penetration test reviews; and descriptions of each deficiency and weakness identified) that go towards ensuring that the SCI systems of SCI entities remain robust with respect to their capacity, integrity, resiliency, availability, and security, and are in compliance with the requirements of Regulation SCI.

Finally, the Commission is proposing several revisions to paragraph (b)(3) of Rule 1003, which relates to submission of the report of the SCI review to the Commission and to the board of directors (or its equivalent) of the SCI entity. First, because Rule 1003(b)(2) now contains details relating to the required contents of the report of the SCI review, the Commission is proposing to update the internal cross-reference in paragraph (b)(3) from "paragraph (b)(1)" to "paragraph (b)(2)." The proposed revisions would also require that, when the report is submitted to the board of directors of the SCI entity and the Commission, it must also include the date the report was submitted to senior management. In addition, the revisions would make mandatory that a response from senior management to the report is included when it is submitted to the Commission and board, whereas previously the language appeared permissive. The Commission believes that mandating a response from senior management will help ensure that both the SCI entity's senior management and board are informed of the findings in the report of the SCI review and that the SCI entity's policies and procedures are reasonably designed, as required by the rule, and as informed by the issues identified in the report.

### b. Request for Comment

75. Do commenters agree with the proposed revisions to the definition of "SCI review" in Rule 1000? Why or why not? Do commenters agree with the proposed addition of "and documented" to require that the work relating to the SCI review be documented? Why or why not? Do commenters agree with the proposed addition that the objective personnel conducting the SCI review use "appropriate risk management methodology?" Why or why not? What risk management methodologies do commenters believe would be appropriate for use by SCI entities? Please describe. Does the requirement that SCI reviews be performed by "objective personnel" remain appropriate? For example, should the term "objective personnel" be defined? Why or why not? Should there be a requirement that the SCI review be performed by an independent third party? Why or why not? Should there be a requirement that senior management certify that the SCI review was performed by objective personnel? Why or why not?

76. What are commenters' views on not specifying a particular control framework to be applied for the internal control assessments? What are the costs and benefits to SCI entities if the Commission required the application of, for example, a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment?

77. With respect to the three assessments proposed to be required by paragraph (1) of the definition of SCI review, do commenters agree that these assessments should be overseen by the objective personnel responsible for the SCI review, rather than utilizing, for example, enterprise or IT risk assessments as the basis for the SCI

review after deeming them "reasonable"? Why or why not? What is the current practice among objective personnel conducting assessments for SCI reviews? Please describe. What do commenters believe would be the advantages and disadvantages for this proposed requirement?

78. Do commenters believe that it is appropriate that the SCI review include an assessment of "the risks related to the capacity, integrity, resiliency, availability, and security," as proposed to be required in paragraph (1)(A) of the definition of SCI review under Rule 1000? Why or why not?
79. Do commenters believe that the revisions to the second assessment proposed to be required in paragraph (1)(A) of the definition of SCI review in Rule 1000 (replacing the phrase "internal control design and effectiveness" with "internal control design and operating effectiveness," and adding "systems capacity and availability" and "information technology service continuity" to the current list of controls to be assessed) are appropriate as part of the SCI review?" Why or why not?
80. Do commenters agree that the third assessment proposed to be required as part of the SCI review, relating to third-party provider management risks and controls, is appropriate? Why or why not?
81. Do commenters agree with the revision that the three assessments in paragraph (1) of the definition of SCI review be made "with respect to each" SCI system and indirect SCI system, thereby requiring that these assessments be made for each applicable system for each SCI review every year? Why or why not?
82. Do commenters agree that the SCI review and report of the SCI review should be conducted by an SCI entity "for each calendar year during which it was an SCI entity

for any part of such calendar year," as proposed to be added to Rule 1003(b)(1)? Why or why not?

83. Do commenters believe that the requirements in proposed Rule 1003(b)(2) are appropriate for the report of the SCI review? Why or why not? Do commenters believe additional requirements should be added or that any proposed requirements should be modified or not included? Why or why not? Please describe.

### 5. Current SCI Industry Standards

#### a. Overview of Current Rule 1001(a)(4)

Rule 1001(a)(4) of Regulation SCI states that, for purposes of paragraph (a) of Rule 1001, an SCI entity's policies and procedures will be deemed to be reasonably designed if they are consistent with "current SCI industry standards." The provision defines "current SCI industry standards" 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." In addition, Rule 1001(a)(4) also states that compliance with such current SCI industry standards shall not be the exclusive means to comply with the requirements of paragraph (a). Thus, Rule 1001(a)(4) provides a safe harbor for SCI entities to comply with Rule 1001(a) (*i.e.*, they will be deemed to comply if they have policies and procedures that are consistent with current SCI industry standards), while at the same time stating that following such current SCI industry standards is not the sole means of achieving compliance with the rule.

### b. Rule 1001(a)(4) Safe Harbor

The Commission believes that utilizing current SCI industry standards is an appropriate way for SCI entities to develop their Rule 1001(a) policies and procedures. It has been the experience of the Commission and its staff that some SCI entities look to publications issued by the federal government's National Institute of Standards and Technology ("NIST") *Framework for Improving Critical Infrastructure Cybersecurity* ("NIST Framework"),[355] or frameworks issued by non-governmental bodies such as the International Organization for Standardization ("ISO")[356] or the Control Objectives for Information and Related Technologies ("COBIT"),[357] and some SCI entities may not point to any specific industry standards at all. In addition, among those SCI entities that utilize industry standards, some may look to a single industry standard for most or all of their policies and procedures, while others may "mix and match" standards for different policies and procedures. And, in some cases, an SCI entity may utilize multiple industry standards for a single set of their policies and procedures.

---

355 The NIST Framework is *available at* https://www.nist.gov/cyberframework/framework.

356 ISO is an independent, non-governmental international organization whose members include national standards bodies that develops and publishes international standards. *See* International Organization for Standardization, *available at* https://www.iso.org.

357 COBIT is a leading framework for the enterprise governance of information and technology and is issued by ISACA, an international professional associated focused on information technology governance. *See* ISACA, *available at* https://www.isaca.org.

The Commission believes that use of industry standards continues to be an appropriate framework for SCI entities to model their policies and procedures.[358] To make clear that Rule 1001(a)(4)'s reference to and definition of "current SCI industry standards" provides a safe harbor for SCI entities with respect to their Rule 1001(a) policies and procedures, the Commission proposes to add the words "safe harbor" in Rule 1001(a)(4).[359]

**c. Identification of Current SCI Industry Standards Used**

In the experience of Commission staff, many SCI entities align their Rule 1001(a) policies and procedures, in part or whole, with current SCI industry standards, often referencing such standards in communications with Commission staff during inspections or examinations. However, some SCI entities do not reference any industry standard(s) for their Rule 1001(a) policies and procedures.

In conjunction with the proposed revision to Rule 1001(a)(4), the Commission is proposing to add a new requirement in Rule 1001(a)(2), which lays out certain minimum requirements for an SCI entity's Rule 1001(a) policies and procedures. Specifically, proposed new 17 CFR 242.1001(a)(2)(xi) ("proposed Rule 1001(a)(2)(xi)") would

---

358 We note that concurrent with the Commission's adoption of Regulation SCI in 2014, Commission staff stated its views regarding "current SCI industry standards," including a listing of examples of publications describing processes, guidelines, frameworks, or standards for each inspection area, or domain, an SCI entity could look to in developing its reasonably designed policies and procedures. *See* Commission, *Staff Guidance on Current SCI Industry Standards* (Nov. 19, 2014), *available at* https://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf. Commission staff is reviewing staff statements with respect to Regulation SCI to determine whether any such statements, or portion thereof, should be revised or withdrawn in connection with any adoption of this proposal. These statements include the Staff Guidance on Current SCI Industry Standards, as well as the Responses to Frequently Asked Questions Concerning Regulation SCI, Sept. 2, 2015 (Updated Aug. 21, 2019), *available at* https://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml.

359 Specifically, the second sentence of Rule 1001(a)(4) would be revised to read: "Compliance with such current SCI industry standards as a safe harbor, however, shall not be the exclusive means to comply with the requirements of paragraph (a) of this section."

require that an SCI entity's policies and procedures include "[a]n identification of the current SCI industry standard(s) with which each such policy and procedure is consistent, if any." SCI entities are not required to avail themselves of the safe harbor of Rule 1001(a)(4) by aligning their policies and procedures required by Rule 1001(a) with current SCI industry standards,[360] but for SCI entities that choose to do so, this proposed provision would require SCI entities to provide a list of the specific current SCI industry standard(s) with which each of its policies and procedures is consistent. Thus, for example, such SCI entities would be required to identify the standard(s) used for their business continuity and disaster recovery policies and procedures, and separately identify the standard(s) used for its vendor management policies and procedures.

In addition, the Commission recognizes that there may be cases in which an SCI entity may draw from multiple current SCI industry standards in developing a given policy and procedure, and proposed Rule 1001(a)(2)(xi) recognizes this may be the case ("…the current SCI industry *standard(s)*…"). In such cases, an SCI entity may simply list multiple standards with which the given policy and procedure is consistent.

**d. Request for Comment**

84. Do commenters agree with the proposed revisions to Rule 1001(a)(4) relating to current SCI industry standards? Why or why not?

85. Do SCI entities seek to make use of the safe harbor contained in Rule 1001(a)(4) for compliance with Rule 1001(a) of Regulation SCI? Why or why not? With what

---

[360] For SCI entities that do not seek to avail themselves of the safe harbor of Rule 1001(a)(4), the requirements of proposed Rule 1001(a)(2)(xi) would not apply.

current SCI industry standard(s) do SCI entities seek to make their policies and procedures consistent?

86. For an SCI entity that seeks to avail itself of the safe harbor, do commenters agree that an SCI entity should identify the current SCI industry standard(s) with which each of its policies and procedures is consistent? Why or why not?

### 6. Other Changes

Rule 1002(c) of Regulation SCI requires that SCI entities disseminate information to their members or participants regarding SCI events.[361] These information dissemination requirements are scaled based on the nature and severity of an event, with SCI entities required to disseminate certain information about the event to members or participants that the SCI entity reasonably estimated to have been affected by the SCI event, and, in the case of a major SCI event, to all members or participants.[362] In connection with the proposal to include SCI broker-dealers as SCI entities, the Commission proposes that an SCI broker-dealer be required to disseminate information about an SCI event it is experiencing, in accordance with the requirements of Rule 1002(c), to its "customers." As discussed above, the Commission proposes to include SCI broker-dealers as SCI entities because it believes that a systems issue at an SCI broker-dealer could, for example, impede the ability of other market participants to trade securities in a fair and orderly manner. As explained in the SCI Adopting Release, information about an SCI event is likely to be of greatest value to those market participants affected by it, who can use such information to evaluate the event's impact

---

[361] *See* 17 CFR 242.1002(c).

[362] *Id*. *See also supra* section II.B.3 (discussing current Rule 1002(c)).

on their trading and other activities and develop an appropriate response.[363] To the extent that an SCI event at a broker-dealer affects its customers (*i.e.*, those with whom it trades or for whom it facilitates trades as an agent), the Commission believes that the SCI broker-dealer should inform them, and do so in the same manner and as required for other SCI entities, pursuant to Rule 1002(c). Similarly, and consistent with the current requirement of Rule 1002(b)(4)(ii)(B), an SCI broker-dealer would be required to include in its notices to the Commission a copy of any information it disseminated to its customers.[364] The Commission requests comment on the proposed amendments to Rule 1002(b)(4)(ii)(B) and Rule 1002(c) in section III.A.2.b above, which discusses the proposed definition of an SCI broker-dealer.[365]

Rule 1005 of Regulation SCI requires SCI entities to make, keep, and preserve certain records related to their compliance with Regulation SCI.[366] Rule 1005(c) specifies that the recordkeeping period survives even if an SCI entity ceases to do business or ceases to be registered under the Exchange Act. The Commission proposes to add that this survival provision applies to an SCI entity "otherwise ceasing to be an SCI entity." This addition accounts for circumstances not expressly covered; specifically, those in which an SCI entity continues to do business or remains a registered entity, but may cease to qualify as an SCI entity, such as an SCI ATS that no longer satisfies a volume threshold. Such entities would not be excepted from complying with the recordkeeping

---

363 *See* SCI Adopting Release, *supra* note 1 at 72334.

364 *Id*. *See also supra* section II.B.3 (discussing current Rule 1002(b)(4).

365 *See supra* section III.A.2.b.

366 *See* 17 CFR 242.1005. Rule 1005(a) of Regulation SCI relates to recordkeeping provisions for SCI SROs, whereas Rule 1005(b) relates to the recordkeeping provision for SCI entities other than SCI SROs.

provisions of Rule 1005 and would be required to make, keep, and preserve their records related to their compliance with Regulation SCI related to the period during which they were an SCI entity.

In addition, Form SCI is proposed to be modified to conform the text of the General Instructions and description of the attached Exhibits to the other changes proposed herein. Specifically, the operational aspects of Form SCI filing are unchanged, except to reflect that quarterly reports of SCI events with no or a de minimis impact would pertain only to systems disruptions, and not to systems intrusions.[367] Furthermore, the instructions to Exhibit 5 of Form SCI is proposed to be modified to reflect the requirement that an SCI entity's senior management respond to the report of the SCI review.[368] In addition, the Commission proposes to update section I of the General Instructions for Form SCI: Explanation of Terms to reflect the proposed changes in the definitions in Rule 1000, by revising the definitions of SCI entity, SCI review, SCI systems, and Systems Intrusion.

### D. SCI Entities Subject to the Exchange Act Cybersecurity Proposal and/or Regulation S-P

#### 1. Discussion

##### a. Introduction

The Commission separately is proposing the Exchange Act Cybersecurity Proposal,[369] and separately is also proposing to amend Regulation S-P.[370] As discussed in

---

367 *See supra* section III.C.3.c (discussing proposed changes to Rule 1002(b)(5)(ii)).

368 *See supra* section III.C.4 (discussing proposed changes to Rule 1003(b)(3)).

369 *See* Exchange Act Cybersecurity Proposal, *supra* note 10.

370 *See* Regulation S-P 2023 Proposing Release *supra* note 10.

more detail below, certain types of SCI entities also are or would be subject to the Exchange Act Cybersecurity Proposal and/or Regulation S-P (currently and as it would be amended).[371] The Exchange Act Cybersecurity Proposal and Regulation S-P (currently and as it would be amended) have or would have provisions requiring policies and procedures that address certain types of cybersecurity risks.[372] The Exchange Act Cybersecurity Proposal also requires certain reporting to the Commission on Form SCIR of certain types of cybersecurity incidents.[373] These notification and subsequent reporting requirements of the Exchange Act Cybersecurity Proposal are triggered by a "significant cybersecurity incident,"[374] which could also be an SCI event such as a "systems intrusion" as that term would be defined in current and proposed Rule 1000 of Regulation SCI.[375] Finally, the Exchange Act Cybersecurity Proposal and Regulation S-P (currently and as it would be amended) have or would have provisions requiring disclosures of

---

371 *See* proposed 17 CFR 242.10 of the Exchange Act Cybersecurity Proposal Rule ("Rule 10"); 17 CFR 248.1 through 248.30 (Regulation S-P). *See also* section III.D.1.b. of this release (discussing the types of SCI Entities that are or would be subject to the Exchange Act Cybersecurity Proposal and/or Regulation S-P).

372 *See infra* section III.D.1.c (discussing the proposed requirements of the Exchange Act Cybersecurity Proposal and the existing and proposed requirements of Regulation S-P to have policies and procedures that address certain cybersecurity risks).

373 *See infra* section III.D.1.d (discussing the proposed Commission notification requirements of the Exchange Act Cybersecurity Proposal).

374 The Exchange Act Cybersecurity Proposal defines a "significant cybersecurity incident" to be a cybersecurity incident, or a group of related cybersecurity incidents, that: (i) Significantly disrupts or degrades the ability of the market entity to maintain critical operations; or (ii) Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in: (A) Substantial harm to the market entity; or (B) Substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other market participant that interacts with the market entity. *See* proposed § 242.10(a) of the Exchange Act Cybersecurity Proposal.

375 *See* current and proposed Rule 1000 of Regulation SCI (defining the term "systems intrusion").

certain cybersecurity incidents.[376] Consequently, if the proposed amendments to Regulation SCI and the other proposals are all adopted as proposed, SCI entities could be subject to requirements of that rule that relate to certain proposed requirements of the Exchange Act Cybersecurity Proposal and certain existing and proposed requirements of Regulation S-P. In the Commission's view, this would be appropriate because, while the current and proposed cybersecurity requirements of Regulation SCI may impose some broadly similar obligations, it has a different scope and purpose than the Exchange Act Cybersecurity Proposal and Regulation S-P. Moreover, in many instances, compliance with the current and proposed cybersecurity requirements of Regulation SCI that relate to the proposed requirements of the Exchange Act Cybersecurity Proposal and the existing or proposed requirements Regulation S-P can be accomplished through similar efforts.

The specific instances in which the cybersecurity requirements of current and proposed Regulation SCI would relate to the proposed requirements of the Exchange Act Cybersecurity Proposal and the existing or proposed requirements of Regulation S-P are discussed briefly below. The Commission encourages interested persons to provide comments on the discussion below, as well as on the potential application of Regulation SCI, the Exchange Act Cybersecurity Proposal, and Regulation S-P. More specifically, the Commission encourages commenters: (1) to identify any areas where they believe the relation between requirements of the existing or proposed requirements of Regulation SCI and the proposed requirements of the Exchange Act Cybersecurity Proposal and the existing or proposed requirements of Regulation S-P would be particularly costly or

---

[376] *See infra* section III.D.1.e (discussing the proposed disclosure requirements of the Exchange Act Cybersecurity Proposal and the existing and proposed disclosure requirements of Regulation S-P).

create practical implementation difficulties; (2) to provide details on why these instances would be particularly costly or create practical implementation difficulties; and (3) to make recommendations on how to minimize these potential impacts, while also achieving the goal of this proposal to address, among other things, the cybersecurity risks faced by SCI entities. To assist this effort, the Commission is seeking specific comment below on these topics.[377]

#### b. SCI Entities That Are Or Would be Subject to the Exchange Act Cybersecurity Proposal and/or Regulation S-P

Various SCI entities under this proposal are or would be subject to the Exchange Act Cybersecurity Proposal and/or Regulation S-P (currently and as it would be amended). In particular, most SCI entities under Regulation SCI (currently and as it would be amended) would be subject to the requirements of Exchange Act Cybersecurity Proposal. Specifically, all SCI entities other than plan processors and SCI competing consolidators that are or would be subject to Regulation SCI also would be subject to the Exchange Act Cybersecurity Proposal as "covered entities"[378] of that proposal. Therefore,

---

377 *See infra* section III.D.2.

378 The requirements of the Exchange Act Cybersecurity Proposal would apply to broker-dealers, clearing agencies, major security-based swap participants, the MSRB, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents. *See* proposed 17 CFR 240.10(a). The Commission believes that a broker-dealer that exceeds one or more of the transaction activity thresholds under the proposed amendments to Regulation SCI (*i.e.*, an SCI broker-dealer) likely would meet one of the broker-dealer definitions of "covered entity" in proposed Rule 10 of the Exchange Act Cybersecurity Proposal given their size and activities. For example, it would either be a carrying broker-dealer, have regulatory capital equal to or exceeding $50 million, have total assets equal to or exceeding $1 billion, or operate as a market maker. *See* paragraphs (a)(1)(i)(A), (C), (D), and (E) of proposed Rule 10. The Commission is seeking comment in the Exchange Act Cybersecurity Proposal as to

if the proposed amendments to Regulation SCI and the Exchange Act Cybersecurity Proposal are all adopted as proposed, these SCI entities would be subject to the requirements of Regulation SCI in addition to the requirements of the Exchange Act Cybersecurity Proposal.

In addition, broker-dealers that would be subject to Regulation SCI and those that operate certain ATSs currently subject to Regulation ATS (*i.e.*, as SCI ATSs or SCI broker-dealers) also are or would be subject to Regulation S-P (currently and as it would be amended).[379] Therefore, if the proposed amendments to Regulation SCI and Regulation S-P are all adopted as proposed, broker-dealers could be subject to Regulation SCI in addition to the requirements of Regulation S-P (currently and as it would be amended).

**c. Policies and Procedures to Address Cybersecurity Risks**

As discussed below, Regulation S-P currently has certain cybersecurity-related provisions. The Exchange Act Cybersecurity Proposal and the proposed amendments to Regulation S-P would add to these requirements. These existing and proposed requirements would relate to certain of the requirements of Regulation SCI (currently and as it would be amended). The Commission believes this result would be appropriate

---

whether a broker-dealer that is an SCI entity should be defined specifically as a "covered entity" under proposed Rule 10. *See* section II.A.10 of the Exchange Act Cybersecurity Proposal. In addition, the Commission requests comment in the Exchange Act Cybersecurity Proposal as to whether plan processors and SCI competing consolidators should be subject to its requirements. *See id*. The discussion in this section III.D focuses on the requirements of the Exchange Act Cybersecurity Proposal only as they would apply to current and proposed SCI entities.

379 Regulation S-P applies to additional types of market participants that are not or would not be subject to Regulation SCI. *See* 17 CFR 248.3. For example, with regard to the proposed inclusion of broker-dealers, Regulation SCI would only be applicable to an estimated 17 broker-dealers under the proposed definition of SCI broker-dealer. The discussion in this section III.D focuses on the current and proposed requirements of Regulation S-P only as they would apply to current and proposed SCI entities.

because the policies and procedures requirements of Regulation SCI (currently and as it would be amended) differ in scope and purpose from those of the Exchange Act Cybersecurity Proposal and Regulation S-P, and because the policies and procedures required under Regulation SCI that relate to cybersecurity (currently and as it would be amended) are generally consistent with the proposed requirements of the Exchange Act Cybersecurity Proposal and the existing and proposed requirements of Regulation S-P that pertain to cybersecurity.

#### i. Different Scope of the Policies and Procedures Requirements

As discussed above in sections II.B and III.C, Regulation SCI (currently and as it would be amended) limits its requirements to *SCI systems*, which are certain systems of the SCI entity that support specified securities market related functions,[380] and *indirect SCI systems*.[381] Therefore, the policies and procedures requirements of Regulation SCI (currently and as it would be amended) that pertain to cybersecurity apply to SCI systems and indirect SCI systems. They do not and would not apply to other systems maintained by an SCI entity.

Regulation S-P's safeguards provisions currently apply to *customer records and information*.[382] Regulation S-P defines "customer" to mean a consumer who has a customer relationship with the broker-dealer.[383] Regulation S-P further defines the term "consumer" to mean an individual who obtains or has obtained a financial product or

---

380 *See* 17 CFR 242.1000 (defining "SCI systems"). *See also supra* section II.B.1.

381 *See* 17 CFR 242.1000 (defining "indirect SCI systems"). *See also supra* section II.B.1.

382 *See* 17 CFR 248.30(a).

383 *See* 17 CFR 248.3(j).

service from the broker-dealer that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.[384] Regulation S-P's disposal provisions apply to *consumer report information* maintained for a business purpose.[385] Regulation S-P currently defines "consumer report information" to mean any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report and also a compilation of such records.[386] The Commission is separately proposing to amend the scope of information covered under both the Regulation S-P safeguards provisions and the Regulation S-P disposal provisions.[387] The amendments, however, would not fundamentally broaden the scope of these provisions. Therefore, the existing and proposed policies and procedures requirements of the Regulation S-P safeguards and disposal provisions that pertain to cybersecurity would apply to customer and consumer-related information. They do not and would not apply to other types of information stored on the information systems of the broker-dealer.[388]

Regulation SCI (currently and as it would be amended), the Exchange Act Cybersecurity Proposal, and Regulation S-P (currently and as it would be amended)

---

384 *See* 17 CFR 248.3(g)(1).

385 *See* 17 CFR 248.30(b)(2).

386 *See* 17 CFR 248.30(b)(1)(ii).

387 *See* Regulation S-P 2023 Proposing Release.

388 Additionally, Regulation S-P (currently and as it would be amended) implicates cybersecurity to the extent that customer records or information or consumer report information is stored on an information system (*e.g.*, on a computer). If this information is stored in paper form (*e.g.*, in a file cabinet), the requirements of Regulation S-P apply but the policies and procedures required under the rule would need to address risks that are different than cybersecurity risks—for example, the *physical security risk* that individuals could gain unauthorized access to the room or file cabinet where the paper records are stored as compared to the *cybersecurity risk* that individuals could gain unauthorized access to the information system on which the records are stored electronically.

would, therefore, differ in scope. The Exchange Act Cybersecurity Proposal would require covered entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.[389] Therefore, the Exchange Act Cybersecurity Proposal does not limit its application to certain systems or information residing on those systems based on the functions and operations performed by the covered entity through the system or the use of the information residing on the system unlike Regulation SCI (currently and as it would be amended). In addition, the Exchange Act Cybersecurity Proposal does not limit its application to a specific type of information residing on an information system unlike Regulation S-P (currently and as it would be amended).

#### ii. Consistency of the Policies and Procedures Requirements

The Commission also believes that it would be appropriate to apply Regulation SCI to SCI entities even if they also are subject to the requirements of the Exchange Act Cybersecurity Proposal and/or Regulation S-P (currently and as it would be amended) because an SCI entity could use one comprehensive set of policies and procedures to satisfy the requirements of the current and proposed cybersecurity-related policies and procedures requirements of Regulation SCI, the Exchange Act Cybersecurity Proposal, and Regulation S-P. As explained below, the more focused current and proposed policies and procedures requirements of Regulation SCI and Regulation S-P addressing certain cybersecurity risks would logically fit within and be consistent with the broader policies

---

389 *See* paragraphs (b) and (e) of proposed Rule 10 (setting forth the requirements of covered entities, among others, to have policies and procedures to address their cybersecurity risks).

and procedures required under the Exchange Act Cybersecurity Proposal to address all cybersecurity risks (including those outside of SCI systems and indirect SCI systems).

SCI entities that would be covered entities under the proposed requirements of the Exchange Act Cybersecurity Proposal would be subject the proposed policies and procedures requirements of the Exchange Act Cybersecurity Proposal. In addition, broker-dealers that would be subject to Regulation SCI and those that operate certain ATSs currently subject to Regulation ATS (*i.e.*, as SCI ATSs or SCI broker-dealers) are subject to the requirements of Regulation S-P (currently and as it would be amended).

*General Cybersecurity Policies and Procedures Requirements*. Regulation SCI, Regulation S-P, and the Exchange Act Cybersecurity Proposal all include requirements that address certain cybersecurity-related risks. Regulation SCI requires an SCI entity to have reasonably designed policies and procedures 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.[390]

Regulation S-P's safeguards provisions require broker-dealers to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[391] Additionally, Regulation S-P's disposal provisions require broker-dealers that maintain or otherwise possess consumer report information for a business purpose to properly dispose of the information by taking

---

390 *See* 17 CFR 242.1001(a)(1).

391 *See* 17 CFR 248.30(a).

reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.[392]

Rule 10 of the Exchange Act Cybersecurity Proposal would require a covered entity to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the covered entity's cybersecurity risks. These requirements are designed to position covered entities to be better prepared to protect themselves against cybersecurity risks, to mitigate cybersecurity threats and vulnerabilities, and to recover from cybersecurity incidents. They are also designed to help ensure that covered entities focus their efforts and resources on the cybersecurity risks associated with their operations and business practices.

A covered entity that implements reasonably designed policies and procedures in compliance with the requirements of the Exchange Act Cybersecurity Proposal that cover its SCI systems and indirect SCI systems should generally satisfy the current and proposed general policies and procedures requirements of Regulation SCI that pertain to cybersecurity.[393] Similarly, policies and procedures implemented by a broker-dealer that

---

392 *See* 17 CFR 248.30(b)(2). Regulation S-P currently defines the term "disposal" to mean: (1) the discarding or abandonment of consumer report information; or (2) the sale, donation, or transfer of any medium, including computer equipment, on which consumer report information is stored. *See* 17 CFR 248.30(b)(1)(iii).

393 The CAT System is a facility of each of the Participants and an SCI system. *See also Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, Securities Exchange Act Release No. 79318 (Nov. 15, 2016), 81 FR 84696, 84758 (Nov. 23, 2016) ("CAT NMS Plan Approval Order"). It would also qualify as an "information system" of each national securities exchange and each national securities association under the Exchange Act Cybersecurity Proposal. The CAT NMS Plan requires the CAT's Plan Processor to follow certain security protocols and industry standards, including the NIST Cyber Security Framework, subject to Participant oversight. *See, e.g.*, CAT NMS Plan at Appendix D, Section

is an SCI entity that are reasonably designed in compliance with the current and proposed cybersecurity requirements of Regulation SCI should generally satisfy the existing general policies and procedures requirements of Regulation S-P safeguards and disposal provisions discussed above that pertain to cybersecurity.

*Requirements to Oversee Service Providers*. Under the amendments to Regulation SCI, the policies and procedures required of SCI entities would need to include a program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for SCI systems and indirect SCI systems, and are discussed above in more detail in section III.C.2. In addition, proposed amendments to Regulation S-P's safeguards provisions would require broker-dealers to include written policies and procedures within their response programs that require their service providers, pursuant to a written contract, to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the broker-dealer in the event of any breach in security resulting in unauthorized access to a customer information maintained by the service provider to enable the broker-dealer to implement its response program.[394]

Proposed Rule 10 of the Exchange Act Cybersecurity Proposal would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks to these proposed amendments to Regulation SCI and

---

4.2. For the reasons discussed above and below with respect to SCI systems, the policies and procedures requirements of Regulation SCI are not intended to be inconsistent with the security protocols set forth in the CAT NMS Plan. Moreover, to the extent the CAT NMS Plan requires security protocols beyond those that would be required under Regulation SCI, those additional security protocols should generally fit within and be consistent with the policies and procedures required under the Exchange Act Cybersecurity Proposal to address all cybersecurity risks.

[394] *See* Regulation S-P 2023 Proposing Release.

Regulation S-P. First, a covered entity's policies and procedures under proposed Rule 10 would need to require periodic assessments of cybersecurity risks associated with the covered entity's information systems and information residing on those systems.[395] This element of the policies and procedures would need to include requirements that the covered entity identify its service providers that receive, maintain, or process information, or are otherwise permitted to access its information systems and any of its information residing on those systems, and assess the cybersecurity risks associated with its use of these service providers.[396] Second, under proposed Rule 10, a covered entity's policies and procedures would need to require oversight of service providers that receive, maintain, or process its information, or are otherwise permitted to access its information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider, and through that written contract the service providers would need to be required to implement and maintain appropriate measures that are designed to protect the covered entity's information systems and information residing on those systems.[397]

A covered entity that implements these requirements of proposed Rule 10 of the Exchange Act Cybersecurity Proposal with respect to its SCI systems and indirect SCI systems should generally satisfy the proposed requirements of Regulation SCI that the SCI entity's policies and procedures include a program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for SCI

---

395 *See* paragraph (b)(1)(i)(A) of proposed Rule 10; *see also* section II.B.1.a of the Exchange Act Cybersecurity Proposal (discussing this requirement in more detail).

396 *See* paragraph (b)(1)(i)(A)(*2*) of proposed Rule 10.

397 *See* paragraphs (b)(1)(iii)(B) of proposed Rule 10; *see also* section II.B.1.c. of this release (discussing this requirement in more detail).

systems and indirect SCI systems. Similarly, a broker-dealer that is an SCI entity that implements these requirements of Regulation SCI should generally comply with the proposed requirements of Regulation S-P's safeguards provisions relating to the oversight of service providers.

*Unauthorized Access Requirements*. Under the proposed amendments to Regulation SCI, SCI entities would be required to have a program to prevent the unauthorized access to their SCI systems and indirect SCI systems, and information residing therein, and are discussed above in more detail in section III.C.3.a. The proposed amendments to Regulation S-P's disposal provisions would require broker-dealers that maintain or otherwise possess consumer information or customer information for a business purpose to properly dispose of this information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.[398] The broker-dealer would be required to adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information in accordance with this standard.[399]

Proposed Rule 10 of the Exchange Act Cybersecurity Proposal would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks to these proposed requirements of Regulation SCI and the proposed disposal provisions of Regulation S-P. First, a covered entity's policies and

---

398 *See* Regulation S-P 2023 Proposing Release. As discussed above, the general policies and procedures requirements of Regulation S-P's safeguards provisions require the policies and procedures—among other things—to protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. *See* 17 CFR 248.30(a)(3).

399 *See* Regulation S-P 2023 Proposing Release.

procedures under proposed Rule 10 would need controls: (1) requiring standards of behavior for individuals authorized to access the covered entity's information systems and the information residing on those systems, such as an acceptable use policy; (2) identifying and authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification; (3) establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication; (4) restricting access to specific information systems of the covered entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the covered entity; and (5) securing remote access technologies.[400]

Second, under proposed Rule 10, a covered entity's policies and procedures would need to include measures designed to protect the covered entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the covered entity's information systems and the information that resides on the systems.[401] The periodic assessment would need to take into account: (1) the sensitivity level and importance of the information to the covered entity's business operations; (2) whether any of the information is personal information; (3) where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission; (4) the information systems'

---

400 *See* paragraphs (b)(1)(ii)(A) through (E) of proposed Rule 10; *see also* section II.B.1.b of the Exchange Act Cybersecurity Proposal (discussing these requirements in more detail).

401 *See* paragraph (b)(1)(iii)(A) of proposed Rule 10; *see also* section II.B.1.c. of the Exchange Act Cybersecurity Proposal (discussing these requirements in more detail).

access controls and malware protection; and (5) the potential effect a cybersecurity incident involving the information could have on the covered entity and its customers, counterparties, members, registrants, or users, including the potential to cause a significant cybersecurity incident.[402]

A covered entity that implements these requirements of proposed Rule 10 of the Exchange Act Cybersecurity Proposal with respect to its SCI systems and indirect SCI systems should generally satisfy the proposed requirements of Regulation SCI that the SCI entity's policies and procedures include a program to prevent the unauthorized access to their SCI systems and indirect SCI systems, and information residing therein. Similarly, a broker-dealer that is an SCI entity that implements these proposed requirements of Regulation SCI should generally satisfy the proposed requirements of Regulation S-P's disposal provisions to adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information.

*Review Requirements.* The current and proposed provisions of Regulation SCI prescribe certain elements that must be included in each SCI entity's policies and procedures relating to regular reviews and testing, penetration testing, and the SCI review, and are discussed above in more detail in sections II.B.2, II.B.4, III.C.3.b, and III.C.4.

Proposed Rule 10 of the Exchange Act Cybersecurity Proposal would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks to these existing and proposed requirements of Regulation

---

402 *See* paragraphs (b)(1)(iii)(A)(*1*) through (*5*) of proposed Rule 10.

SCI. First, a covered entity's policies and procedures under proposed Rule 10 would need to require periodic assessments of cybersecurity risks associated with the covered entity's information systems and information residing on those systems.[403] Moreover, this element of the policies and procedures would need to include requirements that the covered entity categorize and prioritize cybersecurity risks based on an inventory of the components of the covered entity's information systems and information residing on those systems and the potential effect of a cybersecurity incident on the covered entity.[404] Second, under proposed Rule 10, a covered entity's policies and procedures would need to require measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the covered entity's information systems and the information residing on those systems.[405]

A covered entity that implements these requirements of proposed Rule 10 with respect to its SCI systems and indirect SCI systems should generally satisfy the current requirements of Regulation SCI that the SCI entity's policies and procedures require regular reviews and testing of SCI systems and indirect SCI systems, including backup systems, to identify vulnerabilities from internal and external threats. Further, while proposed Rule 10 does not require penetration testing, the proposed rule requires measures designed to protect the covered entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the covered entity's information systems and the information that

---

403 *See* paragraph (b)(1)(i)(A) of proposed Rule 10; *see also* section II.B.1.a of the Exchange Act Cybersecurity Proposal (discussing this requirement in more detail).

404 *See* paragraph (b)(1)(i)(A)(*1*) of proposed Rule 10.

405 *See* paragraph (b)(1)(iv) of proposed Rule 10; *see also* section II.B.1.d of the Exchange Act Cybersecurity Proposal (discussing this requirement in more detail).

resides on the systems[406] and penetration testing could be part of these measures.[407] Therefore, the existing and proposed requirements of Regulation SCI requiring penetration testing could be incorporated into and should logically fit within a covered entity's policies and procedures to address cybersecurity risks under proposed Rule 10 of the Exchange Act Cybersecurity Proposal.

*Response Program*. Regulation SCI requires SCI entities to have policies and procedures to monitor its SCI systems and indirect SCI systems for SCI events, which include systems intrusions for unauthorized access, and also requires them to have policies and procedures that include escalation procedures to quickly inform responsible SCI personnel of potential SCI events, which are discussed above in more detail in section II.B.2.[408] The amendments to Regulation S-P's safeguards provisions would require the policies and procedures to include a response program for unauthorized access to or use of customer information. Further, the response program would need to be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including procedures, among others: (1) to assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization; and (2) to take appropriate steps

---

406 *See* paragraph (b)(1)(iii)(A) of proposed Rule 10.

407 *See also* section II.B.1.c of the Exchange Act Cybersecurity Proposal.

408 *See* paragraphs (a)(2)(vii) and (c)(1) of Rule 1001 of Regulation SCI, respectively. *See also* Rule 1002(a) of Regulation SCI and *supra* sections II.B.3 and III.C.3.c (discussing Regulation SCI's current and proposed requirements with respect to taking corrective action for SCI events, including systems intrusions).

to contain and control the incident to prevent further unauthorized access to or use of customer information.[409]

Proposed Rule 10 of the Exchange Act Cybersecurity Proposal would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks to these proposed requirements of Regulation SCI and the proposed requirements of the safeguards provisions of Regulation S-P. First, under proposed Rule 10, a covered entity's policies and procedures would need to have measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the covered entity's information systems and the information residing on those systems.[410] Second, under proposed Rule 10, a covered entity's policies and procedures would need to have measures designed to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure (among other things): (1) the continued operations of the covered entity; (2) the protection of the covered entity's information systems and the information residing on those systems; and (3) external and internal cybersecurity incident information sharing and communications.[411]

---

409 *See* Regulation S-P 2023 Proposing Release. The response program also would need to have procedures to notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. *See id.*

410 *See* paragraph (b)(1)(iv) of proposed Rule 10; *see also* section II.B.1.d of the Exchange Act Cybersecurity Proposal (discussing this requirement in more detail).

411 *See* paragraph (b)(1)(v) of proposed Rule 10; *see also* section II.B.1.e of the Exchange Act Cybersecurity Proposal (discussing this requirement in more detail).

A covered entity that implements reasonably designed policies and procedures in compliance with these requirements of proposed Rule 10 of the Exchange Act Cybersecurity Proposal should generally satisfy the current and proposed requirements of Regulation SCI and Regulation S-P's safeguards provisions relating to response programs for unauthorized access.

**d. Commission Notification**

As discussed above in sections II.B.3 and III.C.3.c, Regulation SCI (currently and as it would be amended) provides the framework for notifying the Commission of SCI events including, among other things, requirements to: notify the Commission of the event immediately; provide a written notification on Form SCI within 24 hours that includes a description of the SCI event and the system(s) affected, with other information required to the extent available at the time; provide regular updates regarding the SCI event until the event is resolved; and submit a final detailed written report regarding the SCI event.[412] If proposed Rule 10 of the Exchange Act Cybersecurity Proposal is adopted as proposed, it would establish a framework for covered entities to provide the Commission (and other regulators, if applicable) with immediate written electronic notice of a significant cybersecurity incident affecting the covered entity and, thereafter, report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission (and other regulators, if applicable).[413] Part I

---

412 *See* 17 CFR 242.1002(b); *supra* sections II.B.2 and III.C.3.c (discussing Regulation SCI's current and proposed requirements relating to SCI events, which include systems intrusions, and Commission notification for SCI events).

413 *See* paragraphs (c)(1) and (2) of proposed Rule 10 (requiring covered entities to provide immediate written notice and subsequent reporting on Part I of proposed Form SCIR of significant cybersecurity incidents); and sections II.B.2. and II.B.4. of the Exchange Act Cybersecurity Proposal (discussing the requirements of paragraphs (c)(1) and (2) of proposed Rule 10 and Part I of Form SCIR in more detail).

of proposed of Form SCIR would elicit information about the significant cybersecurity incident and the covered entity's efforts to respond to, and recover from, the incident.

Consequently, an SCI entity that is also a covered entity under the Exchange Act Cybersecurity Proposal that experiences a systems intrusion under Regulation SCI that also is a significant cybersecurity incident under proposed Rule 10 would be required to make two filings for the single incident: one on Form SCI and the other on Part I of proposed Form SCIR. The SCI entity also would be required to make additional filings on Forms SCI and SCIR pertaining to the systems intrusion (*i.e.*, to provide updates and final reports). The Commission believes the approach of having two separate notification and reporting programs—one under Regulation SCI and the other under proposed Rule 10 of the Exchange Act Cybersecurity Proposal—would be appropriate for the following reasons.

As discussed earlier, most broker-dealers would not be SCI entities under the current and proposed requirements of Regulation SCI.[414] Certain of the broker-dealers that are not SCI entities (currently and as it would be amended) would be covered entities under the Exchange Act Cybersecurity Proposal, as would other types of entities.[415] In addition, the current and proposed reporting requirements of Regulation SCI are or would be triggered by events impacting *SCI systems* and *indirect SCI systems*. In addition to SCI systems and indirect SCI systems, covered entities that are or would be SCI entities use and rely on information systems that are not SCI systems or indirect SCI systems under the current and proposed amendments to Regulation SCI. For these reasons, covered

---

414 *See* section II.F.1.b of the Exchange Act Cybersecurity Proposal.

415 *See* paragraphs (a)(1)(i)(A) and (F) of proposed Rule 10 (defining the categories of broker-dealers that would be covered entities); *see also supra* note 378.

entities under the Exchange Act Cybersecurity Proposal could be impacted by significant cybersecurity incidents that do not trigger the current and proposed notification requirements of Regulation SCI either because they do not meet the current or proposed definitions of "SCI entity" or because the significant cybersecurity incident does not meet the current or proposed definitions of "SCI event."

The objective of notification and reporting requirements of proposed Rule 10 of the Exchange Act Cybersecurity Proposal is to improve the Commission's ability to monitor and respond to significant cybersecurity incidents and use the information reported about them to better understand how they can be avoided or mitigated.[416] For this reason, Part I of proposed Form SCIR is tailored to elicit information relating specifically to cybersecurity, such as information relating to the threat actor, and the impact of the incident on any data or personal information that may have been accessed.[417] The Commission and its staff could use the information reported on Part I of Form SCIR to monitor the U.S. securities markets and the covered entities that support those markets broadly from a cybersecurity perspective, including identifying cybersecurity threats and trends from a market-wide view. By requiring all covered entities to report information about a significant cybersecurity incident on a common form, the information obtained from these filings over time would create a comprehensive set of data of all significant cybersecurity incidents impacting covered entities that is based on these entities responding to the same check boxes and questions on the form. This would facilitate analysis of the data, including analysis across different

---

416 *See* section II.B.2.a of the Exchange Act Cybersecurity Proposal.

417 *See* section II.B.2.b of the Exchange Act Cybersecurity Proposal.

covered entities and significant cybersecurity incidents. Eventually, this set of data and the ability to analyze it by searching and sorting how different covered entities responded to the same questions on the form could be used to spot common trending risks and vulnerabilities as well as best practices employed by covered entities to respond to and recover from significant cybersecurity incidents.[418]

The current and proposed definitions of "SCI event" include not only cybersecurity events, but also events that are not related to significant cybersecurity incidents under the Exchange Act Cybersecurity Proposal.[419] For example, under the current and proposed requirements of Regulation SCI, the definition of "SCI event" includes "systems disruptions," which are events in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system.[420] Therefore, the definitions are not limited to events in an SCI entity's SCI systems that disrupt, or significantly degrade, the normal operation of an SCI system *caused by a significant cybersecurity incident*. The information elicited in Form SCI reflects the broader scope of the reporting requirements of Regulation SCI (as compared to the narrower focus of proposed Rule 10 on reporting about significant cybersecurity incidents). For example, Form SCI requires the SCI entity to identify the type of SCI event: systems compliance

---

418 FSOC has found that "[s]haring timely and actionable cybersecurity information can reduce the risk that cybersecurity incidents occur and can mitigate the impacts of those that do occur." FSOC, *Annual Report (2021)*, *available at* https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf ("FSOC 2021 Annual Report").

419 *See* 17 CFR 242.1000 (defining the term "SCI event"); *see also supra* sections II.B.3 and III.C.3.c (discussion the current and proposed requirements relating to SCI events, including systems intrusions).

420 *See* 17 CFR 242.1000 (defining the term "system disruption" and including that term in the definition of "SCI event").

issue, systems disruption, and/or systems intrusion. In addition, Form SCI is tailored to elicit information specifically about SCI systems. For example, the form requires the SCI entity to indicate whether the type of SCI system impacted by the SCI event directly supports: (1) trading; (2) clearance and settlement; (3) order routing; (4) market data; (5) market regulation; and/or (6) market surveillance. If the impacted system is a critical SCI system, the SCI entity must indicate whether it directly supports functionality relating to: (1) clearance and settlement systems of clearing agencies; (2) openings, reopenings, and closings on the primary listing market; (3) trading halts; (4) initial public offerings; (5) the provision of consolidated market data; and/or (6) exclusively listed securities. The form also requires the SCI entity to indicate if the systems that provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.

**e. Information Dissemination and Disclosure**

As discussed above in sections II.B.3 and III.C.3.c, Regulation SCI (currently and as it would be amended) would require that SCI entities disseminate information to their members, participants, or customers (as applicable) regarding SCI events, including systems intrusions.[421] The proposed amendments to Regulation S-P would require broker-dealers to notify affected individuals whose sensitive customer information was,

---

[421] *See* 17 CFR 242.1002(c).

or is reasonably likely to have been, accessed or used without authorization.[422] Proposed Rule 10 of the Exchange Act Cybersecurity Proposal would require a covered entity to make two types of public disclosures relating to cybersecurity on Part II of proposed Form SCIR.[423] Covered entities would be required to make the disclosures by filing Part II of proposed Form SCIR on the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system and posting a copy of the filing on their business websites.[424] In addition, a covered entity that is either a carrying or introducing broker-dealer would be required to provide a copy of the most recently filed Part II of Form SCIR to a customer as part of the account opening process. Thereafter, the carrying or introducing broker-dealer would need to provide the customer with the most recently filed form annually. The copies of the form would need to be provided to the customer using the same means that the customer elects to receive account statements (*e.g.*, by email or through the postal service). Finally, a covered entity would be required to make updated disclosures promptly through each of the methods described above (as applicable) if the information required to be disclosed about cybersecurity risk or significant cybersecurity incidents materially changes, including, in the case of the disclosure about significant cybersecurity incidents, after the occurrence of a new significant cybersecurity incident or when

---

422 However, disclosure under proposed Regulation S-P would not be required if "a covered institution has determined, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience." *See* Regulation S-P 2023 Proposing Release. The proposed amendments to Regulation S-P would define "sensitive customer information" to mean any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. *Id.* The proposed amendments would provide example of sensitive customer information. *Id.*

423 *See* paragraph (d)(1) of proposed Rule 10.

424 *See* section II.B.3.b (discussing these proposed requirements in more detail).

information about a previously disclosed significant cybersecurity incident materially changes.

Consequently, a covered entity would, if it experiences a "significant cybersecurity incident," be required to make updated disclosures under proposed Rule 10 by filing Part II of proposed Form SCIR on EDGAR, posting a copy of the form on its business website, and, in the case of a carrying or introducing broker-dealer, by sending the disclosure to its customers using the same means that the customer elects to receive account statements. Thus, if an SCI entity is a covered entity under the Exchange Act Cybersecurity Proposal and if the SCI event would be a significant cybersecurity incident under the Exchange Act Cybersecurity Proposal, the SCI entity also could be required to disseminate certain information about the SCI event to certain of its members, participants, or customers (as applicable). Further, if the SCI entity is a broker-dealer and, therefore, subject to Regulation S-P (as it is proposed to be amended), the broker-dealer also could be required to notify individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.

However, the Commission believes that this result would be appropriate. First, as discussed above, Regulation SCI (currently and as it would be amended), proposed Rule 10, and Regulation S-P (as proposed to be amended) require different types of information to be disclosed. Second, as discussed above, the disclosures, for the most part, would be made to different persons: (1) affected members,[425] participants, or customers (as applicable) of the SCI entity in the case of Regulation SCI; (2) the public at

---

425 Information regarding major SCI events would be required to be disseminated by an SCI entity to all of its members, participants, or customers (as applicable). *See* current and proposed Rule 1002(c)(3) of Regulation SCI.

large in the case of proposed Rule 10 of the Exchange Act Cybersecurity Proposal;[426] and (3) affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization or, in some cases, all individuals whose information resides in the customer information system that was accessed or used without authorization in the case of Regulation S-P (as proposed to be amended).[427] For these reasons, the Commission believes it would be appropriate to apply these current and proposed requirements of Regulation SCI to SCI entities even if they would be subject to the disclosure requirements of proposed Rule 10 of the Exchange Act Cybersecurity Proposal and/or Regulation S-P (as proposed to be amended).

### 2. Request for Comment

The Commission requests comment on the relation between the requirements of Regulation SCI (as it currently exists and as it is proposed to be amended), proposed Rule 10, and Regulation S-P (as it currently exists and as it is proposed to be amended). In addition, the Commission is requesting comment on the following matters:

87. Should the policies and procedures requirements of current and proposed Regulation SCI regarding cybersecurity be modified to address SCI entities that also would be subject to proposed Rule 10 of the Exchange Act Cybersecurity Proposal and/or the existing and proposed requirements of Regulation S-P? For example, would it be

---

426 A carrying broker-dealer would be required to make the disclosures to its customers as well through the means by which they receive account statements.

427 Under the Regulation SCI and Regulation S-P proposals, there could be circumstances in which a compromise involving sensitive customer information at a broker-dealer that is an SCI entity could result in two forms of notification being provided to customers for the same incident. In addition, under the Exchange Act Cybersecurity Proposal, the broker-dealer also may need to publicly disclose a summary description of the incident via EDGAR and the entity's business Internet website, and, in the case of an introducing or carrying broker-dealer, send a copy of the disclosure to its customers.

particularly costly or create practical implementation difficulties to apply the requirements of current and proposed Regulation SCI to have policies and procedures to address cybersecurity risks to SCI entities even if they also would be subject to requirements to have policies and procedures under proposed Rule 10 (if it is adopted) and/or Regulation S-P that address certain cybersecurity risks (currently and it they would be amended)? If so, explain why. If not, explain why not. Are there ways the policies and procedures requirements of current or proposed Regulation SCI regarding could be modified to minimize these potential impacts while achieving the separate goals of this proposal? If so, explain how and suggest specific modifications.

88. Should the Commission notification and reporting requirements of current and proposed Regulation SCI be modified to address SCI entities that also would be subject to the proposed requirements of Rule 10 of the Exchange Act Cybersecurity Proposal? For example, would it be particularly costly or create practical implementation difficulties to apply the Commission notification and reporting requirements of current and proposed Regulation SCI and Form SCI to SCI entities even if they also would be subject to immediate notification and subsequent reporting requirements under proposed Rule 10 of the Exchange Act Cybersecurity Proposal and Part I of proposed Form SCIR (if they are adopted)? If so, explain why. If not, explain why not. Are there ways the Commission notification and reporting requirements of current or proposed Regulation SCI and Form SCI could be modified to minimize these potential impacts while achieving the separate goals of this proposal? If so, explain how and suggest specific modifications. For example, should Form SCI be modified to include a section that incorporates the check boxes and

questions of Part I of Form SCIR so that a single form could be filed to meet the reporting requirements of Regulation SCI and proposed Rule 10? If so, explain why. If not, explain why not. Should the Commission modify the proposed Commission notification framework for systems intrusions that are also significant cybersecurity incidents under Rule 10? For example, should such systems intrusions be initially reported (i.e., immediately and for the 24-hour notification) on Form SCI, with subsequent reports exempted from Rule 1002(b)'s requirements if they are reported to the Commission on Form SCIR pursuant to the proposed requirements of Rule 10? Why or why not? Are there other ways Form SCI could be modified to combine the elements of Part I of Form SCIR? If so, explain how.

89. Should the disclosure requirements of proposed and current Regulation SCI be modified to address SCI entities that also would be subject to the proposed requirements of the Exchange Act Cybersecurity Proposal and the existing and proposed requirements of Regulation S-P? For example, would it be particularly costly or create practical implementation difficulties to apply the disclosure requirements of current and proposed Regulation SCI to SCI entities even if they also would be subject to the proposed Rule 10 and Part II of proposed form SCIR (if they are adopted) the current and proposed requirements of Regulation S-P? If so, explain why. If not, explain why not. Are there ways the disclosure requirements of Regulation SCI could be modified to minimize these potential impacts while achieving the separate goals of this proposal? If so, explain how and suggest specific modifications.

90. Would the addition of the requirements in the Exchange Act Cybersecurity Proposal—together with the current broker-dealer regulatory regime, including the Market Access Rule and other Commission and FINRA rules—be sufficient to reasonably ensure the operational capability of the technological systems of the proposed SCI broker-dealers? Why or why not? For example, are there any provisions of Regulation SCI that, if added to the Exchange Act Cybersecurity Proposal as it applies to broker-dealers, would help ensure the operational capability of the technological systems of the proposed SCI broker-dealers? Which provisions?

## IV. Paperwork Reduction Act

Certain provisions of the proposal would contain a new "collection of information" within the meaning of the Paperwork Reduction Act of 1995 ("PRA").[428] The Commission is submitting the proposed rule amendments to the Office of Management and Budget ("OMB") for review and approval in accordance with the PRA and its implementing regulations.[429] An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number.[430] The Commission is proposing to alter the 31 existing collections of information and apply such collections of information to new categories of respondents. The title for the collections of information is: Regulation Systems Compliance and Integrity (OMB control number 3235–0703). The burden estimates

---

428 *See* 44 U.S.C. 3501 *et seq.*

429 *See* 44 U.S.C. 3507; 5 CFR 1320.11.

430 *See* 5 CFR 1320.11(l).

contained in this section do not include any other possible costs or economic effects beyond the burdens required to be calculated for PRA purposes.

### A. Summary of Collections of Information

The proposed amendments to Regulation SCI create paperwork burdens under the PRA by (1) adding new categories of respondents to the 31 existing collections of information (across 7 rules) noted above and (2) modifying the requirements of 16 of those collections, as noted below. For entities that are already required to comply with Regulation SCI ("Current SCI Entities"), the proposed amendments would result in the modification of certain collections of information. Entities that would become subject to Regulation SCI as a result of the proposed amendments ("New SCI Entities") would be newly subject to the 31 existing collections of information, including the modifications.[431] The collections of information and applicable categories of new respondents are summarized (by rule) in the following table.[432]

---

431 *See infra* section IV.C (Respondents) for more information on Current SCI Entities and New SCI Entities.

432 Unless otherwise described, none of the existing information collections are being revised with new requirements.

| Collection of Information | Rule | Burden Description | Respondent Categories |
|---|---|---|---|
| Rule 1001 of Regulation SCI | Rule 1001(a) | Rule Description: Requirement to establish, maintain, and enforce written policies and procedures related to capacity, integrity, resiliency, availability, and security.<br><br>Revised Burden: ensure policies and procedures include a program to manage and oversee third-party providers that provide functionality, support or service for the SCI entity's SCI systems; inventory all SCI systems, include a program to prevent unauthorized access to SCI system access and the information residing therein, identify the SCI industry standard with which such policy and procedure is consistent, if any. | Current SCI Entities and New SCI Entities |
| | Rule 1001(b) | Rule Description: Requirement to establish, maintain, and enforce policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Exchange Act, rules and regulations thereunder, and the entity's rules and governing documents | New SCI Entities |
| | Rule 1001(c) | Rule Description: Establish, maintain, and enforce reasonably | New SCI Entities |

| | | | |
|---|---|---|---|
| | | designed written policies and procedures that include the criteria for identifying responsible SCI personnel, the designation and documentation of responsible SCI personnel, and escalation procedures to inform responsible SCI personnel of potential SCI events. | |
| Rule 1002 of Regulation SCI | Rule 1002(a) | Rule Description: Each SCI entity is required to take appropriate corrective action upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. | New SCI Entities |
| | Rule 1002(b) | Rule Description: Rules 1002(b)(1) through (4): Requirement that each SCI entity, upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, notify the Commission immediately of such SCI event and submit a written notification within 24 hours of responsible SCI personnel having a reasonable basis to conclude there was an SCI event. Periodic updates are required pertaining to the SCI event on either a regular basis or at such frequency requested by representatives of the Commission. An interim written notification is required if the SCI event is not closed within 30 | Current SCI Entities and New SCI Entities |

| | | | |
|---|---|---|---|
| | | days of its occurrence. A final notification is required to be submitted within five days of the resolution and closure of the SCI event.<br>Rule 1002(b)(5): For events that the SCI entity reasonably estimates would have no, or a de minimis impact on the SCI entity's operations or on market participants, submit a report within 30 days after the end of each calendar quarter containing a summary description of such systems disruptions and systems intrusions.<br>Revised burden: add (1) cybersecurity events that disrupt, or significantly degrade the normal operation of an SCI system, and (2) significant attempted unauthorized entries into SCI systems or indirect SCI systems, as determined by the SCI entity pursuant to established reasonable written criteria, to the definition of systems intrusions in Rule 1000, thus requiring that SCI entities provide notifications under Rule 1002(b)(1) through (4); eliminate the de minimis exception's applicability to systems intrusions, thus requiring all systems intrusions to be reported pursuant to Rule 1002(b)(1) through (4); | |

| | | | |
|---|---|---|---|
| | | require interim written notification to the Commission to include a copy of any information disseminated pursuant to Rule 1002(c) regarding the SCI event by SCI broker-dealers to their customers. | |
| | Rule 1002(c) | Rule Description: Requirements to disseminate certain information to members and participants concerning SCI events promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event has occurred. For major SCI events, information must be disseminated to all members and participants, and for SCI events that are not major, the information must be disseminated to members or participants that any responsible SCI personnel has reasonably estimated may have been affected by the SCI event. Revised burden: add cybersecurity events to the definition of systems intrusions in Rule 1000, thus making them SCI events and requiring that SCI entities provide notifications under Rule 1002(c)(2) for those additional SCI events; exclude systems intrusions that are significant attempted unauthorized entries into | Current SCI Entities and New SCI Entities |

| | | | |
|---|---|---|---|
| | | the SCI systems or indirect SCI systems of an SCI entity from information dissemination requirements; add that SCI broker-dealers would notify their customers (rather than members or participants). | |
| Rule 1003 of Regulation SCI | Rule 1003(a) | Rule Description: Submit quarterly report describing completed, ongoing, and planned material changes to SCI systems and the security of indirect SCI systems; establish reasonable written criteria to identify changes to SCI systems and the security of indirect SCI systems as material and report such changes in accordance with such criteria. Promptly submit a supplemental report notifying the Commission of a material error in or material omission from a previously submitted report. | New SCI Entities |
| | Rule 1003(b) | Rule Description: Requirement to conduct an SCI review of the SCI entity's compliance with Regulation SCI not less than once each calendar year; conduct penetration test reviews not less than once every three years. Revised burden: include certain additional requirements and information in SCI reviews, require the SCI review to be performed annually, and require a | Current SCI Entities and New SCI Entities |

| | | | |
|---|---|---|---|
| | | response by senior management be reported to the Commission. | |
| Rule 1004 of Regulation SCI | Rule 1004 | Rule Description: Establish standards to designate members and participants that are the minimum necessary for the maintenance of fair and orderly markets, designate members or participants and require their participation in testing of the BC/DR plans pursuant to such standards, and coordinate testing on an industry or sector-wide basis with other SCI entities.<br>Revised burden: require SCI entities to establish standards for designating certain third-party providers that are the minimum necessary for the maintenance of fair and orderly markets, and designate third-party providers for BC/DR testing pursuant to those standards. | Current SCI Entities and New SCI Entities |
| Rule 1005 of Regulation SCI | Rule 1005 | Rule Description: Requirement to make, keep, and preserve all documents relating to compliance with Regulation SCI.<br>Revised burden: Entities that "otherwise [cease] to be an SCI entity" are required to comply with the recordkeeping requirements in this section. | Current SCI Entities and New SCI Entities |

| | | | |
|---|---|---|---|
| Rule 1006 | Rule 1006 | Rule Description: Require submissions to the Commission pursuant to Regulation SCI to be made electronically on Form SCI. | New SCI Entities |
| Rule 1007 | Rule 1007 | Rule Description: Requirement that SCI entities make available records required to be filed or kept under Regulation SCI that are prepared or maintained by a service bureau or other recordkeeping service on behalf of the SCI entity. | New SCI Entities |

### B. Proposed Use of Information

The existing information collections and the proposed amendments are used as described below:

#### 1. Rule 1001 of Regulation SCI

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 their SCI systems and, for purposes of security standards, indirect SCI 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.[433] Rule 1001(a)(2) of Regulation SCI requires that, at a minimum, such policies and procedures include: current and future capacity planning; periodic stress testing; systems development and testing methodology; reviews and testing to identify vulnerabilities; business continuity and disaster recovery planning (inclusive of backup systems that are geographically diverse and designed to meet specified recovery time objectives);

[433] *See* 17 CFR 242.1001(a)(1).

standards for market data collection, processing, and dissemination; and monitoring to identify potential SCI events.[434] Rule 1001(a)(3) of Regulation SCI requires that SCI entities periodically review the effectiveness of these policies and procedures and take prompt action to remedy any deficiencies.[435] Rule 1001(a)(4) of Regulation SCI provides that an SCI entity's policies and procedures will be deemed to be reasonably designed if they are consistent with current SCI industry standards, which is defined 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;[436] however, Rule 1001(a)(4) of Regulation SCI also makes clear that compliance with such "current SCI industry standards" is not the exclusive means to comply with these requirements.

Rule 1001(b) of Regulation SCI requires each SCI entity to establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Exchange Act and the rules and regulations thereunder and the entity's rules and governing documents, as applicable, and specifies certain minimum requirements for such policies and procedures.[437] Rule 1001(c) of Regulation SCI requires SCI entities to establish, maintain, and enforce reasonably designed written policies and procedures that include the criteria for identifying responsible SCI personnel, the designation and documentation of responsible

---

434 *See* 17 CFR 242.1001(a)(2).

435 *See* 17 CFR 242.1001(a)(3).

436 *See* 17 CFR 242.1001(a)(4).

437 *See* 17 CFR 242.1001(b).

SCI personnel, and escalation procedures to quickly inform responsible SCI personnel of potential SCI events.[438]

The Commission is proposing revisions to Rule 1001(a)(2) and (4) of Regulation SCI to include four additional elements in the policies and procedures: (1) the maintenance of a written inventory of all SCI systems, critical SCI systems, and indirect SCI systems, including a lifecycle management program with respect to such systems; (2) a program to manage and oversee third-party providers that includes an initial and periodic review of contracts with third-party providers and a risk-based assessment of each third-party provider's criticality to the SCI entity; (3) a program to prevent unauthorized SCI system access; and (4) identification of the SCI industry standard with which such policies and procedures are consistent, if any. The Commission also proposes to amend the existing requirements in Rule 1001(a)(2)(v) for the BC/DR plan to include the requirement to maintain backup and recovery capabilities that are reasonably designed to address the unavailability of any third-party provider without which there would be a material impact on any of its critical SCI systems.

The requirement to have a third-party provider management program would help ensure that any third-party provider an SCI entity selects is able to support the SCI entity's compliance with Regulation SCI's requirements.

Additionally, the proposed revisions would ensure SCI entities are creating an inventory of their SCI systems, critical SCI systems, and indirect SCI systems and have a lifecycle management program for such systems, which would ensure that SCI entities are able to identify when a system becomes an SCI system or indirect SCI system and

---

438 *See* 17 CFR 242.1001(c).

when it ceases to be one. Next, the revisions would require SCI entities to have in place a program to prevent unauthorized SCI system access. The existing collections of information, which would be extended to new SCI entities would advance the goals of promoting the maintenance of fair an orderly markets and improving Commission review and oversight of U.S. securities market infrastructure. The proposed additional collections of information would advance these same goals.

### 2. Rule 1002 of Regulation SCI

Under Rule 1002 of Regulation SCI, SCI entities have certain obligations regarding SCI events. Rule 1002(a) requires an SCI entity to begin to take appropriate corrective action when any responsible SCI personnel has a reasonable basis to conclude that an SCI event has occurred. The corrective action must include, at a minimum, mitigating potential harm to investors and market integrity resulting from the SCI event and devoting adequate resources to remedy the SCI event as soon as reasonably practicable.[439] Rule 1002(b)(1) requires each SCI entity to immediately notify the Commission of an SCI event.[440] Under 17 CFR 242.1002(b)(2) ("Rule 1002(b)(2)"), each SCI entity is required, within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that the SCI event has occurred, to submit a written notification to the Commission pertaining to the SCI event that includes a description of the SCI event and the system(s) affected, with other information required to the extent available at the time.[441] Under 17 CFR 242.1002(b)(3) ("Rule 1002(b)(3)"), each SCI

---

439 *See* 17 CFR 242.1002(a).

440 *See* 17 CFR 242.1002(b)(1).

441 *See* 17 CFR 242.1002(b)(2).

entity is required to provide regular updates regarding the SCI event until the event is resolved.[442] Under 17 CFR 242.1002(b)(4)(i) ("Rule 1002(b)(4)(i)"), each SCI entity is required to submit written interim reports, as necessary, and a written final report regarding an SCI event to the Commission.[443] Under 17 CFR 242.1002(b)(4)(ii) ("Rule 1002(b)(4)(ii)"), the information that is required to be included in the interim and final written reports is set forth, including the SCI entity's assessment of the types and number of market participants affected by the SCI event and the impact of the SCI event on the market, and a copy of any information disseminated pursuant to Rule 1002(c) regarding the SCI event to the SCI entity's members or participants. For any SCI event that "has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants," Rule 1002(b)(5) provides an exception to the general Commission notification requirements under Rule 1002(b) Instead, an SCI entity must make, keep, and preserve records relating to all such SCI events, and submit a quarterly report to the Commission regarding any such events that are systems disruptions or systems intrusions. SCI events that are reported immediately and later determined to have a de minimis impact may be reclassified as de minimis.[444]

Rule 1002(c) of Regulation SCI requires that SCI entities disseminate information to their members or participants regarding SCI events.[445] Under 17 CFR 242.1002(c)(1)(i) ("Rule 1002(c)(1)(i)"), each SCI entity is required, promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event (other

---

442 *See* 17 CFR 242.1002(b)(3).

443 *See* 17 CFR 242.1002(b)(4).

444 *See* 17 CFR 242.1002(b)(5).

445 *See* 17 CFR 242.1002(c).

than a systems intrusion) has occurred, to disseminate certain information to its members or participants. Under 17 CFR 242.1002(c)(1)(ii) ("Rule 1002(c)(1)(ii)"), each SCI entity is required, when known, to disseminate additional information about an SCI event (other than a systems intrusion) to its members or participants promptly. Under 17 CFR 242.1002(c)(1)(iii) ("Rule 1002(c)(1)(iii)"), each SCI entity is required to provide to its members or participants regular updates of any information required to be disseminated under Rule 1002(c)(1)(i) and (ii) until the SCI event is resolved. Rule 1002(c)(2) requires each SCI entity to disseminate certain information regarding a systems intrusion to its members or participants. For "major SCI events," these disseminations must be made to all of its members or participants. For SCI events that are not "major SCI events," SCI entities must disseminate such information to those SCI entity members and participants reasonably estimated to have been affected by the event.[446] In addition, dissemination of information to members or participants is permitted to be delayed for systems intrusions if such dissemination would likely compromise the security of the SCI entity's systems or an investigation of the intrusion and documents the reasons for such determination.[447] Rule 1002(c)(4) of Regulation SCI provides exceptions to the dissemination requirements under Rule 1002(c) of Regulation SCI for SCI events to the extent they relate to market regulation or market surveillance systems and SCI events that have had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants.[448] Rule 1000 sets out the definition of systems

---

446 *See* 17 CFR 242.1002(c)(3).

447 *See* 17 CFR 242.1002(c)(2).

448 *See* 17 CFR 242.1002(c)(4).

intrusion, which means any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity.

The Commission proposes to amend the definition of systems intrusion in Rule 1000 to include cybersecurity events that disrupt, or significantly degrade, the normal operation of an SCI system and significant attempted unauthorized entries into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria. SCI entities would be required to report information concerning these systems intrusions pursuant to Rule 1002(b). The Commission believes that it is appropriate to expand the definition of systems intrusion to include two additional types of cybersecurity events that are currently not part of the current definition as described above. The additional notifications that would result from the proposed revised definition of systems intrusion would provide the Commission and its staff more complete information to assess the security status of the SCI entity, and also assess the impact or potential impact that unauthorized activity could have on the security of the SCI entity's affected systems as well on other SCI entities and market participants.

The proposed revisions to Rule 1002(b) would eliminate the de minimis exception's applicability to systems intrusions, thus requiring all systems intrusions, whether de minimis or non-de minimis, to be reported pursuant to Rule 1002(b)(1) through (4). The Commission would also amend the information required under Rule 1002(b)(4)(ii) to be included in the interim and final written notifications to include a copy of any information disseminated pursuant to Rule 1002(c) by an SCI broker-dealer to its customers. The Commission would use this information to be aware of potential

and actual security threats to SCI entities, including threats that may extend to other market participants in the securities markets, including other SCI entities.

As a result of the amendment to the definition of systems intrusions, SCI entities would be required to disseminate information to members and participants pursuant to Rule 1002(c)(2) concerning cybersecurity events not currently covered by the rule. This would have the effect of increasing the number of SCI events that would be required to be disseminated. Further, in connection with expansion of Regulation SCI to SCI broker-dealers, amended Rule 1002(c)(3) would require that SCI broker-dealers promptly disseminate information about major SCI events to all of its customers and, for SCI events that are not major SCI events, to customers that any responsible SCI personnel subsequently reasonably estimates may have been affected by the SCI event. Such information would be used by the SCI entity's members and participants, and in the case of an SCI broker-dealer, its customers, to understand better the threats faced by the SCI entity, evaluate the event's impact on their trading or other business with the SCI entity and formulate a response, thereby advance the Commission's goal of promoting fair and orderly markets and investor protection. The proposed revisions to Rule 1002(c), however, would exclude systems intrusions that are significant attempted unauthorized entries into the SCI systems or indirect SCI systems of an SCI entity from the information dissemination requirements of Rule 1002(c)(1) through (3).[449]

### 3. Rule 1003 of Regulation SCI

Rule 1003(a) establishes reporting burdens for all SCI entities. Rule 1003(a)(1) requires each SCI entity to submit to the Commission quarterly reports describing

---

[449] *See* proposed amended Rule 1002(c)(4).

completed, ongoing, and planned material changes to its SCI systems and security of indirect SCI systems during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion.[450] Under 17 CFR 242.1003(a)(2) ("Rule 1003(a)(2)"), each SCI entity is required to promptly submit a supplemental report notifying the Commission of a material error in or material omission from a report previously submitted under Rule 1003(a)(1).

Rule 1003(b) of Regulation SCI also requires that an SCI entity conduct an "SCI review" not less than once each calendar year.[451] "SCI review" is defined in Rule 1000 of Regulation SCI to mean a review, following established procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems, and which review contains: (1) a risk assessment with respect to such systems of an SCI entity; and (2) an assessment of internal control design and effectiveness of its SCI systems and indirect SCI systems to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards Rule 1003(b)(2) requires each SCI entity to submit a report of the SCI review to senior management no more than 30 calendar days after completion of the review.[452] Rule 1003(b) requires that penetration test reviews of the network, firewalls, and production systems shall be conducted at a frequency of not less than once every three years and that assessments of SCI systems directly supporting market regulation or market surveillance shall be conducted at a frequency based upon

---

450 *See* 17 CFR 242.1003(a).

451 *See* 17 CFR 242.1003(b).

452 *See* 17 CFR 242.1003(b)(2).

the risk assessment conducted as part of the SCI review, but in no case less than once every three years.[453] Rule 1003(b)(2) requires that the submission of a report of the SCI review to senior management of the SCI entity for review no more than 30 calendar days after completion of such SCI review.[454] Rule 1003(b)(3) requires each SCI entity to submit the report of the SCI review to the Commission and to its board of directors or the equivalent of such board, together with any response by senior management, within 60 calendar days after its submission to senior management.[455]

The Commission is proposing revisions to Rule 1003(b) and the definition of SCI review. The Commission is proposing to increase the frequency of penetration testing by SCI entities such that they are conducted at least annually, rather than once every three years, and that the penetration tests include any of the vulnerabilities of its SCI systems and indirect SCI systems identified pursuant to Rule 1001(a)(2)(iv).[456] The Commission would use this more frequent information to have more up-to-date information regarding an SCI entity's systems vulnerabilities and help the Commission with its oversight of U.S. securities market technology infrastructure.

In addition, the Commission is proposing a number of revisions to the requirements relating to SCI reviews and for the reports SCI entities submit (both to their board of directors as well as to the Commission). The definition of SCI review in Rule 1000 is proposed to contain the substantive requirements for an SCI review, which would be required to be "a review, following established and documented procedures and

---

453 *See* 17 CFR 242.1003(b)(1)(i) and (ii).

454 *See* 17 CFR 242.1003(b)(2).

455 *See* 17 CFR 242.1003(b)(3).

456 *See* 17 CFR 242.1000.

standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems…"[457] The Commission proposes to amend the definition of SCI review in Rule 1000 to require that the SCI review: (1) use appropriate risk management methodology, (2) include third-party provider management risks and controls, (3) include the risks related to the capacity, integrity, resiliency, availability, and security, and (4) include systems capacity and availability and information technology service continuity within the review of internal control design and operating effectiveness.[458]

The Commission also proposes to amend Rule 1003(b)(2) to require that the SCI review be conducted in each calendar year during which the entity was an SCI entity for any part of that calendar year and that the SCI entity submit the associated report of the SCI review to the SCI entity's senior management and board, as well as to the Commission.[459] The Commission proposes amend Rule 1003(b)(2) to specify that certain elements be included in the report of the SCI review, namely: (1) the dates the SCI review was conducted and the date of completion; (2) the entity or business unit of the SCI entity performing the review; (3) a list of the controls reviewed and a description of each such control; (4) the findings of the SCI review with respect to each SCI system and indirect SCI system, which shall include, at a minimum, assessments of: the risks related to the capacity, integrity, resiliency, availability, and security; internal control design and operating effectiveness; and an assessment of third-party provider management risks and

---

457 *See id.*

458 *See id.*

459 *See* 17 CFR 242.1003(b)(2) and (3).

controls; (5) a summary, including the scope of testing and resulting action plan, of each penetration test review conducted as part of the SCI review; and (6) a description of each deficiency and weakness identified by the SCI review.[460] The Commission also proposes to amend Rule 1003(b)(3) to require a response to the report of the SCI review from senior management and to require that the date the report was submitted to senior management be submitted to the Commission and the board of directors, and that the response from senior management include a response for each deficiency and weakness identified by the SCI review, and the associated mitigation and remediation plan and associated dates for each.[461]

The additional requirements and details are designed to ensure SCI reviews contain certain baseline information and are based on the appropriate risk management methodology. The enhanced SCI review and corresponding report would provide the Commission and its staff greater insight into the SCI entity's compliance with Regulation SCI and would more thoroughly assist the staff in determining how to follow up with the SCI entity in reviewing and addressing any identified weaknesses and vulnerabilities. The Commission would use this additional reporting and information to improve the Commission's oversight of the technology infrastructure of SCI entities further.

#### 4. Rule 1004 of Regulation SCI

Rule 1004 of Regulation SCI requires SCI entities to, with respect to an SCI entity's business continuity and disaster recovery plans, including its backup systems: (a) establish standards for the designation of those members or participants that the SCI

---

460 *See* 17 CFR 242.1003(b)(2).

461 *See* 17 CFR 242.1003(b)(3).

entity reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of such plans; (b) designate members or participants pursuant to such standards and require participation by such designated members or participants in scheduled functional and performance testing of the operation of such plans, in the manner and frequency specified by the SCI entity, provided that such frequency shall not be less than once every 12 months; and (c) coordinate the testing of such plans on an industry- or sector-wide basis with other SCI entities.[462]

The Commission is proposing to include certain third-party providers in the BC/DR testing requirements of Rule 1004. Specifically, an SCI entity would be required to establish standards for the designation of third-party providers (in addition to members or participants) that it determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of the SCI entity's BC/DR plans. In addition, Rule 1004 would require each SCI entity to designate such third-party providers (in addition to members or participants) pursuant to such standards and require their participation in the scheduled functional and performance testing of the operation of such BC/DR plans.[463]

The Commission believes that the requirement that SCI entities establish standards that require designated third-party providers to participate in the testing of their business continuity and disaster recovery plans will help reduce the risks associated with an SCI entity's decision to activate its BC/DR plans and help to ensure that such plans

---

462 *See* 17 CFR 242.1003(b)(4).

463 *See id.*

operate as intended, if activated. The testing participation requirement should help an SCI entity to ensure that its efforts to develop effective BC/DR plans are not undermined by a lack of participation by third-party providers that the SCI entity believes are necessary to the successful activation of such plans. This requirement should also assist the Commission in maintaining fair and orderly markets in a BC/DR scenario following a wide-scale disruption.

### 5. Rule 1005 and 1007 of Regulation SCI

Rule 1005 of Regulation SCI requires SCI entities to make, keep, and preserve certain records related to their compliance with Regulation SCI.[464] Rule 1007 sets forth requirements for a SCI entity whose Regulation SCI records are prepared or maintained by a service bureau or other recordkeeping service on behalf of the SCI entity.[465]

Rule 1005(c) specifies that the requirement that records required to be made, kept, and preserved by Rule 1005 be accessible to the Commission and its representatives for the period required by Rule 1005, in cases where an SCI entity ceases to do business or ceases to be registered under the Exchange Act.[466] The Commission proposes to add that this survival provision similarly applies to an SCI entity that "otherwise [ceases] to be an SCI entity."[467] This addition accounts for circumstances not expressly covered; specifically, the circumstance in which an SCI entity continues to do business or remains a registered entity, but may cease to qualify as an SCI entity (*e.g.*, an SCI ATS that no

---

464 *See* 17 CFR 242.1005. Rule 1005(a) of Regulation SCI relates to recordkeeping provisions for SCI SROs, whereas Rule 1005(b) relates to the recordkeeping provision for SCI entities other than SCI SROs.

465 *See* 17 CFR 242.1007.

466 *See* 17 CFR 242.1005(c).

467 *See id.*

longer satisfies a volume threshold). Such entities would not be excepted from complying with the recordkeeping provisions of Rule 1005.

The Commission believes the records of entities that ceased being SCI entities are important for assisting the Commission and its staff in understanding whether such an SCI entity met its obligations under Regulation SCI, assessing whether such an SCI entity had appropriate policies and procedures with respect to its technology systems, helping to identify the causes and consequences of an SCI event, and understanding the types of material systems changes that occurred at such an SCI entity. The Commission expects this revision to facilitate the Commission's inspections and examinations of SCI entities that have ceased to be SCI entities and assist it in evaluating such SCI entity's previous compliance with Regulation SCI. Furthermore, having an SCI entity's records available even after it has ceased to be an SCI entity should provide an additional tool to help the Commission to reconstruct important market events and better understand the impact of such events. There are no amendments to Rule 1007, which sets forth requirements for a SCI entity whose Regulation SCI records are prepared or maintained by a service bureau or other recordkeeping service on behalf of the SCI entity.

**6. Rule 1006 of Regulation SCI**

Rule 1006 requires each SCI entity, with a few exceptions, to file any notification, review, description, analysis, or report to the Commission required under Regulation SCI electronically on Form SCI.[468] There are no amendments to this section. The Commission staff would use the collection of information in its examination and oversight program in identifying patterns and trends across registrants.

---

[468] *See* 17 CFR 242.1003(b)(6).

### C. Respondents

The collection of information requirements contained in Regulation SCI apply to SCI entities. As of 2021, there were an estimated 47 Current SCI Entities (*i.e.,* entities that met the definition of SCI entity)[469] that were subject to the requirements of Regulation SCI.[470] The Commission preliminarily estimates that as a result of the proposed amendments to Rule 1000, there would be a total of 23 New SCI Entities (*i.e.,* meet the amended definition of SCI entity) that would become subject to the requirements of Regulation SCI. Thus, the Commission preliminarily estimates that a total of 70 entities would be subject to the requirements of Regulation SCI. The Commission preliminarily believes that the remaining amendments would not add any additional respondents but would result in additional reporting burdens, which are discussed in section IV.D (Total Initial and Annual Reporting Burdens).

The following table summarizes the estimated number of Current SCI Entities and New SCI Entities:

---

469 In 2020, the Commission amended Regulation SCI to add as SCI entities SCI competing consolidators, defined as competing consolidators that exceed a five percent consolidated market data gross revenue threshold over a specified time period. *See* Market Data Infrastructure Adopting Release, *supra* note 24. The Commission estimated that seven persons would meet the definition of SCI competing consolidator and be subject to Regulation SCI, two of which would be Current SCI Entities (as plan processors) and five of which would be new SCI competing consolidators, if they registered as competing consolidators and exceeded the threshold. *See Extension Without Change of a Currently Approved Collection: Regulation SCI and Form SCI*; ICR Reference No. 202111-3235-005; OMB Control No. 3235-0703 (Mar. 3, 2022), *available at* https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=202111-3235-005 ("2022 PRA Supporting Statement"). Currently, no competing consolidators have registered with the Commission. As a result, no competing consolidators (in addition to the two current plan processors that are Current SCI Entities) are included as Current SCI Entities. To the extent that a competing consolidator registers with the Commission and qualifies as an SCI competing consolidator it would be subject to the same additional burdens as Current SCI Entities as a result of the proposed amendments to Regulation SCI. The additional burdens for Current SCI Entities are set forth in section IV.D.

470 Proposed Collection; Comment Request; Extension: Regulation SCI, Form SCI; SEC File No. 270-653, OMB Control No. 3235-0703, 87 FR 3132.

| Type of SCI Entity | Number |
|---|---|
| **Current SCI Entities** | **47** |
| | |
| **New SCI Entities:** | |
| SBSDR[1] | 3 |
| SCI broker-dealers[2] | 17 |
| Exempt Clearing Agencies[3] | 3 |
| **Total New SCI Entities** | **23** |
| | |
| **Total SCI Entities** | **70** |

[1] *See supra* notes 118, 124 and accompanying text. As noted earlier, two SBSDRs are currently registered with the Commission. The Commission estimates for purposes of the PRA that one additional entity may seek to register as an SBSDR in the next three years, and so for purposes of this proposal the Commission has assumed three SBSDR respondents.

[2] *See supra* note 219 and accompanying text.

[3] *See supra* notes 240 and accompanying text. As noted earlier, the Commission proposes to expand the scope of "SCI entity" to cover two additional exempt clearing agencies that are not subject to ARP, which are Euroclear Bank SA/NV and Clearstream Banking, S.A. The Commission estimates for purposes of the PRA that one additional entity may receive an exemption from registration as a clearing agency in the next three years, and so for purposes of this proposal the Commission has assumed three exempt clearing agency respondents.

### D. Total Initial and Annual Reporting Burdens

As stated above, each requirement to disclose information, offer to provide information, or adopt policies and procedures constitutes a collection of information requirement under the PRA. We discuss below the collection of information burdens associated with the proposed rules and rule amendments.

#### 1. Rule 1001

The rules under Regulation SCI that would require an SCI entity to establish policies and procedures are discussed more fully in sections II.B, and the proposed amendments are discussed more fully in sections III.A and III.C above.

##### a. Rule 1001(a)

Current SCI Entities are already required to establish, maintain, and enforce policies and procedures pursuant to Rule 1001(a) and therefore already incur baseline

initial[471] and ongoing burden[472] for complying with Rule 1001(a), so the amendments should only impose a burden required to comply with the additional requirements.[473] Presently, none of the New SCI Entities are required to comply with the policies and procedures requirement of Rule 1001(a), but the proposed amendments will newly impose the baseline burden to develop and draft written policies and procedures and review and update annually such policies and procedures, as well as the additional burden to include the proposed requirements in the policies and procedures. The Commission estimates an initial compliance burden of 386 additional hours[474] for Current SCI Entities and 890 hours[475] for New SCI Entities. The Commission estimates an annual compliance

---

471 The Commission's currently approved baseline for average compliance burden per SCI entity to develop and draft the policies and procedures required by Rule 1001(a) (except for 17 CFR 242.1001(a)(2)(vi) ("Rule 1001(a)(2)(vi)")) is 534 hours. *See Extension Without Change of a Currently Approved Collection: Regulation SCI and Form SCI*; ICR Reference No. 202111-3235-005; OMB Control No. 3235-0703 (Mar. 3, 2022), *available at* https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=202111-3235-005 ("2022 PRA Supporting Statement"). Rule 1001(a)(2) currently requires six elements (excluding Rule 1001(a)(2)(vi)) to be included in the policies and procedures required by Rule 1001(a)(1). The burden hours for each element would be 89 hours per policy element (534 hours/6 policy elements).

472 The Commission's currently approved baseline for average compliance burden per SCI entity to review and update the policies and procedures required by Rule 1001(a) (except for Rule 1001(a)(2)(vi)) is 87 hours. *See* 2022 PRA Supporting Statement, *supra* note 471. The burden hours for each element would be 14.5 hours per policy element (87 hours/6 policy elements).

473 The Commission estimates that at the additional burden would be the result of the additions to Rule 1001(a)(2), specifically the proposed requirement in the BC/DR plan and the four proposed additional policy elements. The Commission does not anticipate that Current SCI Entities or New SCI Entities would incur any additional burden from the amendment to Rule 1001(a)(4) above and beyond the burden hours estimated for the policies and procedures in this release.

474 89 hours x 4 additional policy elements = 356 hours. The Commission estimates a one-time burden of 30 hours (one-third of 89 hours per policy element) for SCI entities to address the unavailability of third-party providers in their BC/DR plans. 356 hours + 30 hours = 386 hours. The burden hours include 139 Compliance Manager hours, 139 Attorney hours, 43 Senior System Analyst hours, 43 Operations Specialist hours, 15 Chief Compliance Officer hours, and 7 Director of Compliance hours.

475 534 baseline burden hours + 356 additional burden hours = 890 hours. The burden hours include 320 Compliance Manager hours, 320 Attorney hours, 100 Senior System Analyst hours, 100 Operations Specialist hours, 33 Chief Compliance Officer hours, and 17 Director of Compliance hours.

burden of 58 hours[476] for Current SCI Entities and 145 hours[477] for New SCI Entities.[478] The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

| Respondent Type | Burden Type | Estimated Respondents | Burden Hours per Entity | Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity) |
|---|---|---|---|---|
| Current SCI Entities | Initial | 47 entities | 386 hours | 18,142 hours |
| | Annual | 47 entities | 58 hours | 2,726 hours |
| New SCI Entities | Initial | 23 entities | 890 hours | 20,470 hours |
| | Annual | 23 entities | 145 hours | 3,335 hours |

The table below summarizes the Commission's estimates for the average internal cost of compliance for Current SCI Entities and New SCI Entities:

476 14.5 hours x 4 additional policy elements = 58 hours. The burden hours include 19 Compliance Manager hours, 19 Attorney hours, 5 Senior System Analyst hours, 5 Operations Specialist hours, 7 Chief Compliance Officer hours, and 3 Director of Compliance hours.

477 87 baseline burden hours + 58 additional burden hours = 145 hours. The burden hours include 47 Compliance Manager hours, 47 Attorney hours, 13 Senior System Analyst hours, 13 Operations Specialist hours, 17 Chief Compliance Officer hours, and 8 Director of Compliance hours.

478 The Commission recognizes that the some of the Regulation SCI requirements and certain proposed requirements in the Exchange Act Cybersecurity Proposal rule may appear duplicative. The Commission believes that although the requirements are related, they are ultimately separate obligations. Thus, the Commission has not considered the requirements of the Exchange Act Cybersecurity Proposal rule in formulating its estimates.

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity) |
|---|---|---|---|---|
| Current SCI Entities | Initial | 47 entities | $144,787[1] | $6,804,989 |
| | Annual | 47 entities | $23,403[2] | $1,099,941 |
| New SCI Entities | Initial | 23 entities | $333,371[3] | $7,667,533 |
| | Annual | 23 entities | $58,315[4] | $1,341,245 |

[1] (139 Compliance Manager hours x $344) + (139 Attorney hours x $462) + (43 Senior Systems Analyst hours x $316) + (43 Operations Specialist hours x $152) + (15 Chief Compliance Officer hours x $589) + (7 Director of Compliance hours x $542) = $144,787. The Commission derived this estimate based on per hour figures from SIFMA's Management & Professional Earnings in the Securities Industry 2013, modified by Commission staff to account for an 1,800-hour work-year and inflation, and multiplied by 5.35 to account for bonuses, firm size, employee benefits, and overhead.

[2] (19 Compliance Manager hours x $344) + (19 Attorney hours x $462) + (5 Senior Systems Analyst hours x $316) + (5 Operations Specialist hours x $152) + (7 Chief Compliance Officer hours x $589) + (3 Director of Compliance hours x $542) = $23,403.

[3] (320 Compliance Manager hours x $344) + (320 Attorney hours x $462) + (100 Senior Systems Analyst hours x $316) + (100 Operations Specialist hours x $152) + (33 Chief Compliance Officer hours x $589) + (17 Director of Compliance hours x $542) = $333,371.

[4] (47 Compliance Manager hours x $344) + (47 Attorney hours x $462) + (13 Senior Systems Analyst hours x $316) + (13 Operations Specialist hours x $152) + (17 Chief Compliance Officer hours x $589) + (8 Director of Compliance hours x $542) = $58,315.

The proposed amendments would newly impose a burden on New SCI Entities to comply with Rule 1001(a)(2)(vi), which requires the policies and procedures required by Rule 1001(a) to include standards that result in systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data.[479] The Commission estimates that New SCI Entities would incur an initial burden of 160 hours and an ongoing burden

[479] Current SCI Entities would incur no additional burden as they are already required to include the required standards in their policies and procedures.

of 145 hours to annually review and update the policies and procedures.[480] The table below summarizes the initial and ongoing annual burden estimates for New SCI Entities to comply with Rule 1001(a)(2)(vi):

| Respondent Type | Burden Type | Estimated Respondents | Burden Hours per Entity | Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity) |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | 160 hours | 3,680 hours |
| | Annual | 23 entities | 145 hours | 3,335 hours |

The table below summarizes the Commission's estimates for the average internal cost of compliance for New SCI Entities:

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | $60,980[1] | $1,402,540 |
| | Annual | 23 entities | $52,380[2] | $1,204,740 |

[1] (100 Senior Systems Analyst hours x $316) + (20 Chief Compliance Officer hours x $589) + (10 Director of Compliance hours x $542) + (30 Compliance Attorney hours x $406) = $60,980.

[2] (100 Senior Systems Analyst hours x $316) + (10 Chief Compliance Officer hours x $589) + (5 Director of Compliance hours x $542) + (30 Compliance Attorney hours x $406) = $52,380.

The Commission estimates that on average, Current SCI Entities would seek outside legal and/or consulting services to initially update their policies and procedures

[480] These estimates are consistent with the Commission-approved baseline initial and ongoing average compliance burdens per SCI entity. *See* 2022 PRA Supporting Statement, *supra* note 471. The 160 hour initial burden includes 100 Compliance Manager hours, 20 Chief Compliance Officer hours, 10 Director of Compliance hours, and 30 Compliance Attorney hours. The 145 annual burden hours includes 100 Compliance Manager hours, 10 Chief Compliance Officer hours, 5 Director of Compliance hours, and 30 Compliance Attorney hours.

for the proposed additional requirements at a cost of $29,050 per SCI entity,[481] while New SCI Entities would seek such services in the initial preparation of the policies and procedures (including the proposed requirements) at a cost of $73,800 per SCI entity.[482]

| Respondent Type | Estimated Respondents | Average External Cost per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average External Cost per Entity |
|---|---|---|---|
| Current SCI Entities | 47 entities | $29,050 | $1,365,350 |
| New SCI Entities | 23 entities | $73,800 | $1,697,400 |

**b. Rule 1001(b)**

New SCI Entities would be required to meet the requirements of Rule 1001(b), which requires each SCI entity to establish, maintain, and enforce systems compliance policies. The Commission estimates a compliance burden of 270 hours initially to design the systems compliance policies and procedures and 95 hours annually to review and

481 The Commission's currently approved baseline for annualized recordkeeping cost per SCI entity to consult outside legal and/or consulting services in the initial preparation policies and procedures required by Rule 1001(a) is $47,000. *See* 2022 PRA Supporting Statement, *supra* note 471. Rule 1001(a)(2) currently requires seven elements (including Rule 1001(a)(2)(vi)) to be included in the policies and procedures required by Rule 1001(a)(1). The cost per element would be approximately $6,700 per policy element ($47,000 hours/7 policy elements = $6,714). As noted earlier, the Commission proposes to add four additional elements to the policies and procedures. $6,700 per policy element x 4 additional policy elements = $26,800. The Commission also estimates a one-time burden of approximately $2,250 per SCI entity (one-third of $6,700 per policy element) to address the unavailability of third-party providers in their BC/DR plans. $26,800 + $2,250 = $29,050.

482 $47,000 + $26,800 = $73,800.

update such policies and procedures.[483] The table below summarizes the initial and ongoing annual burden estimates for New SCI Entities to comply with Rule 1001(b):

| Respondent Type | Burden Type | Estimated Respondents | Burden Hours per Entity | Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity) |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 | 270 | 6,210 |
| | Annual | 23 | 95 | 2,185 |

The table below summarizes the Commission's estimates for the average internal cost of compliance for New SCI Entities:

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | $96,640[1] | $2,222,720 |
| | Annual | 23 entities | $35,140[2] | $808,220 |

[1] (200 Senior Systems Analyst hours x $316) + (20 Chief Compliance Officer hours x $589) + (10 Director of Compliance hours x $542) + (40 Compliance Attorney hours x $406) = $96,640.

[2] (66 Senior Systems Analyst hours x $316) + (10 Chief Compliance Officer hours x $589) + (5 Director of Compliance hours x $542) + (14 Compliance Attorney hours x $406) = $35,140.

---

[483] The Commission estimates that the burden for New SCI Entities is consistent with the Commission's current approved baselines for the initial and ongoing burdens. For the initial recordkeeping burden, this baseline is 270 hours (40 Compliance Attorney hours + 200 Senior System Analyst hours + 20 Chief Compliance Officer hours + 10 Director of Compliance hours). The Commission estimated separate baselines for the ongoing recordkeeping burden for SCI SROs and entities that were not SROs. Since none of the entities that would potentially be subject to Regulation SCI as a result of the proposed amendments are SROs, the Commission is basing its estimates on the baseline for non-SROs. The Commission's current approved baseline for the ongoing recordkeeping burden for entities that are not SROs is 95 hours (14 Compliance Attorney hours + 66 Senior System Analyst hours + 10 Chief Compliance Officer hours + 5 Director of Compliance hours). *See* 2022 PRA Supporting Statement, *supra* note 471.

In establishing, maintaining, and enforcing the policies and procedures required by Rule 1001(b), the Commission believes that each new SCI entity will seek outside legal and/or consulting services in the initial preparation of such policies and procedures. The total annualized cost of seeking outside legal and/or consulting services will be $621,000.[484]

**c. Rule 1001(c)**

The proposed amendments would newly impose a burden on New SCI Entities to develop and maintain policies with Rule 1001(c), relating to the policies for designation of responsible SCI personnel. The Commission estimates a compliance burden of 114 hours initially to design the systems compliance policies and procedures and 39 hours annually to review and update such policies and procedures.[485] The table below summarizes the initial and ongoing annual burden estimates for New SCI Entities to comply with Rule 1001(b):

---

484 The Commission estimates that the cost for outside legal and/or consulting services for New SCI Entities is consistent with the Commission's current approved baselines, which is $27,000 per new SCI entity. *See* 2022 PRA Supporting Statement, *supra* note 471. $27,000 for the first year × 23 New SCI Entities = 621,000.

485 The Commission's current approved baseline 114 hours for the initial burden to establish the criteria for identifying responsible SCI personnel and the escalation procedures (32 Compliance Manager hours + 32 Attorney hours x $412 + 10 Senior Systems Analyst hours x $282 + 10 Operations Specialist hours x $135 + 20 Chief Compliance Officer hours x $526 + 10 Director of Compliance). The Commission's approved baseline is 39 hours for the ongoing burden to annually review and update the criteria and the escalation procedures (9.5 Compliance Manager hours + 9.5 Attorney hours + 2.5 Senior Systems Analyst hours + 2.5 Operations Specialist hours + 10 Chief Compliance Officer hours + 5 Director of Compliance hours). *See* 2022 PRA Supporting Statement, *supra* note 471.

| Respondent Type | Burden Type | Estimated Respondents | Burden Hours per Entity | Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity) |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 | 114 | 2,622 |
| | Annual | 23 | 39 | 897 |

The table below summarizes the Commission's estimates for the average internal cost of compliance for New SCI Entities:

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | $47,672[1] | $1,096,456 |
| | Annual | 23 entities | $17,427[2] | $400,821 |

[1] (32 Compliance Manager hours x 344) + (32 Attorney hours x $462) + (10 Senior Systems Analyst hours x $316) + (10 Operations Specialist hours x $152) + (20 Chief Compliance Officer hours x $589) + (10 Director of Compliance hours x $542) = $47,672.

[2] (9.5 Compliance Manager hours x $344) + (9.5 Attorney hours x $462) + (2.5 Senior Systems Analyst hours x $316) + (2.5 Operations Specialist hours x $152) + (10 Chief Compliance Officer hours x $589) + (5 Director of Compliance hours x $542) = $17,427.

The Commission does not expect SCI entities to incur any external PRA costs in connection with the policies and procedures required under Rule 1001(c).

**2. Rule 1002**

The rules under Regulation SCI that would require an SCI entity to take corrective action, provide certain notifications and reports, and disseminate certain information regarding SCI events are discussed more fully in sections II.B, and the proposed amendments are discussed more fully in sections III.A and III.C above.

#### a. Rule 1002(a)

As noted above, Rule 1002(a) requires each SCI entity, upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, to begin to take appropriate corrective action. The Commission has previously expressed the view that Rule 1002(a) would likely result in SCI entities developing and revising their processes for corrective action.[486] The Commission believes that the requirement to take corrective action for these additional systems intrusions would likely result in SCI entities updating their processes for corrective action.[487]

The Commission continues to believe that Rule 1002(a) will likely result in SCI entities developing and revising their processes for corrective action as well as review them annually.[488] Current SCI Entities are already required to take corrective action pursuant to Rule 1002(a) and therefore already incur the initial[489] and ongoing[490] baseline burdens for developing and revising their corrective action process, so the amendments should only impose a one-time burden required to update the procedures to account for

---

486 *See* 2022 PRA Supporting Statement, *supra* note 471.

487 The Commission's estimate includes the amendments to the definition of systems intrusions adding (1) cybersecurity events that disrupt, or significantly degrade, the normal operation of an SCI system and (2) significant attempted unauthorized entries into the SCI systems or indirect SCI systems of an SCI entity. It does not include the systems intrusions that would previously have been classified as de minimis events because Current SCI Entities are already required to take corrective action to resolve such SCI events.

488 *See* 2022 PRA Supporting Statement, *supra* note 471.

489 The Commission's currently approved baseline for average compliance burden per respondent to develop a process for corrective action is 114 hours (32 Compliance Manager hours + 32 Attorney hours + 10 Senior Systems Analyst hours + 10 Operations Specialist hours + 20 Chief Compliance Officer hours + 10 Director of Compliance hours). *See* 2022 PRA Supporting Statement, *supra* note 471.

490 The average compliance burden for each SCI entity to review their process is 39 hours (9 Compliance Manager hours + 9 Attorney hours + 3 Senior Systems Analyst hours + 3 Operations Specialist hours + 10 Chief Compliance Officer hours + 5 Director of Compliance hours. *See* 2022 PRA Supporting Statement, *supra* note 471.

the additional types of systems intrusions.[491] The Commission estimates that the one-time burden for each SCI entity to include in its corrective action process the proposed systems intrusions would be 20% of the 114 hours baseline burden.[492] Presently, the New SCI Entities are not required to comply with requirement in Rule 1002(a) to take corrective action, but the proposed amendments will newly impose these burdens, including the burden for incorporating the additional systems intrusions into the corrective action process. For Current SCI Entities, the Commission estimates a one-time compliance burden of 23 hours. For New SCI Entities, the Commission estimates an initial burden of 137 hours[493] and an annual compliance burden of 39 hours[494] for New SCI Entities. The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

---

491 The Commission also proposes to remove the option for SCI entities to classify systems intrusions as de minimis and potentially report them pursuant to Rule 1002(b)(5) on the quarterly SCI reports as de minimis events. SCI entities would instead report these systems intrusions pursuant to Rule 1002(b)(1) through (4). The Commission believes that the burden for developing a corrective action plan for these systems intrusions is already incorporated in the baseline burden estimates. *See supra* notes 489-490.

492 114 hours x 0.20 = 23 hours. The burden hours include 7 Compliance Manager hours, 6 Attorney hours, 2 Senior Systems Analyst hours, 2 Operations Specialist hours, 4 Chief Compliance Officer hours, and 2 Director of Compliance hours.

493 114 baseline burden hours + 23 burden hours for additional systems intrusions = 137 hours. The burden hours include 39 Compliance Manager hours, 38 Attorney hours, 12 Senior Systems Analyst hours, 12 Operations Specialist hours, 24 Chief Compliance Officer hours, and 12 Director of Compliance hours.

494 The Commission estimates that the ongoing recordkeeping burden for each New SCI Entity to review its corrective action process would be the same as the baseline ongoing recordkeeping burden of 39 hours. *See supra* note 490.

| Respondent Type | Burden Type | Estimated Respondents | Burden Hours per SCI Entity | Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity) |
|---|---|---|---|---|
| Current SCI Entities | One-time Burden | 47 | 23 | 1,081 |
| New SCI Entities | Initial | 23 | 137 | 3,151 |
| | Ongoing | | 39 | 897 |

The table below summarizes the Commission's estimates for the cost of compliance for Current SCI Entities and New SCI Entities:

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| Current SCI Entities | One-time Burden | 47 | 9,556[1] | $449,132 |
| New SCI Entities | Initial | 23 | $57,228[2] | $1,316,244, |
| | Ongoing | | $17,258[3] | $396,934 |

[1] (7 Compliance Manager hours x 344) + (6 Attorney hours x $462) + (2 Senior Systems Analyst hours x $316) + (2 Operations Specialist hours x $152) + (4 Chief Compliance Officer hours x $589) + (2 Director of Compliance hours x $542) = $9,556.

[2] (39 Compliance Manager hours x 344) + (38 Attorney hours x $462) + (12 Senior Systems Analyst hours x $316) + (12 Operations Specialist hours x $152) + (24 Chief Compliance Officer hours x $589) + (12 Director of Compliance hours x $542) = $57,228.

[3] (9 Compliance Manager hours x 344) + (9 Attorney hours x $462) + (3 Senior Systems Analyst hours x $316) + (3 Operations Specialist hours x $152) + (10 Chief Compliance Officer hours x $589) + (5 Director of Compliance hours x $542) = $17,258.

The Commission does not expect SCI entities to incur any external PRA costs in connection with the requirement to take corrective actions under Rule 1002(a).

**b. Rule 1002(b)(1) through (4)**

As noted earlier, SCI entities have certain reporting obligations regarding SCI events. Current SCI Entities are already required to submit the notifications, updates, and reports required by Rule 1002(b)(1) through (4) and therefore already incur a baseline burden. As a result of the additional systems intrusions, including the amendments to the

definition of systems intrusions and the exclusion of systems intrusions from de minimis SCI events required to be reported to the Commission, Current SCI Entities could potentially incur new burdens pursuant to Rule 1002(b)(1) through (4) reporting additional SCI events for which they currently either do not report or which they currently report quarterly as de minimis. As proposed, New SCI Entities would for the first time be required to provide the submissions required by Rule 1002(b)(1) through (4) and would bear the existing burden for compliance with Rule 1002(b)(1) through (4) and the additional burden to report the proposed systems intrusions.

The Commission estimates that on average each Current SCI Entity will experience an additional three SCI events each year that are not de minimis SCI events[495] and New SCI Entities will experience an average of eight SCI events each year that are not de minimis SCI events.[496]

As a result, pursuant to Rule 1002(b)(1), which requires immediate notification of SCI events, the Commission estimates that each Current SCI Entity will submit, on average, an additional three notifications per year beyond the current baseline,[497] and

---

495 The Commission's currently approved baseline for the number of SCI events is five events per year that are not de minimis. *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission estimates that as a result of the additional systems intrusions that SCI entities would be required to report, the number of SCI events would increase by three events per year that are not de minimis.

496 The Commission estimates that each New SCI Entity would experience the baseline burden of five SCI events and three additional SCI events, for a total of eight SCI events that are not de minimis.

497 The Commission's currently approved baseline for the number of notifications submitted by an SCI entity pursuant to Rule 1002(b)(1) is five notifications per year, with one-fourth of the five notifications submitted in writing (*i.e.*, approximately one event per year for each SCI entity), and approximately three-fourths provided orally (*i.e.*, approximately four events per year for each SCI entity). *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission estimates that the proposed systems intrusions will result in each SCI entity submitting three additional notifications, one for each of the three estimated additional SCI events.

each New SCI Entity will submit eight notifications per year.[498] These notifications can be made orally or in writing, and the Commission estimates that approximately one-fourth of these notifications will be submitted in writing (*i.e.*, approximately one event per year for each Current SCI Entity and two events per year for each New SCI Entity[499]), and approximately three-fourths will be provided orally (*i.e.*, approximately two events per year for each Current SCI Entity[500] and six events per year for each New SCI Entity[501]). The Commission estimates that each written notification will require two hours and each oral notification will require 1.5 hours.[502] The Commission estimates a burden of 5 hours[503] for each Current SCI Entities and 13 hours[504] for New SCI Entities. The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

---

498 The Commission estimates that each New SCI Entity will submit both the current baseline of five notifications and the additional three notifications, for a total of eight notifications. *See supra* note 497 (discussing the 3 additional notifications).

499 8 SCI events ÷ 4 = 2 SCI events reported in writing. The Commission estimates that each Current SCI Entities already reports one SCI event per year in writing. *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission therefore estimates that they would report one additional SCI event in writing. New SCI Entities would report two SCI events in writing.

500 3 SCI events – 1 SCI event reported in writing = 2 SCI events reported orally.

501 8 SCI events – 2 SCI events reported in writing = 6 SCI events reported orally.

502 The Commission-approved baseline for the burden hours for each notification are 2 hours for written communications (0.5 Compliance Manager hours + 0.5 Attorney hours + 0.5 Senior Systems Analyst hours + 0.5 Senior Business Analyst hours) and 1.5 hours for oral communications (0.25 Compliance Manager hours + 0.25 Attorney hours + 0.5 Senior Systems Analyst hours + (0.5 Senior Business Analyst hours). *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission does not believe that reporting the proposed systems intrusions would change the estimated burden hours.

503 1 written notification each year * 2 hours per notification + 2 oral notifications each year * 1.5 hours per notification = 5 hours.

504 2 written notification each year * 2 hours per notification + 6 oral notifications each year * 1.5 hours per notification = 13 hours.

| Respondent Type | Estimated Respondents | Burden Hours per SCI Entity | Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity) |
|---|---|---|---|
| Current SCI Entities | 47 entities | 5 hours | 235 hours |
| New SCI Entities | 23 entities | 13 hours | 299 hours |

The table below summarizes the Commission's estimates for the average internal cost of compliance associated with the ongoing reporting burden for Current SCI Entities and New SCI Entities:

| Respondent Type | Estimated Respondents | Average Internal Cost of Compliance per SCI Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|
| Current SCI Entities | 47 entities | $1,737.50[1] | $81,663 |
| New SCI Entities | 23 entities | $4,499[2] | $103,477 |

[1] The average internal cost of compliance for each Current SCI entity to submit an additional written notification per year is $713.50 (0.5 Compliance Manager hours x $344) + (0.5 Attorney hours x $462) + (0.5 Senior Systems Analyst hours x $316) + (0.5 Senior Business Analyst hours x $305) = $713.50 per written notification. $713.50 x 1 written notification each year = $713.50.

(0.25 Compliance Manager hours x $344) + (0.25 Attorney hours x $462) + (0.5 Senior Systems Analyst hours x $316) + (0.5 Senior Business Analyst hours x $305) = $512 per oral notification. $512 x 2 = $1,024.

$713.50 + $1,024 = $1,737.50.

[2] $713.50 per written notification x 2 written notifications + $512 per written notification x 6 oral notifications = $4,499.

The Commission estimates that each notification submitted pursuant to Rule 1002(b)(2) will require 24 hours per SCI entity.[505] The Commission estimates an average

[505] The Commission-approved baseline for the burden hours for each written notification is 24 hours (5 Compliance Manager hours + 5 Attorney hours + 6 Senior Systems Analyst hours + 1 Assistant General Counsel hour + 1 Chief Compliance Officer hour + 6 Senior Business Analyst hours) for each SCI entity. *See* 2022 PRA Supporting Statement, *supra* note 471.

of 72 hours[506] for each Current SCI Entity and 192 hours[507] for each New SCI Entity to submit the 24 hour written notifications required by Rule 1002(b)(2). The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

| **Respondent Type** | **Estimated Respondents** | **Burden Hours per SCI Entity** | **Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity)** |
|---|---|---|---|
| Current SCI Entities | 47 entities | 72 hours | 3,384 hours |
| New SCI Entities | 23 entities | 192 hours | 4,416 hours |

The table below summarizes the Commission's estimates for the cost of compliance associated with the ongoing reporting burden for Current SCI Entities and New SCI Entities:

| **Respondent Type** | **Estimated Respondents** | **Average Internal Cost of Compliance per SCI Entity** | **Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity** |
|---|---|---|---|
| Current SCI Entities | 47 entities | $26,589[1] | $1,249,683 |
| New SCI Entities | 23 entities | $70,904[2] | $1,630,792 |

[1] The average internal cost of compliance for each Current SCI entity to submit an additional written notification per year is $8,863 per notification ((5 Compliance Manager hours x $344) + (5 Attorney hours x $462) + (6 Senior Systems Analyst hours x $316) + (1 Assistant General Counsel x $518) + (6 Senior Business Analyst hours x $305) + (1 Chief Compliance Officer hour x $589)). $8,863 per notification x 3 notifications each year = $26,589.

[2] $8,863 per notification x 8 notifications each year = $70,904.

---

506 3 additional notifications x 24 hours per notification = 72 hours. *See supra* note 497 (discussing the three additional notifications for each Current SCI Entity).

507 8 notifications x 24 hours per notification = 192 hours. *See supra* note 498 (discussing the eight notifications for each New SCI Entity).

As for Rule 1002(b)(3), the Commission estimates that, based on past experience, each Current SCI entity will submit 1 additional written update and 1 additional oral update each year and each New SCI Entity will submit 2 written updates (on Form SCI) and 2 oral updates.[508] The Commission estimates that each written update will require 6 hours and each oral update will require 4.5 hours.[509] The Commission estimates a total burden of 10.5 hours[510] for Current SCI Entities and 21 hours[511] for New SCI Entities. The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

| **Respondent Type** | **Estimated Respondents** | **Burden Hours per SCI Entity** | **Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity)** |
|---|---|---|---|
| Current SCI Entities | 47 entities | 10.5 hours | 493.5 hours |
| New SCI Entities | 23 entities | 21 hours | 483 hours |

508 The Commission's currently approved baseline for the number of updates submitted by an SCI entity pursuant to Rule 1002(b)(3) is one written update and one oral update each year, for a total of two updates per a year. *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission estimates that as a result of the three additional SCI events resulting from the additional systems intrusions each SCI entity is potentially required to be report, the total number of updates would increase to two written updates and two oral updates each year, for a total of four updates per a year.

509 The Commission-approved baseline for the burden hours for each update are 6 hours for the written update (1.5 Compliance Manager hours + 1.5 Attorney hours + 1.5 Senior Systems Analyst hours + 1.5 Senior Business Analyst hours) and 4.5 hours for the oral update (0.75 Compliance Manager hours + 0.75 Attorney hours + 1.5 Senior Systems Analyst hours + 1.5 Senior Business Analyst hours). *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission does not propose to change the estimated burden hours at this time and notes that the estimated hours for the Senior Systems Analyst and Senior Business Analyst regarding the oral update reflect a correction to a typographical error in the 2022 PRA Supporting Statement.

510 1 written notification x 6 hours per written notification + 1 oral notification x 4.5 hours per oral notification = 10.5 hours.

511 2 written notifications x 6 hours per written notification + 2 oral notifications x 4.5 hours per oral notification = 21 hours.

The table below summarizes the Commission's estimates for the cost of compliance associated with the ongoing reporting burden for Current SCI Entities and New SCI Entities:

| Respondent Type | Estimated Respondents | Average Internal Cost of Compliance per SCI Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|
| Current SCI Entities | 47 entities | $3,677[1] | $172,819 |
| New SCI Entities | 23 entities | $7,354[2] | $169,142 |

[1] The average internal cost of compliance for each SCI entity to submit an additional written update is $2,141 per notification ((1.5 Compliance Manager hours x $344) + (1.5 Attorney hours x $462) + (1.5 Senior Systems Analyst hours x $316) + (1.5 Senior Business Analyst hours x $305)).

The average internal cost of compliance for each SCI entity to submit an additional oral update is $1,536 ((0.75 Compliance Manager hours x $344) + (0.75 Attorney hours x $462) + (1.5 Senior Systems Analyst hours x $316) + (1.5 Senior Business Analyst hours x $305)).

$2,141 + $1,536 = $3,677 for each Current SCI Entity to submit two additional updates (one written update and one oral update).

[2] $2,141 per written update x 2 written updates per year + $1,536 per oral update x 2 oral updates per year = $7,354 for each New SCI Entity to submit updates in compliance with Rule 1002(b)(3).

As for Rule 1002(b)(4), the Commission estimates that Current SCI Entities will submit an additional 3 reports per year above and beyond the current baseline[512] and New SCI Entities will submit 8 reports per year.[513] The Commission estimates that compliance

---

512 The Commission's currently approved baseline for the number of reports submitted by an SCI entity pursuant to Rule 1002(b)(4) is five reports per year. *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission estimates that as a result of the increase in the estimated number of SCI events from five events to eight events, SCI entities would potentially be required to submit an additional three reports per year.

550 As noted earlier, the Commission estimates that New SCI Entities would submit both the baseline estimate of five reports and the additional three reports, for a total of eight reports.

with Rule 1002(b)(4) for a particular SCI event will require 35 hours.[514] The Commission estimates that each Current SCI Entity will incur 105 hours[515] and each New SCI Entity will incur 280 hours[516] to meet the requirements of Rule 1002(b)(4). The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

| **Respondent Type** | **Estimated Respondents** | **Burden Hours per SCI Entity** | **Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity)** |
|---|---|---|---|
| Current SCI Entities | 47 entities | 105 hours | 4,935 hours |
| New SCI Entities | 23 entities | 280 hours | 6,440 hours |

The Commission estimates that the average internal cost of compliance per notification is $13,672.[517] The table below summarizes the Commission's estimates for the cost of compliance associated with the ongoing reporting burden for Current SCI Entities and New SCI Entities:

---

514 The Commission's currently approved baseline for burden hours each SCI entity would incur to comply with Rule 1002(b)(4) for each SCI event would be 35 hours (8 Compliance Manager hours + 8 Attorney hours + 7 Senior Systems Analyst hours + 2 Assistant General Counsel hours + 1 General Counsel hour + 2 Chief Compliance Officer hours + 7 Senior Business Analyst hours). *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission does not propose to change the estimated burden hours at this time.

515 3 notifications each year × 35 hours per notification = 105 hours.

516 8 notifications each year × 35 hours per notification = 280 hours.

517 (8 Compliance Manager hours x $344) + (8 Attorney hours x $462) + (7 Senior Systems Analyst hours x $316) + (2 Assistant General Counsel hours x $518) + (1 General Counsel hour x $663) + (2 Chief Compliance Officer hours x $589) + (7 Senior Business Analyst hours x $305) = $13,672.

| Respondent Type | Estimated Respondents | Average Internal Cost of Compliance per SCI Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|
| Current SCI Entities | 47 entities | $41,016[1] | $1,927,752 |
| New SCI Entities | 23 entities | $109,376[2] | $2,515,648 |

[1] $13,672 per notification x 3 notifications each year = $41,016.

[2] $13,672 per notification x 8 notifications per year = $109,376 average internal cost of compliance for each New SCI Entity.

### c. Rule 1002(b)(5)

The Commission estimates that eliminating systems intrusions from the SCI events reported as de minimis events[518] on the quarterly reports reduces the burden for each SCI entity to submit the quarterly report by 10% less compared to the current baseline, or 36 hours.[519] Each Current SCI Entity would experience a decrease in its reporting burden of 4 hours per quarterly report,[520] for a total decrease of 16 hours per SCI entity.[521] As New SCI Entities are not currently required to meet this burden, they

---

[518] Systems intrusions, whether de minimis or non-de minimis, would be reported pursuant to Rules 1002(b)(1) through (4), as discussed earlier. *See* section III.C.3. The burdens for reporting all systems intrusions as non-de minimis events is discussed above. *See supra* notes 495-517 and accompanying text.

[519] The Commission's currently approved baseline for the initial and ongoing reporting burden to comply with the quarterly report requirement is 40 hours. *See* 2022 PRA Supporting Statement, *supra* note 471. 40 hours x 10% = 36 hours. This estimate includes 7 hours for a Compliance Manager, 7 hours for an Attorney, 9 hours for a Senior Systems Analyst, 1 hours for an Assistant General Counsel, 9 hours for a Senior Business Analyst, 1 hours for a General Counsel, and 2 hours for a Chief Compliance Officer.

[520] 40 hours (baseline estimate) – 36 hours (revised estimate) = 4 hours per quarterly report. This estimate includes 0.75 hours for a Compliance Manager, 0.75 hours for an Attorney, 1 hour for a Senior Systems Analyst, 0.2 hours for an Assistant General Counsel, 1 hours for a Senior Business Analyst, 0.1 hours for a General Counsel, and 0.2 hours for a Chief Compliance Officer.

[521] 4 quarterly submissions per year x 4 hours per submission = 16 hours decrease per SCI entity.

would newly incur a burden of 36 hours per report, for a total burden per SCI entity of 144 hours.[522]

The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

| Respondent Type | Estimated Respondents | Number of Reports | Hours per Report | Burden Hours per SCI Entity (Number of Reports x Hours per Report) | Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity) |
|---|---|---|---|---|---|
| Current SCI Entities | 47 entities | 4 reports | (4) hours | (16) hours | (752) hours |
| New SCI Entities | 23 entities | 4 reports | 36 hours | 144 hours | 3,312 hours |

The table below summarizes the Commission's estimates for the average internal cost of compliance associated with the ongoing reporting burden for Current SCI Entities and New SCI Entities:

| Respondent Type | Estimated Respondents | Number of Reports | Internal Cost of Compliance per Report | Average Internal Cost of Compliance per SCI Entity (Number of Reports x Internal Cost of Compliance per Report) | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|---|
| Current SCI Entities | 47 entities | 4 reports | $(1,513) [1] | $(6,052) [2] | $(284,444) |
| New SCI Entities | 23 entities | 4 reports | $13,619[3] | $54,476[4] | $1,252,948 |

1 (0.75 Compliance Manager hours x $344) + (0.75 Attorney hours x $462) + (1 Senior Systems Analyst hours x $316) + (0.2 Assistant General Counsel hours x $518) + (0.1 General Counsel hour x $663) + (0.2 Chief Compliance Officer hours x $589) + (1 Senior Business Analyst hours x $305) = $1,513.

2 $1,513 per notification x 4 notifications each year = $6,052 per Current SCI Entity.

3 (6.75 Compliance Manager hours x $344) + (6.75 Attorney hours x $462) + (9 Senior Systems Analyst hours x $316) + (1.8 Assistant General Counsel hours x $518) + (0.9 General Counsel hour x $663) + (1.8 Chief Compliance Officer hours x $589) + (9 Senior Business Analyst hours x $305) = $13,619.

4 $13,619 per notification x 4 notifications each year = $54,476 per New SCI Entity.

522 4 quarterly submissions per year x 36 hours per submission = 144 hours per SCI entity.

The Commission estimates that while SCI entities will handle internally most of the work associated with Rule 1002(b), SCI entities will seek outside legal advice in the preparation of certain Commission notifications. The Commission estimates that the total annual reporting cost of seeing outside legal advice is $5,800 per SCI entity.[523] Because Rule 1002(b) will impose approximately 32 reporting requirements[524] per SCI entity per year and each required notification will be require an average of $181.25.[525] The total annual reporting costs for Current SCI Entities and New SCI Entities is summarized below:

---

523 The Commission-approved baseline for the annual reporting cost of seeking outside legal advice is $5,800 per SCI entity. *See* 2022 PRA Supporting Statement, *supra* note 471.

524 The Commission-approved baseline for the number of reporting requirements required by Rule 1002(b) is 21 requirements for each SCI entity. *See* 2022 PRA Supporting Statement, *supra* note 471. The proposed amendments add an additional 11 reporting requirements (3 immediate notifications + 3 24-hour notifications + 2 updates pertaining to an SCI event + 3 interim/final notifications). 21 + 11 = 32 reporting requirements.

525 $5,800 per SCI entity / 32 reporting requirements = $181.25 per reporting requirement.

| Rule | Type of Respondent | Number of Respondents | Number of Reporting Requirements | Cost per Reporting Requirement | Cost per SCI Entity (Number of Reporting Requirements x Cost per Reporting Requirement) | Total Cost Burdens (Cost per SCI Entity x Number of Respondents) |
|---|---|---|---|---|---|---|
| Rule 1002(b)(1) | Current SCI Entities | 47 | 3 | $181.25 | $544 | $25,556 |
| | New SCI Entities | 23 | 8 | $181.25 | $1,450 | $33,350 |
| Rule 1002(b)(2) | Current SCI Entities | 47 | 3 | $181.25 | $544 | $25,556 |
| | New SCI Entities | 23 | 8 | $181.25 | $1,450 | $33,350 |
| Rule 1002(b)(3) | Current SCI Entities | 47 | 2 | $181.25 | $363 | $17,038 |
| | New SCI Entities | 23 | 4 | $181.25 | $725 | $16,675 |
| Rule 1002(b)(4) | Current SCI Entities | 47 | 3 | $181.25 | $544 | $25,556 |
| | New SCI Entities | 23 | 8 | $181.25 | $1,450 | $33,350 |
| Rule 1002(b)(5) | Current SCI Entities | 47 | 0 | $181.25 | $0 | $0 |
| | New SCI Entities | 23 | 4 | $181.25 | $725 | $16,675 |

#### d. Rule 1002(c)

The Commission anticipates that the proposed amendment will newly impose the information dissemination requirements of Rule 1002(c)(1) on New SCI Entities, and New SCI Entities will incur the same burdens that Current SCI Entities already incur to

comply with these requirements.[526] The table below summarizes the burden that would be newly imposed on New SCI Entities:

| Rule | Respondent Type | Estimated Respondents | Number of Dissemination | Hours per Dissemination | Burden Hours per SCI Entity (Number of Reports x Hours per Report) | Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity) |
|---|---|---|---|---|---|---|
| Rule 1002(c)(1)(i) | New SCI Entities | 23 entities | 3 information disseminations[1] | 7 hours[2] | 21 hours | 483 hours |
| Rule 1002(c)(1)(ii) and (iii) | | | 9 updates[3] | 13 hours[4] | 117 hours | 2,691 hours |

1 The Commission's currently approved baseline for the number of each SCI entity's information disseminations per year under Rule 1002(c)(1)(i) is three information disseminations. *See* 2022 PRA Supporting Statement, *supra* note 471.

2 The Commission's currently approved baseline is that each information dissemination under Rule 1002(c)(1)(i) would require 7 hours. This includes 1 Compliance Manager hour, 2.67 Attorney hours, 1 Senior System Analyst hour, 0.5 General Counsel hours, 0.5 Director of Compliance hours, 0.5 Chief Compliance Officer hours, 0.5 Corporate Communications Manager hours, and 0.33 Webmasters hours. *See* 2022 PRA Supporting Statement, *supra* note 471.

3 The Commission's currently approved baseline for Rule 1002(c)(1)(ii) and (iii) is that each SCI entity will disseminate three updates for each SCI event. 3 updates per SCI Event x 3 SCI events = 9 updates each year.

4 The Commission's currently approved baseline is that each information dissemination under Rule 1002(c)(1)(ii) and (iii) would require 13 hours. This includes 2 Compliance Manager hours, 4.67 Attorney hours, 2 Senior System Analyst hour, 1 General Counsel hours, 1 Director of Compliance hours, 1 Chief Compliance Officer hours, 1 Corporate Communications Manager hours, and 0.33 Webmasters hours. *See* 2022 PRA Supporting Statement, *supra* note 471, at 25-26.

The table below summarizes the Commission's estimates for the average internal cost of compliance associated with the ongoing reporting burden for Current SCI Entities and New SCI Entities:

526 Current SCI Entities are already required to comply with Rule 1002(c)(1). The burdens for compliance are summarized in the most recent PRA Supporting Statement. *See* 2022 PRA Supporting Statement, *supra* note 471. The proposed amendments impose no additional burden related to this section. The Commission does not anticipate that New SCI Entities would incur burdens beyond what is estimated in the 2022 PRA Supporting Statement.

| Rule | Respondent Type | Estimated Respondents | Average Internal Cost of Compliance per SCI Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| Rule 1002(c)(1)(i) | New SCI Entities | 23 entities | $9,212[1] | $211,876 |
| Rule 1002(c)(1)(ii) and (iii) | | | $51,666[2] | $1,188,318 |

[1] (1 Compliance Manager hours x $344) + (2.67 Attorney hours x $462) + (1 Senior Systems Analyst hours x $316) + (0.5 General Counsel hour x $663) + (0.5 Chief Compliance Officer hours x $589) + (0.5 Director of Compliance hours x $542) + (0.5 Corporate Communications Manager hours x $378) + (0.33 Webmaster hours x $276) = $3,071. $3,071 per notification x 3 notifications each year = $9,212.

[2] (2 Compliance Manager hours x $344) + (4.67 Attorney hours x $462) + (2 Senior Systems Analyst hours x $316) + (1 General Counsel hour x $663) + (1 Chief Compliance Officer hours x $589) + (1 Director of Compliance hours x $542) + (1 Corporate Communications Manager hours x $378) + (0.33 Webmaster hours x $276) = $5,741. $5,741 per notification x 9 notifications each year = $51,666.

With respect to the Rule 1002(c)(2) requirement to disseminate information regarding systems intrusions, the Commission estimates that each Current SCI Entity will disseminate information regarding 3 systems intrusions each year and each New SCI Entity will disseminate information regarding 4 systems intrusions each year.[527] The Commission estimates that each dissemination under Rule 1002(c)(2) will require 10 hours.[528]

---

[527] The Commission's currently approved baseline for the number of each SCI entity's information disseminations per year under Rule 1002(c)(2) is that each SCI entity will disseminate information about one systems intrusion each year. *See* 2022 PRA Supporting Statement, *supra* note 471. As discussed above, the Commission estimates an additional three SCI events (*i.e.*, three additional systems intrusions) as a result of the additional types of systems intrusions added to the definition systems intrusions in Rule 1000 and the elimination of systems intrusions from the de minimis SCI events reported quarterly in Rule 1002(b)(5). The Commission estimates that each SCI entity would disseminate information related to four systems intrusions each year. Each Current SCI Entity would disseminate information for three systems intrusions beyond the baseline estimate of one systems intrusion. As New SCI Entities will newly incur this burden, and as a result will report four systems intrusions.

[528] The Commission's currently approved baseline is that each dissemination under Rule 1002(c)(2) will require 10 hours. *See* 2022 PRA Supporting Statement, *supra* note 471.

The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

| Respondent Type | Estimated Respondents | Burden Hours per SCI Entity | Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity) |
|---|---|---|---|
| Current SCI Entities | 47 entities | 30 hours[1] | 1,410 hours |
| New SCI Entities | 23 entities | 40 hours[2] | 920 hours |

[1] 3 information disseminations x 10 hours per dissemination = 30 hours.

[2] 4 information disseminations x 10 hours per dissemination = 40 hours.

The Commission estimates that the average internal cost of compliance per notification is $4,406.[529] The table below summarizes the Commission's estimates for the cost of compliance associated with the ongoing reporting burden for Current SCI Entities and New SCI Entities:

| Respondent Type | Estimated Respondents | Average Internal Cost of Compliance per SCI Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|
| Current SCI Entities | 47 entities | $13,218[1] | $621,246 |
| New SCI Entities | 23 entities | $17,624[2] | $405,352 |

[1] $4,406 per notification x 3 information disseminations each year = $13,218.

[2] $4,406 per notification x 4 information disseminations per year = $17,624.

The Commission believes SCI entities will seek outside legal advice in the preparation of the information dissemination under Rule 1002(c). The Commission

---

[529] (1.5 Compliance Manager hours x $344) + (3.67 Attorney hours x $462) + (1.5 Senior Systems Analyst hours x $316) + (0.75 General Counsel hour x $633) + (0.75 Director of Compliance hours x $542) + (0.75 Chief Compliance Officer hours x $589) + (0.75 Corporate Communications Manager hours x $378) + (0.33 Webmasters hours x $276) = $4,406 per notification.

estimates that the total annual reporting cost of seeing outside legal advice is $3,320 per SCI entity.[530] Because Rule 1002(c) will impose approximately 16 third-party disclosure requirements[531] per SCI entity per year and each required disclosure will be require an average of $207.50.[532] The total annual reporting costs for Current SCI Entities and New SCI Entities are summarized below:

| Rule | Respondent Type | Number of Respondents | Number of Disclosures | Cost per Disclosure | Cost per SCI Entity (Number of Disclosures x Cost per Disclosure) | Total Cost Burdens (Cost per SCI Entity x Number of Respondents) |
|---|---|---|---|---|---|---|
| Rule 1002(c)(1)(i) | New SCI Entities | 23 | 3 | $207.50 | $622.50 | $14,317.50 |
| Rule 1002(c)(1)(ii) and (iii) | New SCI Entities | 23 | 9 | $207.50 | $1,867.50 | $42,952.50 |
| Rule 1002(c)(2) | Current SCI Entities | 47 | 3 | $207.50 | $622.50 | $29,257.50 |
| | New SCI Entities | 23 | 4 | $207.50 | $830 | $19,090 |

As noted above, Regulation SCI requires SCI entities to identify certain types of events and systems. The Commission believes that the identification of critical SCI systems, major SCI events, and de minimis SCI events will impose an initial one-time implementation burden on new SCI entities in developing processes to quickly and

---

530 The Commission-approved baseline for the annual reporting cost of seeking outside legal advice is $3,320 per SCI entity. *See* 2022 PRA Supporting Statement, *supra* note 471.

531 The Commission-approved baseline for the number of disclosure requirements required by Rule 1002(c) is 13 requirements for each SCI entity. *See* 2022 PRA Supporting Statement, *supra* note 471. The proposed amendments add an additional 3 reporting requirements (3 additional information disseminations related to 3 additional systems intrusions). 13 + 3 = 16 disclosure requirements.

532 $3,320 per SCI entity/16 reporting requirements = $207.50 per reporting requirement.

correctly identify the nature of a system or event. The identification of these systems and events may also impose periodic burdens on SCI entities in reviewing and updating the processes. The Commission anticipates that the because the proposed amendment will newly impose the requirements of Rule 1002(b) on New SCI Entities, New SCI Entities will incur the burden to develop processes to comply with these requirements.[533] The Commission estimates that each New SCI entity will initially require 198 hours to establish criteria for identifying material systems changes and 39 hours to annually to review and update the criteria.[534] The table below summarizes the burden that would be newly imposed on New SCI Entities:

| **Respondent Type** | **Burden Type** | **Estimated Respondents** | **Burden Hours per Entity** | **Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity)** |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | 198 hours | 4,554 hours |
| | Annual | 23 entities | 39 hours | 897 hours |

The table below summarizes the Commission's estimates for the average internal cost of compliance for New SCI Entities:

533 Current SCI Entities are already required to comply with Rule 1003(a). The burdens for compliance are summarized in the most recent PRA Supporting Statement. *See* 2022 PRA Supporting Statement, *supra* note 471. The proposed amendments impose no additional burden related to this section.

534 These estimates reflect the Commission-approved baseline. *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission does not anticipate that New SCI Entities would incur burdens beyond what is estimated in the 2022 PRA Supporting Statement.

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | $78,144[1] | $1,797,312 |
| | Annual | 23 entities | $17,258[2] | $396,934 |

[1] (64 Compliance Manager hours x $344) + (64 Attorney hours x $462) + (20 Senior Systems Analyst hours x $316) + (20 Operations Specialist hours x $152) + (20 Chief Compliance Officer hours x $589) + (10 Director of Compliance hours x $542) = $78,144.

[2] (9 Compliance Manager hours x $344) + (9 Attorney hours x $462) + (3 Senior Systems Analyst hours x $316) + (3 Operations Specialist hours x $152) + (10 Chief Compliance Officer hours x $589) + (5 Director of Compliance hours x $542) = $17,258.

As discussed above in section III.C.3.c, the proposed amendments to the definition of systems intrusion would require SCI entities to establish reasonable written criteria to identify significant attempted unauthorized entries into the SCI systems or indirect SCI systems of an SCI entity. As this is a new burden for both Current SCI Entities and New SCI Entities, the Commission estimates an average burden across all

SCI entities of 89 hours[535] initially to establish the criteria for identifying material systems changes and 14.5 hours[536] annually to review and update the criteria.

The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

---

535 This estimate is based on the Commission's burden estimate for Rule 1001(a), because Rule 1001(a) requires policies and procedures. *See supra* notes 474-475 and accompanying text. Rule 1001(a) (excluding Rule 1001(a)(2)(vi)) requires a total of ten policy elements at a minimum, consisting of six currently required policy elements and four proposed policy elements. *See supra* notes 471 and 474. Because the proposed amendment to the definition of systems intrusion in Rule 1000 requires only one set of written criteria, the Commission estimates that the initial staff burden to draft the criteria required to identify significant attempted unauthorized systems intrusions is one-tenth of the initial staff burden to draft the policies and procedures required by Rule 1001(a)(excluding Rule 1001(a)(2)(vi)). 890 hours/10 policy elements = 89 burden hours per policy element. The 89 burden hours includes 25 hours for a Compliance Manager, 25 hours for an Attorney, 8 hours for a Senior Systems Analyst, and 8 hours for an Operations Specialist. The Commission also estimates that a Chief Compliance Officer will spend 15 hours and a Director of Compliance and a Director of Compliance will spend 8 hours reviewing the policies and procedures.

536 This estimate is based on the Commission's burden estimate for Rule 1001(a), because Rule 1001(a) requires policies and procedures. *See supra* notes 475-476 and accompanying text. Rule 1001(a) (excluding Rule 1001(a)(2)(vi)) requires a total of ten policy elements at a minimum, consisting of six currently required policy elements and four proposed policy elements. *See supra* notes 472 and 475. Because the proposed amendment to the definition of systems intrusion in Rule 1000 requires only one set of written criteria, the Commission estimates that the ongoing staff burden to review and update the criteria required to identify significant attempted unauthorized systems intrusions is one-tenth of the ongoing staff burden to review and update the policies and procedures required by Rule 1001(a) (excluding Rule 1001(a)(2)(vi)). 145 hours/10 policy elements = 14.5 burden hours per policy element. The 14.5 burden hours includes 2 hours for a Compliance Manager, 2 hours for an Attorney, 1 hours for a Senior Systems Analyst, and 1 hours for an Operations Specialist. The Commission also estimates that a Chief Compliance Officer will spend 5.5 hours and a Director of Compliance and a Director of Compliance will spend 3 hours reviewing the policies and procedures.

| Respondent Type | Burden Type | Estimated Respondents | Burden Hours per Entity | Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity) |
|---|---|---|---|---|
| Current SCI Entities | Initial | 47 entities | 89 hours | 4,183 hours |
| | Annual | 47 entities | 14.5 hours | 681.5 hours |
| New SCI Entities | Initial | 23 entities | 89 hours | 2,047 hours |
| | Annual | 23 entities | 14.5 hours | 333.5 hours |

The table below summarizes the Commission's estimates for the average internal cost of compliance for New SCI Entities:

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| Current SCI Entities | Initial | 47 entities | $37,065[1] | $1,742,055 |
| | Annual | 47 entities | $6,946[2] | $326,462 |
| New SCI Entities | Initial | 23 entities | $37,065[3] | $852,495 |
| | Annual | 23 entities | $6,946[4] | $159,758 |

[1] (25 Compliance Manager hours x $344) + (25 Attorney hours x $462) + (8 Senior Systems Analyst hours x $316) + (8 Operations Specialist hours x $152) + (15 Chief Compliance Officer hours x $589) + (8 Director of Compliance hours x $542) = $37,065.

[2] (2 Compliance Manager hours x $344) + (2 Attorney hours x $462) + (1 Senior Systems Analyst hours x $316) + (1 Operations Specialist hours x $152) + (5.5 Chief Compliance Officer hours x $589) + (3 Director of Compliance hours x $542) = $6,946.

[3] *See supra* note 1 of this table.

[4] *See supra* note 2 of this table.

### 3. Rule 1003

The Commission anticipates that the proposed amendment will newly impose the Rule 1003(a) requirements to report material system changes on New SCI Entities, and

New SCI Entities will incur the same burdens that Current SCI Entities already incur to comply with these requirements.[537] The table below summarizes the burden that would be newly imposed on New SCI Entities:

| Rule | Respondent Type | Estimated Respondents | Number of Reports | Hours per Report | Burden Hours per SCI Entity (Number of Reports x Hours per Report) | Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity) |
|---|---|---|---|---|---|---|
| Rule 1003(a)(1) | New SCI Entities | 23 entities | 4 reports (1 per quarter) | 125 hours[1] | 500 hours | 11,500 hours |
| Rule 1003(a)(2) | | | 1 supplemental report[2] | 15 hours[3] | 15 hours | 345 hours |

[1] The Commission's currently approved baseline is that each quarterly report under Rule 1003(a)(1) would require 125 hours. This includes 7.5 Compliance Manager hours, 7.5 Attorney hours, 5 Chief Compliance Officer hours, 75 Senior System Analyst hours, and 30 Senior Business Analyst hours. *See* 2022 PRA Supporting Statement, *supra* note 471.

[2] The Commission's currently approved baseline for Rules 1002(c)(1)(ii) and (iii) is that each SCI entity will submit one supplemental report each year. *See* 2022 PRA Supporting Statement, *supra* note 471.

[3] The Commission's currently approved baseline is that the supplemental report under Rule 1003(a)(1) would require 15 hours. This includes 2 Compliance Manager hours, 2 Attorney hours, 1 Chief Compliance Officer hours, 7 Senior System Analyst hours, and 3 Senior Business Analyst hours. *See* 2022 PRA Supporting Statement, *supra* note 471.

The table below summarizes the average internal cost of compliance that would be newly imposed on New SCI Entities:

[537] Current SCI Entities are already required to comply with Rule 1003(a). The burdens for compliance are summarized in the most recent PRA Supporting Statement. *See* 2022 PRA Supporting Statement, *supra* note 471. The proposed amendments impose no additional burden related to this section. The Commission does not anticipate that New SCI Entities would incur burdens beyond what is estimated in the 2022 PRA Supporting Statement.

| Rule | Respondent Type | Estimated Respondents | Number of Reports | Cost of Compliance per Report | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|---|---|
| Rule 1003(a)(1) | New SCI Entities | 23 entities | 4 reports (1 per quarter) | $41,480 hours[1] | $167,360[2] | $3,849,280 |
| Rule 1003(a)(2) | | | 1 supplemental report | $5,328 hours[3] | $5,328 | $122,544 |

[1] (7.5 Compliance Manager hours x $344) + (7.5 Attorney hours x $462) + (5 Chief Compliance Officer hours x $589) + (75 Senior Systems Analyst hours x $316) + (30 Senior Business Analyst hours x $305) = $41,840.

[2] $41,480 per report x 4 reports each year = $167,360.

[3] (2 Compliance Manager hours x $344) + (2 Attorney hours x $462) + (1 Chief Compliance Officer hours x $589) + (7 Senior Systems Analyst hours x $316) + (3 Senior Business Analyst hours x $305) = $5,328.

Rule 1003(a)(1) requires each SCI entity to establish reasonable written criteria for identifying a change to its SCI systems and the security of indirect SCI systems as material. The Commission anticipates that the proposed amendment will newly impose these requirements on New SCI Entities, and New SCI Entities will incur the same burdens that Current SCI Entities already incur to comply with these requirements.[538] The Commission estimates that each New SCI entity will initially require 114 hours to establish criteria for identifying material systems changes and 27 hours to annually to review and update the criteria.[539] The table below summarizes the burden that would be newly imposed on New SCI Entities:

---

538 Current SCI Entities are already required to comply with Rule 1003(a). The burdens for compliance are summarized in the most recent PRA Supporting Statement. *See* 2022 PRA Supporting Statement, *supra* note 471. The proposed amendments impose no additional burden related to this section.

539 These estimates reflect the Commission-approved baseline. *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission does not anticipate that New SCI Entities would incur burdens beyond what is estimated in the 2022 PRA Supporting Statement.

| Respondent Type | Burden Type | Estimated Respondents | Burden Hours per Entity | Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity) |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | 114 hours | 2,622 hours |
| | Annual | 23 entities | 27 hours | 621 hours |

The table below summarizes the Commission's estimates for the cost of compliance for New SCI Entities:

| Respondent Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|
| New SCI Entities | 23 entities | $47,672[1] | $1,096,456 |
| | | $12,929[2] | $297,367 |

[1] (32 Compliance Manager hours x $344) + (32 Attorney hours x $462) + (10 Senior Systems Analyst hours x $316) + (10 Operations Specialist hours x $152) + (20 Chief Compliance Officer hours x $589) + (10 Director of Compliance hours x $542) = $47,672.

[2] (4.5 Compliance Manager hours x $344) + (4.5 Attorney hours x $462) + (1.5 Senior Systems Analyst hours x $316) + (1.5 Operations Specialist hours x $152) + (10 Chief Compliance Officer hours x $589) + (5 Director of Compliance hours x $542) = $12,929.

The Commission does not expect SCI entities to incur any external PRA costs in connection with the reports required under Rule 1003(a).

As for Rule 1003(b), each Current SCI Entity is already required to perform an SCI review and therefore already incurs a baseline burden[540] for compliance, so the

[540] The Commission's currently approved baseline for the annual recordkeeping burden of conducting an SCI review and submitting the SCI review to senior management of the SCI entity for review is 690 hours (35 Compliance Manager hours + 80 Attorney hours + 375 Senior Systems Analyst hours + 5 General Counsel hours + 5 Director of Compliance hours + 20 Chief Compliance Officer hours +170 Internal Audit Manager hours). *See* 2022 PRA Supporting Statement, *supra* note 471.

amendments should only impose a burden required to comply with the additional requirements. Presently, none of the New SCI Entities are required to comply with the requirements of Rule 1003(b), but the proposed amendments will newly impose both the baseline burden to conduct the SCI review and the additional burden to meet the proposed requirements for the SCI review.

The Commission estimates that the proposed additional requirements for conducting the SCI review will increase the burden of conducting the SCI review and submitting the report by 50%. With respect to Rule 1003(b)(1) and (2), the Commission estimates an additional burden for Current SCI Entities of 345 hours[541] and 1,035 hours[542] for New SCI Entities. The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

| **Respondent Type** | **Estimated Respondents** | **Burden Hours per Entity** | **Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity)** |
|---|---|---|---|
| Current SCI Entities | 47 entities | 345 hours | 16,215 hours |
| New SCI Entities | 23 entities | 1,035 hours | 23,805 hours |

The table below summarizes the Commission's estimates for the average internal cost of compliance for Current SCI Entities and New SCI Entities:

---

541 690 hours (baseline burden) x 0.5 = 345 hours. This estimate includes 17.5 hours for a Compliance Manager, 40 hours for an Attorney, 187.5 hours for a Senior Systems Analyst, 2.5 hours for General Counsel, 10 hours for a Chief Compliance Officer, 2.5 hours for a Director of Compliance, and 85 hours for an Internal Audit Manager.

542 690 baseline burden hours + 345 additional burden hours = 1,035 hours. This estimate includes 52.5 hours for a Compliance Manager, 120 hours for an Attorney, 562.5 hours for a Senior Systems Analyst, 7.5 hours for General Counsel, 30 hours for a Chief Compliance Officer, 7.5 hours for a Director of Compliance, and 255 hours for an Internal Audit Manager.

| Respondent Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|
| Current SCI Entities | 47 entities | $123,848[1] | $5,820,856 |
| New SCI Entities | 23 entities | $371,543[2] | $8,545,489 |

[1] (17.5 Compliance Manager hours x $344) + (40 Attorney hours x $462) + (187.5 Senior Systems Analyst hours x $316) + (2.5 General Counsel hours x $663) + (2.5 Director of Compliance hours x $542) + (10 Chief Compliance Officer hours x $589) + (85 Internal Audit Manager hours x $367) = $123,848.

[2] (52.5 Compliance Manager hours x $344) + (120 Attorney hours x $462) + (562.5 Senior Systems Analyst hours x $316) + (7.5 General Counsel hours x $663) + (7.5 Director of Compliance hours x $542) + (30 Chief Compliance Officer hours x $589) + (255 Internal Audit Manager hours x $367) = $371,543.

With respect to Rule 1003(b)(3), the Commission estimates that the burden for SCI entities would increase to 25 hours from the current baseline estimate.[543] Thus, the Commission estimates an additional burden for Current SCI Entities of 24 hours[544] and a new burden of 25 hours[545] for New SCI Entities. The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

---

543 The Commission's currently approved baseline to submit the report for the SCI review to the board of directors is 1 hour (1 Attorney hour). *See* 2022 PRA Supporting Statement, *supra* note 471. The Commission estimates an increase to 25 hours as a result of the proposed requirement that senior management provide a response to the SCI review.

544 25 hours (revised estimate) – 1 hour (baseline estimate) = 24 hours. This estimate includes 1 hours for a Compliance Manager, 3 hours for an Attorney, 13 hours for a Senior Systems Analyst, 1 hours for a Chief Compliance Officer, and 6 hours for an Internal Audit Manager.

545 This estimate includes 1 hours for a Compliance Manager, 3 hours for an Attorney, 14 hours for a Senior Systems Analyst, 1 hours for a Chief Compliance Officer, and 6 hours for an Internal Audit Manager.

| Respondent Type | Estimated Respondents | Burden Hours per Entity | Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity) |
|---|---|---|---|
| Current SCI Entities | 47 entities | 24 hours | 1,128 hours |
| New SCI Entities | 23 entities | 25 hours | 575 hours |

The table below summarizes the Commission's estimates for the average internal cost of compliance for Current SCI Entities and New SCI Entities:

| Respondent Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|
| Current SCI Entities | 47 entities | $8,629[1] | $405,563 |
| New SCI Entities | 23 entities | $8,945[2] | $205,735 |

[1] (1 Compliance Manager hours x $344) + (3 Attorney hours x $462) + (13 Senior Systems Analyst hours x $316) + (1 Chief Compliance Officer hours x $589) + (6 Internal Audit Manager hours x $367) = $8,629.

[2] (1 Compliance Manager hours x $344) + (3 Attorney hours x $462) + (14 Senior Systems Analyst hours x $316) + (1 Chief Compliance Officer hours x $589) + (6 Internal Audit Manager hours x $367) = $8,945.

Rule 1003(b) imposes recordkeeping costs for SCI entities. The Commission estimates that while SCI entities will handle internally some or most of the work associated with compliance with Rule 1003(b), SCI entities will outsource some of the work associated with an SCI review. The Commission estimates that the proposed amendments to the SCI review would increase the annual recordkeeping cost by 50%

beyond the current baseline.[546] The table below summarizes the Commission's estimates for the cost of outsourcing for Current SCI Entities and New SCI Entities:

| Respondent Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|
| Current SCI Entities | 47 entities | $25,000[1] | $1,175,000 |
| New SCI Entities | 23 entities | $75,000[2] | $1,725,000 |

[1] 50,000 (baseline estimate) x 0.5 = $25,000.

[2] 50,000 (baseline estimate) x 1.5 = $75,000.

### 4. Rule 1004

The rules under Regulation SCI that would require an SCI entity to mandate member or participant participation in business continuity and disaster recovery plan testing are discussed more fully in sections II.B, and the proposed amendments including third-party providers in the requirement are discussed more fully in III.C.2 above.

Current SCI Entities are already required to establish standards and designate members or participants for testing pursuant to Rule 1004 and therefore already incur baseline initial[547] and ongoing burdens[548] for complying with Rule 1004, so the

---

546 The Commission-approved baseline for the annual recordkeeping cost per SCI entity of outsourcing is $50,000. *See* 2022 PRA Supporting Statement, *supra* note 471.

547 The Commission's currently approved baseline for average initial compliance burden per respondent with 17 CFR 242.1004(a) ("Rule 1004(a)") (*i.e.*, establishment of standards for the designation of members and participants) and (c) (*i.e.*, the coordination of testing on an industry- or sector-wide basis) is 360 hours (40 Compliance Manager hours + 60 Attorney hours + 20 Assistant General Counsel hours + 60 Senior Operations Manager hours + 140 Operations Specialist hours + 26 Chief Compliance Officer hours + 14 Director of Compliance hours). *See* 2022 PRA Supporting Statement, *supra* note 471. The estimate of 360 hours includes the burden for designating members or participants for testing, as required by 17 CFR 242.1004(b) ("Rule 1004(b)"). *Id.* at 18 n.50.

548 The average annual compliance burden for each SCI entity to review and update the policies and procedures is 135 hours for each entity that is not a plan processor. *See* 2022 PRA Supporting Statement, *supra* note 471. None of the New SCI Entities are plan processors, so the Commission is applying the 135 hour estimate to the New SCI Entities.

amendments should only impose a burden required to comply with the additional requirements. Presently, none of the New SCI Entities are required to comply with the requirements of Rule 1004, but the proposed amendments will newly impose both the baseline burden to establish standards for the designation of members and participants for BC/DR testing and coordinate industry or sector-wide basis testing and additional burden to establish standards for the designation of third-party providers for BC/DR testing and coordinate industry or sector-wide basis testing for third-party providers. The Commission estimates an initial compliance burden of 90 hours[549] for Current SCI Entities and 450 hours[550] for New SCI Entities. The Commission estimates an annual compliance burden of 34 hours[551] for Current SCI Entities and 169 hours[552] for New SCI Entities. The table below summarizes the initial and ongoing annual burden estimates for Current SCI Entities and New SCI Entities:

---

549 The Commission estimates that the additional burden to establish standards for the designation of third-party providers for BC/DR testing and coordinate testing would be 25% of the 360 hour baseline burden hours. 360 hours x 0.25 = 90 hours. The burden hours include 10 Compliance Manager hours, 15 Attorney hours, 5 Assistant General Counsel hours, 35 Operations Specialist hours, 6 Chief Compliance Officer hours, 4 Director of Compliance hours, and 15 Senior Operations Manager hours.

550 360 baseline burden hours + 90 additional burden hours = 450 hours.

551 The Commission estimates that the additional annual burden would be 25% of the 135 hour baseline burden hours, or 34 hours (135 hours x 0.25). The burden hours include 3 Compliance Manager hours, 3 Attorney hours, 1 Assistant General Counsel hours, 18 Operations Specialist hours, 3 Chief Compliance Officer hours, 1 Director of Compliance hours, and 5 Senior Operations Manager hours.

552 135 baseline burden hours + 34 additional burden hours = 169 hours.

| Respondent Type | Burden Type | Estimated Respondents | Burden Hours per Entity | Estimated Burden Hours for All Entities (Estimated Respondents x Burden Hours per Entity) |
|---|---|---|---|---|
| Current SCI Entities | Initial | 47 entities | 90 hours | 4,230 hours |
| | Annual | 47 entities | 34 hours | 1,598 hours |
| New SCI Entities | Initial | 23 entities | 450 hours | 10,350 hours |
| | Annual | 23 entities | 169 hours | 3,887 hours |

The table below summarizes the Commission's estimates for the cost of compliance for Current SCI Entities and New SCI Entities:

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| Current SCI Entities | Initial | 47 entities | $ 30,072[1] | $1,413,384 |
| | Annual | 47 entities | $ 10,011[2] | $470,517 |
| New SCI Entities | Initial | 23 entities | $ 150,478[3] | $3,460,994 |
| | Annual | 23 entities | $ 50,331[4] | $1,157,613 |

[1] (10 Compliance Manager hours x $344) + (15 Attorney hours x $462) + (5 Assistant General Counsel hours x $518) + (35 Operations Specialist hours x $152) + (6 Chief Compliance Officer hours x $589) + (4 Director of Compliance hours x $542) + (15 Senior Operations Manager hours x $406) = $30,072.

[2] (3 Compliance Manager hours x $344) + (3 Attorney hours x $462) + (1 Assistant General Counsel hours x $518) + (18 Operations Specialist hours x $152) + (3 Chief Compliance Officer hours x $589) + (1 Director of Compliance hours x $542) + (5 Senior Operations Manager hours x $406) = $10,011.

[3] (50 Compliance Manager hours x $344) + (75 Attorney hours x $462) + (25 Assistant General Counsel hours x $518) + (175 Operations Specialist hours x $152) + (32.5 Chief Compliance Officer hours x $589) + (17.5 Director of Compliance hours x $542) + (75 Senior Operations Manager hours x $406) = $150,478.

[4] (13 Compliance Manager hours x $344) + (18 Attorney hours x $462) + (6 Assistant General Counsel hours x $518) + (88 Operations Specialist hours x $152) + (13 Chief Compliance Officer hours x $589) + (6 Director of Compliance hours x $542) + (25 Senior Operations Manager hours x $406) = $50,331.

The Commission continues to believe that SCI entities (other than plan processors) would handle internally the work associated with the requirements of Rule 1004.

### 5. Rule 1005

Rules 1005 and 1007 impose on SCI entities recordkeeping requirements related to their compliance with Regulation SCI. These requirements would be newly imposed on New SCI Entities as a result of the proposed amendment. The table below summarizes the Commission's estimates as to the burden that each New SCI Entity would incur to meet the requirements of Rules 1005 and 1007:[553]

| Respondent Type | Burden Type | Estimated Respondents | Burden Hours per SCI Entity | Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity) |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | 170 hours[1] | 3,910 hours |
| | Annual | | 25 hours[2] | 575 hours |

[1] The Commission approved baseline estimate for each new non-SRO SCI entity to set up or modify a recordkeeping system is 170 hours. *See* 2022 PRA Supporting Statement, *supra* note 471.

[2] The Commission approved baseline estimate for each new non-SRO SCI entity to make, keep, and preserve records relating to compliance with Regulation SCI, as required by Rule 1005(b), is 25 hours. *See* 2022 PRA Supporting Statement, *supra* note 471.

The table below summarizes the average internal cost of compliance that would be newly imposed on New SCI Entities:

[553] Current SCI Entities are already required to comply with Rules 1005 and 1007. The burdens for compliance are summarized in the most recent PRA Supporting Statement. *See* 2022 PRA Supporting Statement, *supra* note 471. The proposed amendments impose no additional burden related to this section. The Commission does not anticipate that New SCI Entities would incur burdens beyond what is estimated in the 2022 PRA Supporting Statement.

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | $13,260[1] | $304,980 |
| | Annual | | $1,950[2] | $44,850 |

[1] 170 Compliance Clerk hours x $78 per hour = $13,260.

[2] 25 Compliance Clerk hours x $78 per hour = $1,950.

The recordkeeping requirements impose recordkeeping costs for SCI entities other than SCI SROs. The Commission estimates that a New SCI Entity other than an SCI SRO will incur a one-time cost of $900 for information technology costs for purchasing recordkeeping software, for a total of $20,700.[554]

**6. Rule 1006**

SCI entities submit Form SCI through the Electronic Form Filing System ("EFFS"), which is also used by SCI SROs to file Form 19b-4 filings. Access to EFFS establishes reporting burdens for all SCI entities. An SCI entity will submit to the Commission an External Application User Authentication Form ("EAUF") to register each individual at the SCI entity who will access the EFFS system on behalf of the SCI entity. The Commission is including in its burden estimates the reporting burden for completing the EAUF for each individual at a New SCI Entity that will request access to

[554] $900 per SCI entity x 21 SCI entities = $18,900.

EFFS.[555] The table below summarizes the initial and ongoing burdens that would be New SCI Entities would incur to establish access to EFFS:

| Respondent Type | Type of Burden | Estimated Respondents | Number of Individuals Requesting Access | Time to Complete EAUF | Burden Hours per SCI Entity (Number of Individuals Requesting Access x Time to Complete EAUF) | Burden Hours for All Respondents (Estimated Respondents x Burden Hours per SCI Entity) |
|---|---|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | 2 individuals[1] | 0.15 hours[2] | 0.3 hours | 6.9 hours |
| | Annual | | 1 individual[3] | | 0.15 hours | 3.5 hours |

[1] The Commission approved baseline estimate for the number of individuals per SCI entity who will request access to EFFS initially through the EAUF is two individuals. *See* 2022 PRA Supporting Statement, *supra* note 471.

[2] The Commission approved baseline estimate to complete the EAUF is 0.15 hours. *See* 2022 PRA Supporting Statement, *supra* note 471.

[3] The Commission approved baseline estimate for the number of individuals per SCI entity who will request access to EFFS annually through the EAUF is one individual. *See* 2022 PRA Supporting Statement, *supra* note 471.

The table below summarizes the average internal cost of compliance that would be newly imposed on New SCI Entities:

[555] Current SCI Entities would already have incurred these burdens, which are summarized in the most recent PRA Supporting Statement. *See* 2022 PRA Supporting Statement, *supra* note 471. The proposed amendments impose no additional burden related to this section. The Commission does not anticipate that New SCI Entities would incur burdens beyond what is estimated in the 2022 PRA Supporting Statement.

| Respondent Type | Burden Type | Estimated Respondents | Average Internal Cost of Compliance per Entity | Total Internal Cost of Compliance (Estimated Respondents x Average Internal Cost of Compliance per Entity |
|---|---|---|---|---|
| New SCI Entities | Initial | 23 entities | $139[1] | $3,197 |
| | Annual | | $69[2] | $1,587 |

[1] 0.3 Attorney hours x $462 = $139.

[2] 0.15 Attorney hours x $462 = $69.

Obtaining the ability for an individual to electronically sign a Form SCI imposes reporting costs for SCI entities. The table below summarizes the cost for individuals at each New SCI Entity to obtain digital IDs to sign Form SCI:

| Respondent Type | Estimated Respondents | Number of Individuals to Sign Form SCI | Cost to Obtain Digital ID | Cost per SCI Entity (Number of Individuals Requesting Access x Time to Complete EAUF) | Cost for All Respondents (Estimated Respondents x Burden Hours per SCI Entity) |
|---|---|---|---|---|---|
| New SCI Entities | 23 entities | 2 individuals[1] | $25[2] | $50 | $1,150 |

[1] The Commission approved baseline estimate for the number of individuals per SCI entity who will sign Form SCI each year is two individuals. *See* 2022 PRA Supporting Statement, *supra* note 471.

[2] The Commission approved baseline estimate to obtain a digital ID is $50. *See* 2022 PRA Supporting Statement, *supra* note 471.

### 7. Summary of the Information Collection Burden

The table below summarizes the Commission's estimate of the total hourly burden, total internal costs of compliance, and external cost estimates for SCI entities under Regulation SCI.

| Rule | Respondent Type | Burden Hours | | Costs of Compliance | |
|---|---|---|---|---|---|
| | | Initial | Annual | Initial | Annual |
| Policies and procedures required by Rule 1001(a) (except Rule 1001(a)(2)(vi)) (Recordkeeping) | Current SCI Entities | 18,142 | 2,726 | $6,804,989 | $1,099,941 |
| | New SCI Entities | 20,470 | 3,335 | $7,667,533 | $1,341,245 |
| Policies and procedures required by Rule 1001(a)(2)(vi) (Recordkeeping) | New SCI Entities | 3,680 | 3,335 | $1,402,540 | $1,204,740 |
| Costs for outside legal/consulting services in initial preparation of policies and procedures required by Rule 1001(a) (Recordkeeping) | Current SCI Entities | N/A | N/A | $1,365,350 | N/A |
| | New SCI Entities | N/A | N/A | $1,697,400 | N/A |
| **Policies and procedures required by Rule 1001(a) Total** | Current SCI Entities | 18,142 | 2,726 | $8,170,339 | $1,099,941 |
| | New SCI Entities | 24,150 | 6,670 | $10,767,473 | $2,545,985 |
| Policies and procedures required by Rule 1001(b) (Recordkeeping) | New SCI Entities | 6,210 | 2,185 | $2,222,720 | $808,220 |
| Costs for outside legal/consulting services in initial preparation of policies and procedures required by Rule 1001(b) (recordkeeping) | New SCI Entities | N/A | N/A | $621,000 | $0 |
| **Policies and procedures required by Rule 1001(b) Total** | New SCI Entities | 6,210 | 2,185 | $2,843,720 | $808,220 |
| **Policies and procedures required by Rule 1001(c) (Recordkeeping)** | New SCI Entities | 2,622 | 897 | $1,096,456 | $400,821 |
| **Mandate participation in certain testing required by Rule 1004 (Recordkeeping)** | Current SCI Entities | 4,230 | 1,598 | $1,413,384 | $470,517 |
| | New SCI Entities | 10,350 | 3,887 | $3,460,994 | $1,157,613 |
| SCI Event Notice Required By Rule 1002(b)(1) (Reporting) | Current SCI Entities | 235 | 235 | $81,663 | $81,663 |
| | New SCI Entities | 299 | 299 | $103,477 | $103,477 |
| External Legal Costs for Rule 1001(b)(1) (Reporting) | Current SCI Entities | N/A | N/A | $25,556 | $25,556 |
| | New SCI Entities | N/A | N/A | $33,350 | $33,350 |
| **SCI Event Notice Required By Rule 1002(b)(1) Total** | Current SCI Entities | 235 | 235 | $107,219 | $107,219 |
| | New SCI Entities | 299 | 299 | $136,827 | $136,827 |
| SCI Event Notice Required By Rule 1002(b)(2) (Reporting) | Current SCI Entities | 3,384 | 3,384 | $1,249,683 | $1,249,683 |
| | New SCI Entities | 4,416 | 4,416 | $1,630,792 | $1,630,792 |
| External Legal Costs for Rule | Current SCI Entities | N/A | N/A | $25,556 | $25,556 |

| | | | | | |
|---|---|---|---|---|---|
| 1001(b)(2) (Reporting) | New SCI Entities | N/A | N/A | $33,350 | $33,350 |
| **SCI Event Notice Required By Rule 1002(b)(2) Total** | Current SCI Entities | 3,384 | 3,384 | $1,275,239 | $1,275,239 |
| | New SCI Entities | 4,416 | 4,416 | $1,664,142 | $1,664,142 |
| SCI Event Notice Required By Rule 1002(b)(3) (Reporting) | Current SCI Entities | 493.5 | 493.5 | $172,819 | $172,819 |
| | New SCI Entities | 483 | 483 | $169,142 | $169,142 |
| External Legal Costs for Rule 1002(b)(3) (Reporting) | Current SCI Entities | N/A | N/A | $17,038 | $17,038 |
| | New SCI Entities | N/A | N/A | $16,675 | $16,675 |
| **SCI Event Notice Required By Rule 1002(b)(3) Total** | Current SCI Entities | 493.5 | 493.5 | $189,857 | $189,857 |
| | New SCI Entities | 483 | 483 | $185,817 | $185,817 |
| SCI Event Notice Required By Rule 1002(b)(4) (Reporting) | Current SCI Entities | 4,935 | 4,935 | $1,927,752 | $1,927,752 |
| | New SCI Entities | 6,440 | 6,440 | $2,515,648 | $2,515,648 |
| External Legal Costs for 1001(b)(4) (Reporting) | Current SCI Entities | N/A | N/A | $25,556 | $25,556 |
| | New SCI Entities | N/A | N/A | $33,350 | $33,350 |
| **SCI Event Notice Required By Rule 1002(b)(4) Total** | Current SCI Entities | 4,935 | 4,935 | $1,953,308 | $1,953,308 |
| | New SCI Entities | 6,440 | 6,440 | $2,548,998 | $2,548,998 |
| SCI Event Notice Required By Rule 1002(b)(5) (Reporting) | Current SCI Entities | (752) | (752) | ($284,444) | ($284,444) |
| | New SCI Entities | 3,312 | 3,312 | $1,252,948 | $1,252,948 |
| External Legal Costs for Rule 1002(b)(5) (Reporting) | Current SCI Entities | N/A | N/A | $0 | $0 |
| | New SCI Entities | N/A | N/A | $16,675 | $16,675 |
| **SCI Event Notice Required By Rule 1002(b)(5) Total** | Current SCI Entities | (752) | (752) | ($284,444) | ($284,444) |
| | New SCI Entities | 3,312 | 3,312 | $1,269,623 | $1,269,623 |
| Dissemination of information required by Rule 1002(c)(1) (Third-Party Disclosure) | New SCI Entities | 3,174 | 3,174 | $1,400,194 | $1,400,194 |
| External Legal Costs for Rule 1002(c)(1) (Third-Party Disclosure) | New SCI Entities | N/A | N/A | $57,270 | $57,270 |
| **Dissemination of information required by Rule 1002(c)(1) Total** | New SCI Entities | 3,174 | 3,174 | $1,457,464 | $1,457,464 |
| Dissemination of information required by Rule 1002(c)(2) (Third-Party Disclosure) | Current SCI Entities | 1,410 | 1,410 | $621,246 | $621,246 |
| | New SCI Entities | 920 | 920 | $405,352 | $405,352 |
| External Legal Costs for Rule 1002(c)(2) (Third-Party Disclosure) | Current SCI Entities | N/A | N/A | $29,257.50 | $29,257.50 |
| | New SCI Entities | N/A | N/A | $19,090 | $19,090 |
| **Dissemination of information required by Rule 1002(c)(2) Total** | Current SCI Entities | 1,410 | 1,410 | $650,503.5 | $650,503.5 |
| | New SCI Entities | 920 | 920 | $424,442 | $424,442 |

| | | | | | |
|---|---|---|---|---|---|
| **Burden to develop processes to identify the nature of a system or event** | New SCI Entities | 4,554 | 897 | $1,797,312 | $396,934 |
| **Establish reasonable written criteria for identifying a significant attempted unauthorized systems intrusion** | Current SCI Entities | 4,183 | 681.5 | $1,742,055 | $326,462 |
| | New SCI Entities | 2,047 | 333.5 | $852,495 | $159,758 |
| **Material systems change notice required by Rule 1003(a)(1) and (2) (Reporting)** | New SCI Entities | 11,845 | 11,845 | $3,971,824 | $3,971,824 |
| **Establish reasonable written criteria for identifying a material change to its SCI systems and the security of indirect SCI systems** | New SCI Entities | 2,622 | 621 | $1,096,456 | $297,367 |
| SCI review required by Rule 1003(b)(1) and (2) (Recordkeeping) | Current SCI Entities | 16,215 | 16,215 | $5,820,856 | $5,820,856 |
| | New SCI Entities | 23,805 | 23,805 | $8,545,489 | $8,545,489 |
| SCI review required by Rule 1003(b)(3) (Reporting) | Current SCI Entities | 1,128 | 1,128 | $405,563 | $405,563 |
| | New SCI Entities | 575 | 575 | $205,735 | $205,735 |
| External Legal Costs for Rule 1003(b) (Recordkeeping) | Current SCI Entities | N/A | N/A | $1,175,000 | $1,175,000 |
| | New SCI Entities | N/A | N/A | $1,725,000 | $1,725,000 |
| **SCI Review Costs (Rule 1003(b)) Total** | Current SCI Entities | 17,343 | 17,343 | $7,401,419 | $7,401,419 |
| | New SCI Entities | 24,380 | 24,380 | $10,476,224 | $10,476,224 |
| **Corrective action required by Rule 1002(a) (Recordkeeping)** | Current SCI Entities | 1,081 | N/A | $449,132 | N/A |
| | New SCI Entities | 3,151 | 897 | $1,316,244 | $396,934 |
| Recordkeeping required by Rules 1005/1007 (Recordkeeping) | New SCI Entities | 3,910 | 575 | $304,980 | $44,850 |
| One-time cost to purchase recordkeeping software Rules 1005/1007 (Recordkeeping) | New SCI Entities | N/A | N/A | $20,700 | N/A |
| **Total recordkeeping costs required by Rules 1005/1007** | New SCI Entities | 3,910 | 575 | $325,680 | $44,850 |
| Request access to EFFS (Rule 1006) (Reporting) | New SCI Entities | 6.9 | 3.5 | $3,197 | $1,587 |
| Rule 1006 - obtain digital IDs (Reporting) | New SCI Entities | N/A | N/A | $1,150 | $1,150 |
| **Total Costs to comply with Rule 1006** | New SCI Entities | 6.9 | 3.5 | $4,347 | $2,737 |

| | | | | | |
|---|---|---|---|---|---|
| Total | Overall Total | 169,576 | 104,289 | $68,764,549 | $41,536,601 |
| | Current SCI Entities | 54,685 | 32,054 | $23,068,011 | $13,190,021 |
| | New SCI Entities | 112,845 | 72,235 | $45,696,538 | $28,346,580 |
| Per Entity Hourly Burden/Cost | Current SCI Entities[1] | 1,163 | 682 | $490,808.75 | $280,639.75 |
| | New SCI Entities | 4,995 | 3,141 | $1,986,806 | $1,232,460 |

[1] As noted earlier, currently no SCI competing consolidators have registered with the Commission. *See supra* note 469. To the extent that a competing consolidator registers with the Commission, its initial and ongoing burdens as a result of the proposed amendments would be the same as the initial and ongoing burden per entity calculated for Current SCI Entities.

In summary, the estimated paperwork related compliance burdens for SCI entities as a result of the amendments are approximately 170,000 hours and $69 million initially and approximately 104,000 hours and $41 million annually.

**E. Collection of Information is Mandatory**

The collections of information pursuant to Regulation SCI is mandatory as to all entities subject to the rule.

**F. Confidentiality of Responses to Collection of Information**

The Commission expects that the written policies and procedures, processes, criteria, standards, or other written documents developed or revised by SCI entities pursuant to Regulation SCI will be retained by SCI entities in accordance with, and for the periods specified in 17 CFR 240.17a-1 ("Rule 17a-1" of the Exchange Act) and Rule 1005, as applicable. Should such documents be made available for examination or inspection by the Commission and its representatives, they would be kept confidential subject to the provisions of applicable law.[556] In addition, the information submitted to the Commission pursuant to Regulation SCI that is filed on Form SCI, as required by Rule 1006, will be treated as confidential, subject to applicable law, including amended

[556] *See*, *e.g.*, 15 U.S.C. 78x (governing the public availability of information obtained by the Commission); 5 U.S.C. 552 *et seq.*

17 CFR 240.24b-2 ("Rule 24b-2").[557] The information disseminated by SCI entities pursuant to Rule 1002(c) under Regulation SCI to their members or participants will not be confidential.

### G. Request for Comment

Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission solicits comment on the proposed collections of information in order to:

91. Evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the Commission, including whether the information would have practical utility;
92. Evaluate the accuracy of the Commission's estimates of the burden of the proposed collections of information;
93. Determine whether there are ways to enhance the quality, utility, and clarity of the information to be collected; and
94. Evaluate whether there are ways to minimize the burden of the collection of information on those who respond, including through the use of automated collection techniques or other forms of information technology.

Persons submitting comments on the collection of information requirements should direct them to the Office of Management and Budget, Attention: Desk Officer for the Securities and Exchange Commission, Office of Information and Regulatory Affairs, Washington, DC 20503, and should also send a copy of their comments to Vanessa A. Countryman, Secretary, Securities and Exchange Commission, 100 F Street NE,

---

557 *See*, *e.g.*, 15 U.S.C. 78x (governing the public availability of information obtained by the Commission); 5 U.S.C. 552 *et seq. See also* Form SCI section IV (including a provision stating "Confidential treatment is requested pursuant to 17 CFR 240.24b-2(g) ("Rule 24b-2(g)")).

Washington, DC 20549-1090, with reference to File Number S7-07-23. Requests for materials submitted to OMB by the Commission with regard to this collection of information should be in writing, with reference to File Number S7-07-23 and be submitted to the Securities and Exchange Commission, Office of FOIA/PA Services, 100 F Street NE., Washington, DC 20549-2736. As OMB is required to make a decision concerning the collections of information between 30 and 60 days after publication, a comment to OMB is best assured of having its full effect if OMB receives it within 30 days of publication.

## V. Economic Analysis

### A. Introduction

The Commission is sensitive to the economic effects, including the costs and benefits, of its rules. When engaging in rulemaking pursuant to the Exchange Act that requires the Commission to consider or determine whether an action is necessary or appropriate in the public interest, section 3(f) of the Exchange Act requires the Commission to consider, in addition to the protection of investors, whether the action would promote efficiency, competition, and capital formation. In addition, section 23(a)(2) of the Exchange Act requires the Commission in making rules pursuant to the Exchange Act to consider the impact any such rule would have on competition. The Exchange Act prohibits the Commission from adopting any rule that would impose a burden on competition not necessary or appropriate in furtherance of the purposes of the Exchange Act.

As explained above, the Commission believes that developments in the U.S. securities markets since the adoption of Regulation SCI in 2014 warrant expanding the scope of Regulation SCI as well as strengthening the obligations of SCI entities. These

developments include the growth of electronic trading, which allows greater volumes of securities transactions to take place across a multitude of trading systems in our markets. In addition, large institutional and other professional market participants today employ sophisticated methods to trade electronically on multiple venues simultaneously in ever-increasing volumes with increasing speed. In recent years, financial institutions have increasingly used and relied on third parties that provide information and communications technology systems.[558] Together, these developments have resulted in greater dispersal, sophistication, and interconnection of the systems underpinning our U.S. securities markets, thereby bringing potential new risks.

The proposed amendments to Regulation SCI would expand the definition of "SCI entity" to include a broader range of entities that perform key functions in U.S. securities market infrastructure, and update certain other definitions and provisions to take account of technological market developments, including cybersecurity and vendor management, since the adoption of Regulation SCI in 2014. The proposed expansion would add to the definition of "SCI entity" registered security-based swap data repositories, and registered broker-dealers exceeding certain asset and transaction activity thresholds, and the proposal would expand the category of exempt clearing agencies subject to Regulation SCI to include all clearing agencies exempted from registration. Additional proposed amendments to Regulation SCI are designed to update the

---

558 *See, e.g.*, FINRA, *Cloud Computing in the Securities Industry* (Aug. 16, 2021), *available at* https://www.finra.org/rules-guidance/key-topics/fintech/report/cloud-computing; *see also* Franklin Allen et al., *A Survey of Fintech Research and Policy Discussion*, 1 Rev. Corp. Fin. 259, 259 (2021) ("Cloud storage and cloud computing have also played increasing roles in payment systems, financial services, and the financial system overall"). *See also* Financial Stability Board, *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*, (discussion paper Nov. 9, 2020), *available at* https://www.fsb.org/wp-content/uploads/P091120.pdf.

requirements of Regulation SCI relating to: (i) systems classification and lifecycle management; (ii) vendor management; (iii) cybersecurity; (iv) SCI review; (v) current SCI industry standards; and (vi) other matters.

The Commission is sensitive to the economic effects of the proposed expansion and strengthening of Regulation SCI, including its costs and benefits. As discussed further below, the Commission requests comment on all aspects of the costs and benefits of the proposal, including any effects the proposed rules may have on efficiency, competition, and capital formation.

### B. Baseline

The Commission proposes to expand the scope of Regulation SCI to include new entities as well as strengthen the obligations of SCI entities. In order to assess the benefits and costs that can properly be attributed to the proposed rules, the Commission begins by considering the relevant baselines—the current market practices as well as applicable regulations in the absence of these proposed rules.

#### 1. New SCI Entities

The proposed rules will affect new SCI entities, specifically SBSDRs, certain broker-dealers, and certain exempt clearing agencies, in addition to existing SCI entities. The baseline for each category of entities is discussed in turn, including applicable regulatory baselines and relevant market descriptions.

##### a. Registered Security-Based Swap Data Repositories

###### i. Affected Parties

The Commission proposes to include SBSDRs as SCI entities. SBSDRs are required for the dissemination of SBS market data to provide price transparency, limit risk posed to the maintenance of fair and orderly markets, promote the market stability,

prevent market abuses, and reduce operational risk. They play an important role in transparency in the market for SBSs and make available to the Commission SBS data that will provide a broad view of this market and help monitor for pockets of risk and potential market abuses that might not otherwise be observed by the Commission and other relevant authorities.

Security-based swaps entail the transfer of financial obligations between two parties with sometimes a long time horizon. Counterparties to a security-based swap rely on each other's creditworthiness and bear this credit risk and market risk until the security-based swap terminates or expires.[559] The information provided by SBSDRs, such as individual counterparty trade and position data, helps the Commission gain a better understanding of the actual and potential market risks.[560] This information also helps the Commission and other relevant authorities investigate market manipulation, fraud, and other market abuses.

As of February 2023, two data repositories for security-based swap markets are registered with the Commission. The registered SBSDRs are Depository Trust & Clearing Corporation Data Repository ("DDR") and the ICE Trade Vault ("ITV"). DDR operates as a registered SBSDR for security-based swap transactions in the credit, equity, and interest rate derivatives asset classes. ITV operates as a registered SBSDR for security-based swap transactions in the credit derivatives asset class.[561] As of March

---

559 For cleared trades, the clearing agencies generally step in the place of the original counterparties and effectively assume the risk should there be a default.

560 *See* SBSR Adopting Release, *supra* note 96 (for information required to be reported by SBSDRs to the Commission).

561 *See* DTCC Data Repository (U.S.) LLC; Order Approving Application, *supra* note 111; ICE Trade Vault, LLC; Order Approving Application, *supra* note 111. Note that additional entities may register as SBSDRs in the future.

2022, 47 entities had registered with the Commission as security-based swap dealers and pursuant to Regulation SBSR, they are required to report the trade activities to the SBSDRs.[562] In total, these two SBSDRs received approximately 542.6 million reports[563] between November 2021 and September 2022, from contracts of 15,593 distinct counterparties.[564]

### ii. Regulatory Baseline

As discussed above in section III.A.2, SBSDRs are subject to Rule 13n-6, which requires that "every security-based swap data repository, with respect to those systems that support or are integrally related to the performance of its activities, shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its systems provide adequate levels of capacity, integrity, resiliency, availability, and security."[565] The SBSDRs registered with the Commission are also registered with the CFTC as swap data repositories and accordingly are also subject to CFTC rules and regulations related to swap data repositories, including the "SDR System Safeguards" rule.[566] That rule requires swap data repositories to establish and maintain emergency procedures, geographically diverse backup facilities and staff, and a business continuity

---

562 *See List of Registered Security-Based Swap Dealers and Major Security-Based Swap Participants*, *supra* note 110 (providing the list of registered security-based swap dealers and major SBS participants that was updated as of Mar. 28, 2022).

563 The transaction reports include not only the initial trade, but also life-cycle events.

564 Number of reports and number of counterparties are calculated from trade activities data of the DDR and ITV reports. Number of counterparties is calculated as the number of unique counterparties' IDs. Due to data limitation, we only included reports occurred on or after Nov. 8, 2021.

565 *See* 17 CFR 240.13n-6.

566 *See* 17 CFR 49.24.

and disaster recovery plan that should enable next day resumption of the swap data repository's operations following the disruption.[567]

In addition, the rule requires programs of risk analysis and oversight with respect to its operations and automated systems to address each of the following categories of risk analysis and oversight: (1) information security; (2) business continuity and disaster recovery planning and resources; (3) capacity and performance planning; (4) systems operations; (5) systems development and quality assurance; (6) physical security and environmental controls; and (7) enterprise risk management.[568] This rule also requires systems monitoring to identify potential systems disruptions and cybersecurity attacks via provisions relating to capacity and performance planning, information security, and physical security and environmental controls. It also requires swap data repositories to maintain a security incident response plan that must include, among other items, policies and procedures for reporting security incidents and for internal and external communication and information sharing regarding security incidents, the hand-off and escalation points in its security incident response process, and the roles and responsibilities of its management, staff and independent contractors in responding to security incidents.[569]

Furthermore, the rule requires regular, periodic testing and review of business continuity and disaster recovery capabilities.[570] Under the rule, both the senior management and the board of directors of a swap data repository receive and review

---

567 *See* 17 CFR 49.24(a).

568 *See* 17 CFR 49.24(b).

569 *See* 17 CFR 49.24.

570 *Id*.

reports setting forth the results of the specified testing and assessment. A swap data repository is required to establish and follow appropriate procedures for the remediation of issues identified through the review, and for evaluation of the effectiveness of testing and assessment protocols.[571]

The System Safeguards rule requires SDRs to conduct testing and review sufficiency to ensure that their automated systems are reliable, secure, and have adequate scalable capacity.[572] The System Safeguards rule requires SDRs to conduct external and internal penetration testing at a frequency determined by an appropriate risk analysis, but no less frequently than annually.[573]

The System Safeguards rule also specifies and defines five types of system safeguards testing that a SDR necessarily must perform to fulfill the testing requirement: vulnerability testing; penetration testing; controls testing; security incident response plan testing; and enterprise technology risk assessment.[574] SDRs are required to notify CFTC staff of any system malfunctions, cyber security incidents, or activation of the business continuity and disaster recovery plan.[575] A swap data repository must also give CFTC staff advance notice of planned changes to automated systems that may affect the reliability, security, or adequate scalable capacity of such systems.[576] Finally, the CFTC's System Safeguards rule requires an SDR to follow generally accepted standards and best

---

571 17 CFR 49.24(m) (Internal reporting and review).

572 *See* 17 CFR 49.24(j).

573 *See* 17 CFR 49.24(j)(3).

574 *Id*.

575 *See* 17 CFR 49.24(g).

576 *See* 17 CFR 49.24(h).

practices with respect to the development, operation, reliability, security, and capacity of automated systems related to SDR data.[577]

### b. Broker-Dealers

#### i. Affected Parties

The Commission is proposing to expand the application of Regulation SCI to include certain broker-dealers in the definition of SCI entity. There are approximately 3,500 broker-dealers registered with the Commission pursuant to section 15(b) of the Exchange Act as of Q3 2022.[578] Figure 1 represents the distribution of all registered broker-dealer firms between Q4 2021 and Q3 2022 by level of total assets[579] (Panel A) and by percentage of aggregate total assets[580] (Panel B) with firm size (Panel A) and percentage of aggregate total assets (Panel B) increasing along the x-axis from left to right. These entities encompass a broad range of sizes, business activities, and business models.[581] The distribution of firms[582] by level of total assets (Panel A) shows that the vast majority of firms[583] fall somewhere within the $30,000 to $450,000,000 dollar range, with a small minority of firms showing up as a descending long right tail. The

---

577 *See* 17 CFR 49.24(c).

578 *See supra* note 131.

579 The level of total assets is measured by the average quarterly total assets for each broker-dealer between Q4 2021 and Q3 2022.

580 The percentage of aggregate total assets is estimated by the average quarterly percentage of aggregate total assets for each broker-dealer between Q4 2021 and Q3 2022.

581 *See 2022 FINRA Industry Snapshot*, *supra* note 131.

582 Panel A of Figures 1 through 5 is represented on a logarithmic scale for ease of viewing when the distribution is far less evenly distributed if displayed using a standard x-axis.

583 This represents the range of the average quarterly total assets for firms that fall between the 5th and 95th percentile.

distribution of broker-dealers[584] by percentage of aggregate total assets (Panel B) shows that a small number of firms individually had percentages of aggregate total assets in the high single digits to low double digits.

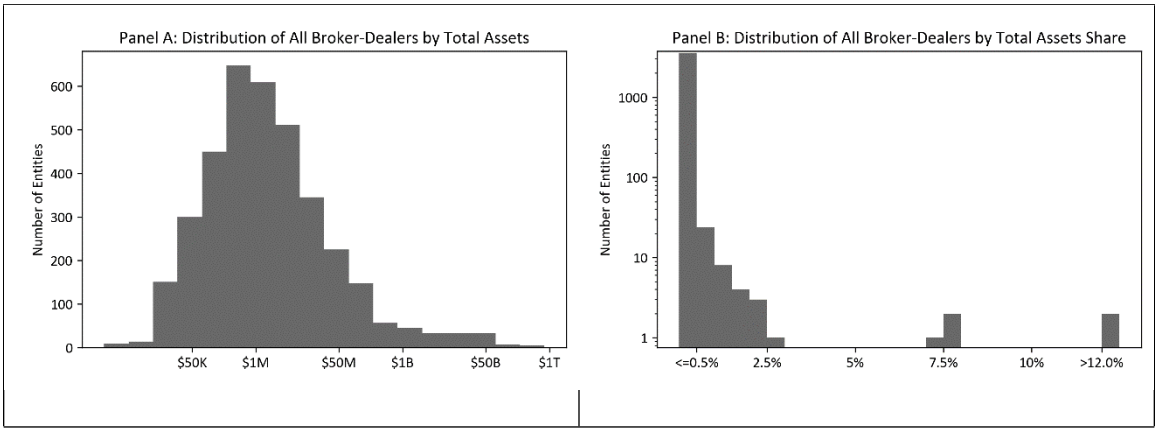



FIGURE 1. DISTRIBUTION OF BROKER-DEALERS BY TOTAL ASSETS (PANEL A) AND TOTAL ASSETS SHARE (PANEL B)

*Notes:* Panel (A): distribution of broker-dealers by average quarterly total assets. Panel (B): distribution of broker-dealers by average quarterly percentage of aggregate total assets. Data are from broker-dealer FOCUS Report Form X-17A-5 Schedule II filings from Q4 2021 to Q3 2022. Also for additional detail on the calculation of total assets of all security broker-dealers, *see supra* note 127.

Figures 2 through 5 represent the distribution of firms by level of transaction activity[585] as measured by average daily dollar volume[586] (Panel A) and the distribution of firms by percentage of transaction activity[587] (Panel B) for each of four asset classes

584 The number of individual firms in Panel B of Figures 1 through 5 is more visible here due to use of a standard x-axis even though the y-axis is represented logarithmically. The use of a logarithmic y-axis does however flatten the overall distribution with a disproportionate effect on the firms with percentage of aggregate average daily dollar volume between 0% and 2.5% making it slightly less obvious upon first glance that the vast majority of firms actually fall between 0% and 2.5%.

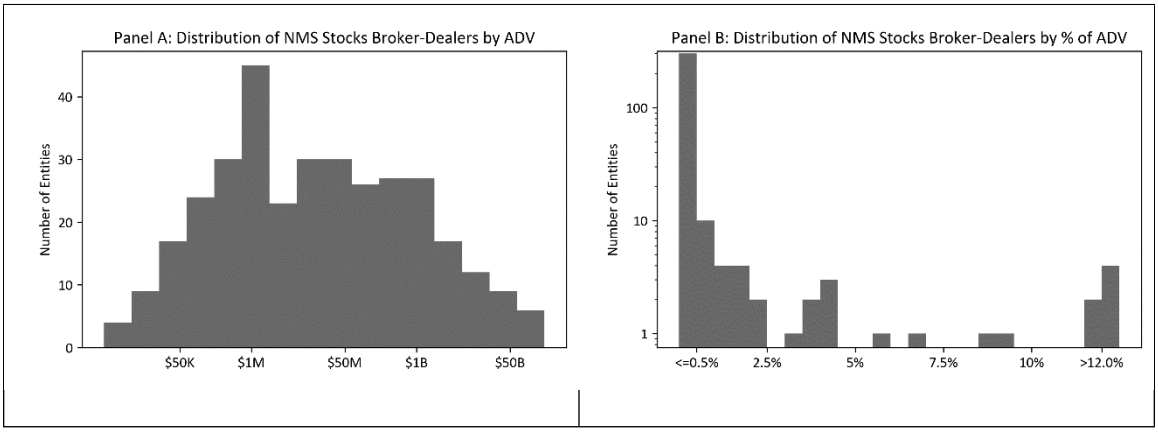
585 The level of transaction activity in Panel A of Figures 2 through 5 is measured by the average of monthly average daily dollar volume for each broker-dealer from Jan. 2022 to June 2022.

586 These measures are described in more detail in section III.A.2.b.iii.

587 *Id.*

including NMS stocks, exchange-listed options, U.S. Treasury Securities, and Agency Securities respectively. The distributions of firms[588] by level of transaction activity (Panel A) show that the vast majority of firms[589] fall somewhere within the $30,000 to $14.4 billion dollar range, $500,000 to $3.1 billion dollar range, $2,000 to $4.0 billion dollar range, and $500 to $1.2 billion dollar range for the NMS, stock exchange-listed options, U.S. Treasury Securities, and Agency Securities markets, respectively.

Figures 2 through 5 (Panel B), showing the distribution of broker-dealers by percentage of aggregate average daily dollar volume,[590] indicate that a very small number of firms[591] individually had percentages of aggregate average daily dollar volume in the high single digits to low double digits.




588 *See supra* note 582.

589 This represents the range of the average of monthly average daily dollar volume for firms that fall between the 5th and 95th percentile.

590 The percentage of aggregate average daily dollar volume in Panel B of figures 2 through 5 is estimated by the average of monthly percentage for each broker-dealer of aggregate average daily dollar volume reported to the plan processors (SIPs) of the CTA/CQ Plans and Nasdaq UTP Plan, OPRA Plan, or FINRA TRACE in each respective asset class from Jan. 2022 to June 2022.

591 *See supra* note 584.

FIGURE 2. DISTRIBUTION OF BROKER-DEALERS, NMS STOCKS ASSET CLASS

*Notes:* Panel (A): distribution of broker-dealers by average of monthly average daily dollar volume. Panel (B): distribution of broker-dealers by average of monthly percentage of aggregate average daily dollar volume. Data are from Consolidated Audit Trail (CAT) data from Jan. 2022 to June 2022 and the plan processors (SIPs) of the CTA/CQ Plans and Nasdaq UTP Plan. CTA Plan, available at https://www.ctaplan.com; Nasdaq UTP Plan, available at https://www.utpplan.com.

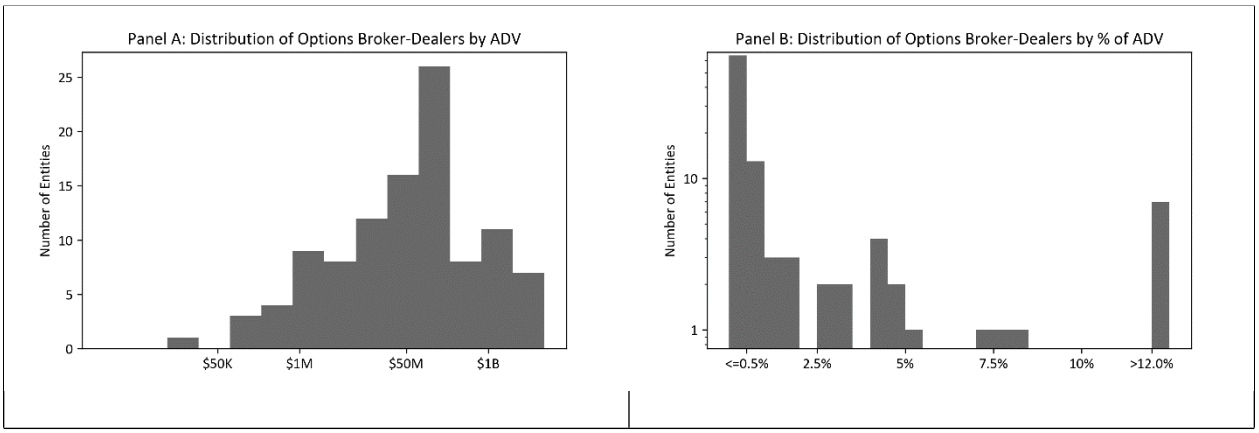



FIGURE 3. DISTRIBUTION OF BROKER-DEALERS, EXCHANGE-LISTED OPTIONS ASSET CLASS

*Notes:* Panel (A): distribution of broker-dealers by average of monthly average daily dollar volume. Panel (B): distribution of broker-dealers by average of monthly percentage of aggregate average daily dollar volume. Data are from Consolidated Audit Trail (CAT) data from Jan. 2022 to June 2022 and Options Price Reporting Authority (OPRA) data.

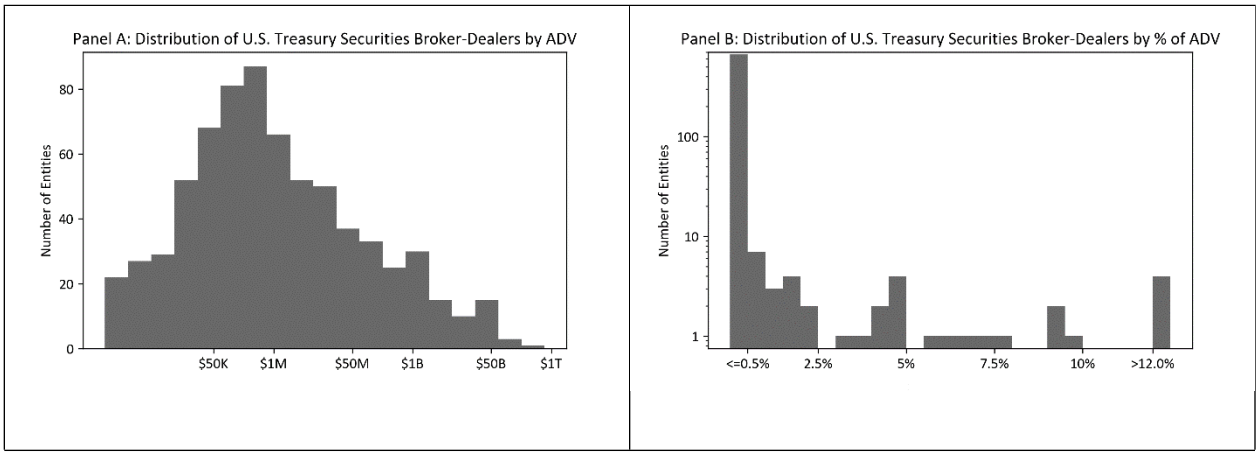



FIGURE 4. DISTRIBUTION OF BROKER-DEALERS, U.S. TREASURY SECURITIES ASSET CLASS

*Notes*: Panel (A): distribution of broker-dealers by average of monthly average daily dollar volume. Panel (B): distribution of broker-dealers by average of monthly percentage of aggregate average daily dollar volume. Data are from TRACE for Treasury Securities data from Jan. 2022 to June 2022 and FINRA TRACE.

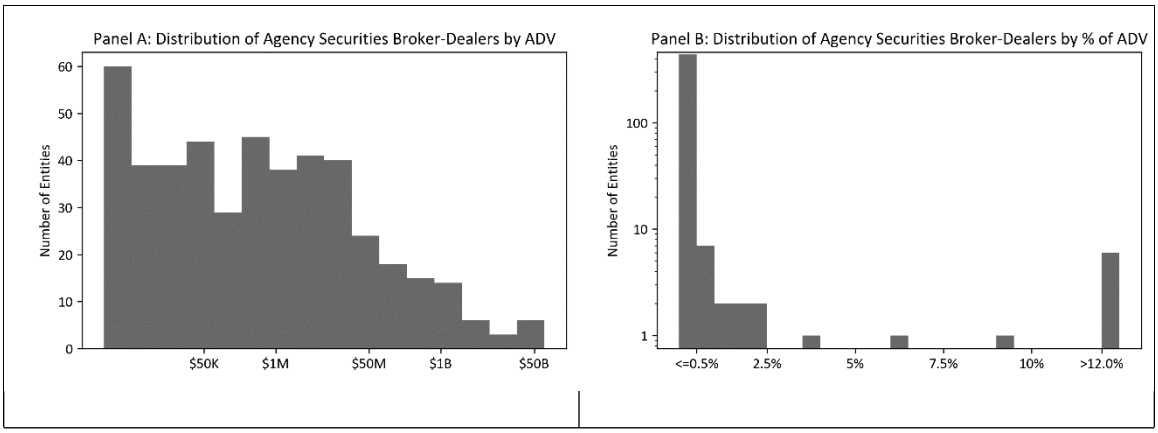



FIGURE 5. DISTRIBUTION OF BROKER-DEALERS, AGENCY SECURITIES ASSET CLASS

*Notes*: Panel (A): distribution of broker-dealers by average of monthly average daily dollar volume. Panel (B): distribution of broker-dealers by average of monthly percentage of aggregate average daily dollar volume. Data are from regulatory TRACE data from Jan. 2022 to June 2022 and FINRA TRACE.

A substantial number of firms had transaction activity[592] across these four markets: 336 had transaction activity in NMS equities,[593] 105 had options transaction activity,[594] 703 had transaction activity in U.S. Treasury Securities,[595] and 461 had transaction activity in Agency Securities.[596]

### ii. Regulatory Baseline

As discussed above in section III.A.2.b.ii, there are already a number of Exchange Act and FINRA rules that affect how broker-dealers design and maintain their technology

592 The number of firms that had transaction activity here may be different than the number of firms that reported business lines on Form BD at least in part due to differences in how business activities are categorized on Form BD, and also because firms are able to indicate lines of business based on expected business rather than current business. With respect to categorical differences, Form BD does not allow firms to distinguish between NMS and OTC equity business as both types of stocks can be traded over the counter. Additionally, Form BD does not distinguish between lines of business for exchange-traded or OTC options. Finally, Form BD allows firms to indicate government securities broker or dealer lines of business but does not allow firms to specify more granularly treasury or agency securities businesses.

593 Estimate is based on Consolidated Audit Trail (CAT) data from Jan. 2022 to June 2022.

594 *Id.*

595 Estimate is based on TRACE for Treasury Securities data from Jan. 2022 to June 2022 and firm names as of Feb. 1, 2023.

596 Estimate is based on regulatory TRACE data from Jan. 2022 to June 2022.

and promote business continuity and regulatory compliance. These include: Commission broker-dealer rules;[597] FINRA supervision rules[598] (discussed at length in section III.A.2.b); and FINRA's business continuity and reporting rules (Rule 4370 and 4530, respectively) discussed previously in section III.A2.b and further in this section. Furthermore, the Commission's cybersecurity-related regulations (Regulation S-P and 17 CFR part 248, subpart C (Regulation S-ID)) are discussed further below.[599]

FINRA Rule 4370 primarily requires that each broker-dealer create and maintain a written business continuity plan[600] identifying procedures relating to an emergency or significant business disruption that are reasonably designed to enable them to meet their existing obligations to customers with explicit requirements for data back-up and recovery with respect to mission critical systems as well as an alternate physical location of employees.[601] Each broker-dealer must update its plan in the event of any material change to the member's operations, structure, business or location. Each member must also conduct an annual review of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location. FINRA identified that firms[602] frequently tested their BC/DRs plans

---

597 *See supra* section III.A.2.b (discussing Rules 17a-3, 17a-4, 17a-11, 15c3-1, 15c3-3, and 15c3-5 (the Market Access Rule)).

598 FINRA rule 3110 and 3130.

599 *See supra* note 156.

600 *See* FINRA, *2019 Report on Examination Findings and Observations: Business Continuity Plans (BCPs)* (Oct. 16, 2019), *available at* https://www.finra.org/rules-guidance/guidance/reports/2019-report-exam-findings-and-observations. Broker-dealers are required to conduct an annual review of their business continuity plans along with recommended testing and evaluation of its effectiveness with vendor participation.

601 FINRA Rules 4370, 3110 (Supervision), and 4511 (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.

602 FINRA did not disclose the number or identity of these firms.

as part of their annual review and also included key vendors in those tests.[603] Furthermore, a broker-dealer must disclose to its customers through public disclosure statements how its business continuity plan addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope. Such required business continuity public disclosure statements[604] offer some summary information on broker-dealer actual practices that relate to FINRA Rule 4370. Recent FINRA exam findings reports[605] in relation to FINRA Rule 4370 suggest increasing attention by broker-dealers to operational resiliency issues and the value of capacity planning, stress testing, and the review of testing and development methodology.

FINRA rules relating to supervision[606] require each member to establish, maintain, and enforce written procedures to supervise the types of business in which it engages and the activities of its associated persons that are reasonably designed to achieve compliance with applicable securities laws and regulations including Federal

---

603 *See* FINRA, 2019 Report on Examination Findings and Observations: Business Continuity Plans (BCPs), *supra* note 600.

604 While broker-dealers are required to provide a brief summary disclosure statement regarding their BCPs to customers, they do not disclose the actual BCP. Based on a review of 2021 and 2022 BCP disclosure statements, firms often did not provide any detail on operational capacity to meet demand surges or any specific timeframes for resumption of service. They sometimes mention the use of redundant service centers, data centers, systems, and staff across geographically diverse locations in case primary centers and systems go offline; immediate failover to backup systems and plans to restore services quickly in the event of a technology disruption; and review of third parties' business contingency plans.

605 *See* FINRA, *2022 Report on FINRA's Examination and Risk Monitoring Program* (Feb. 9, 2022), *available at* https://www.finra.org/sites/default/files/2022-02/2022-report-finras-examination-risk-monitoring-program.pdf. *See also* FINRA, *2020 Risk Monitoring and Examination Priorities Letter* (Jan. 9, 2020), *available at* https://www.finra.org/rules-guidance/communications-firms/2020-risk-monitoring-and-examination-priorities-letter; FINRA, *Equity Trading Initiatives: Supervision and Control Practices for Algorithmic Trading Strategies* (Mar. 2015), *available at* https://www.finra.org/sites/default/files/notice_doc_file_ref/Notice_Regulatory_15-09.pdf.

606 FINRA Rules 3110 (Supervision) and 3120 (Supervisory Control Systems).

cybersecurity laws and regulations applicable to broker-dealers such as Regulation S-P[607] and Regulation S-ID.[608] As discussed in section III.D.1.c.i, Regulation S-P's safeguards provisions require broker-dealers to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[609] The Regulation S-P Safeguards Rule further provides that these policies and procedures must: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[610] Additionally, the Regulation S-P Disposal Rule requires broker-dealers that maintain or otherwise possess consumer report information for a business purpose to properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.[611] In contrast, Regulation S-ID is more narrowly concerned with identity theft. Broker-dealers subject to Regulation S-ID must develop and implement a written identity theft program that includes policies and procedures to identify and detect relevant red flags.[612]

---

607 *See* 17 CFR 248.1 through 248.30.

608 *See* 17 CFR 248.201 and 248.202.

609 *See* 17 CFR 248.30(a).

610 *See* 17 CFR 248.30(a)(1) through (3).

611 *See* 17 CFR 248.30(b)(2). Regulation S-P currently defines the term "disposal" to mean: (1) the discarding or abandonment of consumer report information; or (2) the sale, donation, or transfer of any medium, including computer equipment, on which consumer report information is stored. *See* 17 CFR 248.30(b)(1)(iii).

612 *See* 17 CFR 248.201.

Past Commission staff statements[613] and FINRA guidance[614] with respect to these rules identify common elements of reasonably designed cybersecurity policies and

---

613 *See* OCIE, SEC, *Cybersecurity: Safeguarding Client Accounts against Credential Compromise* (Sep. 15, 2020), *available at* https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf; OCIE, SEC, *Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers* (Aug. 12, 2020), *available at* https://www.sec.gov/files/Risk%20Alert%20-%20COVID-19%20Compliance.pdf; OCIE, SEC, *Cybersecurity: Ransomware Alert* (July 10, 2020), *available at* https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf; OCIE, SEC, *Report on OCIE Cybersecurity and Resiliency Observations* (Jan. 27, 2020), *available at* https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf; OCIE, SEC, *OCIE Safeguarding Customer Records and Information in Network Storage—Use of Third Party Security Features* (May 23, 2019), *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf; OCIE, SEC, *Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P—Privacy Notices and Safeguard Policies* (Apr. 16, 2019), *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf; OCIE, SEC, *Observations from Cybersecurity Examinations* (Aug. 7, 2017), *available at* https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf; OCIE, SEC, *Cybersecurity: Ransomware Alert* (May 17, 2017), *available at* https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf; OCIE, SEC, *OCIE's 2015 Cybersecurity Examination Initiative* (Sep. 15, 2015), *available at* https://www.sec.gov/files/ocie-2015-cybersecurity-examination-initiative.pdf; OCIE, SEC, *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf; OCIE, SEC, *OCIE's 2014 Cybersecurity Initiative* (Apr. 15, 2014), *available at* https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

614 *See* FINRA, *Core Cybersecurity Threats and Effective Controls for Small Firms* (May 2022), *available at* https://www.finra.org/sites/default/files/2022-05/Core_Cybersecurity_Threats_and_Effective_Controls-Small_Firms.pdf; FINRA, *Cloud Computing in the Securities Industry* (Aug. 16, 2021), *available at* https://www.finra.org/rules-guidance/key-topics/fintech/report/cloud-computing; FINRA, *Common Cybersecurity Threats* (July 9, 2019), *available at* https://www.finra.org/rules-guidance/guidance/common-cybersecurity-threats; FINRA, *Report on Selected Cybersecurity Practices* (Dec. 1, 2018), *available at* https://www.finra.org/rules-guidance/guidance/common-cybersecurity-threats; FINRA, *Report on FINRA Examination Findings* (Dec. 6, 2017), *available at* https://www.finra.org/sites/default/files/2017-Report-FINRA-Examination-Findings.pdf; FINRA, *Small Firm Cybersecurity Checklist* (May 23, 2016), *available at* https://www.finra.org/compliance-tools/small-firm-cybersecurity-checklist. Cybersecurity has also been a regular theme of FINRA's Regulatory and Examination Priorities Letter since 2008 often with reference to Regulation S-P. Similarly the SEC sponsored a Cybersecurity Roundtable and the Division of Examination conducted cybersecurity initiative I and II to assess industry practices and legal and compliance issues associated with broker-dealer and investment adviser cybersecurity preparedness.

procedures including risk assessment, user security and access, information protection, incident response,[615] and training.[616]

Consistent with these rules, nearly all broker-dealers that participated in two Commission exam sweeps in 2015 and 2017 reported[617] maintaining some cybersecurity policies and procedures; conducting some periodic risk assessments to identify threats and vulnerabilities,[618] conducting firm-wide systems inventorying or cataloguing, ensuring regular system maintenance including the installation of software patches to address security vulnerabilities, performing some penetration testing,[619] although both sweeps also discussed various flaws in compliance. A separate staff statement, based on observed industry practices, noted that at least some firms implemented capabilities that

---

615 *See FINRA, 2021 Report on FINRA's Examination and Risk Monitoring Program* (Feb. 01, 2021), *available at* https://www.finra.org/rules-guidance/guidance/reports/2021-finras-examination-and-risk-monitoring-program/cybersecurity (FINRA recommended among effective practices with respect to incident response: Establishing and regularly testing (often using tabletop exercises) a written formal incident response plan that outlines procedures for responding to cybersecurity and information security incidents; and developing frameworks to identify, classify, prioritize, track and close cybersecurity-related incidents.).

616 These categories vary somewhat in terms of nomenclature and the specific categories themselves across different Commission and FINRA publications.

617 *See Cybersecurity Examination Sweep Summary*, *supra* note 613 (Of 57 examined broker-dealers, the vast majority adopted written information security policies, conducted periodic audits to determine compliance with these information security policies and procedures, conducted risk assessments and reported considering such risk assessments in establishing their cybersecurity policies and procedures. With respect to vendors, the majority of the broker-dealers required cybersecurity risk assessments of vendors with access to their firms' networks and had at least some specific policies and procedures relating to vendors.). *See also Observations from Cybersecurity Examinations*, *supra* note 613 (This largely aligned with the prior 2015 Exam Sweep but is based on additional data from a mixed group of 75 broker-dealers and investment advisers. For example, nearly all firms had incident response plans. Still, it appeared that a number of firms did not appear to fully remediate some of the high risk observations that they discovered from these tests and vulnerability scans in a timely manner or failed to conduct penetration testing regularly).

618 *See Report on Selected Cybersecurity Practices*, *supra* note 614. According to FINRA's 2018 RCA, 94% of higher revenue firms and 70% of mid-level revenue firms use a risk assessment as part of their cybersecurity program. The Risk Control Assessment (RCA) Survey is a voluntary survey conducted by FINRA on an annual basis with all active member firms.

619 *Id*. According to FINRA's 2018 RCA, 100% of higher revenue firms include penetration testing as a component in their overall cybersecurity program.

are able to control, monitor, and inspect all incoming and outgoing network traffic to prevent unauthorized or harmful traffic and implemented capabilities that are able to detect threats on endpoints.[620] In the two Commission exam sweeps, many firms indicated that policies and procedures were vetted and approved by senior management and that firms provided annual cybersecurity reports to the board while some also provided ad hoc reports in the event of major cybersecurity events.[621] Broadly, many broker-dealers reported relying on industry standards with respect to cybersecurity[622] typically by adhering to a specific industry standard or combination of industry standards or by using industry standards as guidance in designing policies and procedures. In the Commission's 2017 sweep, however, weaknesses in policies and procedures and failure to implement policies and procedures were observed at a majority of the participating firms.[623]

FINRA Rule 3110's supervisory obligation also extends to member firms' outsourcing of certain "covered activities"— activities or functions that, if performed directly by a member firm, would be required to be the subject of a supervisory system and written supervisory procedures pursuant to FINRA Rule 3110. These vendor

---

620 *See Cybersecurity and Resiliency Observations, supra* note 614.

621 *See Cybersecurity Examination Sweep Summary*, *supra* note 613, and *Observations from Cybersecurity Examinations*, *supra* note 613.

622 *Id.* Among the firms that were part of the sweep, nearly 90% used one or more of the NIST, ISO or ISACA frameworks or standards. More specifically, 65% of the respondents reported that they use the ISO 27001/27002 standard while 25% use COBIT. Some firms use combinations of these standards for various parts of their cybersecurity programs. While the report focused on firm utilization of cybersecurity frameworks specifically, in many cases, the referenced frameworks were broader IT frameworks.

623 *See* OCIE, SEC, *Observations from Cybersecurity Examinations* (Aug. 7, 2017), *available at* https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

management obligations are discussed in further guidance.[624] As discussed in section III.A.2.b of this release, FINRA Rule 4530 requires broker-dealer reporting of certain events to FINRA, including, among other things, compliance issues and other events[625] where a broker-dealer has concluded or should have reasonably concluded that a violation of securities or other enumerated law, rule, or regulation of any domestic or foreign regulatory body or SRO has occurred. Broker-dealers affiliated with a banking organization[626] may also be affected by a cybersecurity notification requirement. For example, if a broker-dealer is a subsidiary of a bank holding company, an incident at the broker-dealer would likely be reported by the bank holding company to its respective banking regulator.

Aside from specific dissemination obligations under Regulation SCI for a limited number of broker-dealers with respect to their related SCI ATSs, there are no Commission or FINRA requirements for broker-dealers to disseminate notifications of breaches to members or clients although many firms do so[627] pursuant to various state

---

624 *See Regulatory Notice 21-29: Vendor Management and Outsourcing*, *supra* note 165; *Notice to Members 05-48: Outsourcing*, *supra* note 165. FINRA found that most firms had adequate privacy and security language in contracts where customer or firm confidential data or high-risk systems were at risk. Standard contract language topics that firms included were: non-disclosure agreements/confidentiality agreements, data storage, retention, and delivery; breach notification responsibilities; right-to-audit clauses; vendor employee access limitations; use of subcontractors; and vendor obligations upon contract termination. *Id.*

625 While FINRA has urged firms to report material cyber incidents that do not trigger a reporting obligation to their regulatory coordinator, current practices are unclear.

626 In the simplification of the Volcker Rule, effective Jan. 21, 2020, Commission staff estimated that there were 202 broker-dealers that were affiliated with banking organizations.

627 *See Cybersecurity Examination Sweep Summary*, *supra* note 613 (Based on a small sample of firms, the vast majority of broker-dealers maintained plans for data breach incidents and most had plans for notifying customers of material events.)

data breach laws.[628] Broker-dealers are subject to state laws known as "Blue Sky Laws," which generally are regulations established as safeguards for investors against securities fraud.[629] All 50 states have enacted laws in recent years requiring firms to notify individuals of data breaches, standards differ by state, with some states imposing heightened notification requirements relative to other states.[630]

Additionally, market data, including bids, offers, quotation sizes, among other types of data, are currently collected from broker-dealers and consolidated and distributed pursuant to a variety of Exchange Act rules and joint industry plans.[631]

#### c. Exempt Clearing Agencies

##### i. Affected Parties

Certain SCI entities are in the market for clearance and settlement services. Registered clearing agencies and certain exempt clearing agencies are already SCI entities. The Commission proposes to extend Regulation SCI to include all other exempt

---

628 *See* Digital Guardian, *The Definitive Guide to U.S. State Data Breach Laws*, digitalguardian.com, *available at* https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf (last visited Nov. 15, 2022).

629 *See, e.g.*, Office of Investor Education and Advocacy, Commission, *Blue Sky Laws*, *available at* https://www.investor.gov/introduction-investing/investing-basics/glossary/blue-sky-laws.

630 For example, some states may require a firm to notify individuals when a data breach includes biometric information, while others do not. *Compare* Cal. Civil Code sec. 1798.29 (notice to California residents of a data breach generally required when a resident's personal information was or is reasonably believed to have been acquired by an unauthorized person; "personal information" is defined to mean an individual's first or last name in combination with one of a list of specified elements, which includes certain unique biometric data), *with* Ala. Stat. secs. 8-38-2, 8-38-4, 8-38-5 (notice of a data breach to Alabama residents is generally required when sensitive personally identifying information has been acquired by an unauthorized person and is reasonably likely to cause substantial harm to the resident to whom the information relates; "sensitive personally identifying information" is defined as the resident's first or last name in combination with one of a list of specified elements, which does not include biometric information).

631 *See, e.g.,* Rules 601 through 17 CFR 242.604 ("Rule 604") of Regulation NMS and 17 CFR 242.301(b)(3) ("Rule 301(b)(3)") of Regulation ATS.

clearing agencies. The proposed amendment would have the immediate effect of introducing two exempt clearing agencies into the scope of Regulation SCI.

There are broadly two types of clearing agencies: registered clearing agencies and exempt clearing agencies. There are seven registered and active clearing agencies: DTC, FICC, NSCC, ICC, ICEEU, the Options Clearing Corp., and LCH SA. There are two other clearing agencies that are no longer active but both maintain registration with the Commission.[632] In addition to these registered clearing agencies, there are clearing agencies that have received from the Commission an exemption from registration as a clearing agency under section 17A of the Exchange Act. There are five exempt clearing agencies: Bloomberg STP (inactive), ITPMATCH (DTCC), SSCNET (SS&C Technologies), Euroclear Bank SA/NV, and Clearstream Banking, S.A. Of these exempt clearing agencies, Bloomberg STP, ITPMATCH (DTCC), and SSCNET (SS&C Technologies) are subject to Regulation SCI as "exempt clearing agencies subject to ARP," together with registered clearing agencies.

The other two, Euroclear Bank SA/NV, and Clearstream Banking, S.A, both exempt clearing agencies,[633] have not been required to comply with Regulation SCI. Each

---

632 *See* BSECC Notice and SCCP Notice, *supra* note 230.

633 *See* Euroclear Exemption, *supra* note 231 (providing an exemption to Euroclear Bank SA/NV (successor in name to Morgan Guaranty Trust Company of NY)); Clearstream Exemption, *supra* note 231 (providing an exemption to Clearstream Banking, S.A. (successor in name to Cedel Bank, société anonyme, Luxembourg)). Furthermore, pursuant to the Commission's statement on CCPs in the European Union ("EU") authorized under the European Markets Infrastructure Regulation ("EMIR"), an EU CCP may request an exemption from the Commission where it has determined that the application of SEC requirements would impose unnecessary, duplicative, or inconsistent requirements in light of EMIR requirements to which it is subject. *See Statement on Central Counterparties Authorized under the European Markets Infrastructure Regulation Seeking to Register as a Clearing Agency or to Request Exemptions from Certain Requirements Under the Securities Exchange Act of 1934 supra* note 240 (stating that in seeking an exemption, an EU CCP could provide "a self-assessment. . . [to] explain how the EU CCP's compliance with EMIR corresponds to the requirements in the Exchange Act and applicable SEC rules thereunder, such as Rule 17Ad-22 and Regulation SCI.").

performs CSD functions and provides clearance and settlement for U.S. Treasury transactions, subject to volume limits set forth in their exemptions. Euroclear Bank also provides collateral management services for U.S. equity transactions involving a U.S. person and a non-U.S. person.

### ii. Regulatory Baseline

The two exempt clearing agencies not subject to ARP are required per Commission exemptive orders to submit to the Commission a number of items including transaction volume data,[634] notification regarding material adverse changes in any account maintained for customers,[635] one or more disclosure documents, amendments to its application for exemption on Form CA–1,[636] responses to a Commission request for information,[637] etc. In the case of one exempt clearing agency, its exemptive order also requires submission of additional items related to its systems including quarterly reports

---

634 *Id.* This is provided in the form of quarterly reports, calculated on a twelve-month rolling basis, of volume statistics related to government securities. One exempt clearing agency also reports volume statistics related to equities.

635 *Id.* This is for customers that are members or affiliates of members of a U.S. registered clearing agency in the case of one exempt clearing or US participants in the case of the other.

636 *Id.* This must be filed prior to the implementation of any change in stated policies, practices, or procedures that makes the information contained in the original Form CA-1 incomplete or inaccurate in any material respect.

637 *Id.* This would typically concern a U.S. customer or its affiliate about whom the Commission has financial solvency concerns.

describing completed, ongoing, and planned material system changes,[638] notification[639] regarding systems events;[640] as well as a requirement to take appropriate corrective action regarding such systems events. This exempt clearing agency is also required to maintain policies and procedures that are reasonably designed to identify, manage, and monitor systems operational risk; clearly define the roles and responsibilities of personnel for addressing operational risk; review such policies and procedures; conduct systems audits and system tests periodically and at implementation of significant changes; clearly define operational reliability objectives for the systems; ensure that the systems have scalable capacity adequate to handle increasing stress volumes and achieve the systems service-level objectives; establish comprehensive physical and information security policies that address all potential vulnerabilities and threats to the systems; and establish a business continuity plan[641] for the systems that addresses events posing a significant risk of disrupting the systems' operations, including events that could cause a wide-scale or

---

638 This must be filed within 30 calendar days after the end of each quarter. These reported information represents changes related to the Clearing Agency Activities during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion.

639 This requires notification of such systems event within 24 hours after occurrence; regular updates until such time as a systems event is resolved and investigation of the systems event is closed; interim written notification within 48 hours after the occurrence of a systems event or promptly thereafter if such a deadline cannot be met; a written final report within ten business days after the occurrence of a systems event or promptly thereafter if such a deadline cannot be met. For systems events characterized as ''bronze level'' events (i.e., a Systems Event in which the incident is clearly understood, almost immediately under control, involves only one business unit and/or entity, and is resolved within a few hours), the clearing agency is instead required to provide on a quarterly basis an aggregated list of bronze level events.

640 This includes disruptions, compliance issues, or intrusions of the systems that impact, or is reasonably likely to impact clearing agency activities.

641 The business continuity plan would require the use of a secondary site designed to ensure two-hour resumption of operation following disruptive events; regular testing of business continuity plans; identification, monitoring, and management of the risks that key participants, other financial market infrastructures, and service and utility providers might pose to the systems' operations in relation to the clearing agency activities.

major disruption in the provision of the clearing agency activities. Such policies and procedures should be consistent with current information technology industry standards[642] and be reasonably designed to ensure that the systems operate on an ongoing basis in a manner that complies with the conditions applicable to the systems and with the exempt clearing agency's rules and governing documents applicable to the clearing agency activities. This exempt clearing agency must also provide the Commission with an annual update regarding policies and procedures.

Additionally, the two exempt clearing agencies not subject to ARP are subject to Europe's Central Securities Depositories Regulation (CSDR) which provides a set of common requirements for CSDs operating securities settlement systems across the EU.[643] CSDR provides, among other things, Operational Risk rules (Article 45).[644] There are more specific requirements in the CSDR's Regulatory Technical Standards[645] including

---

642 The exempt clearing agency is required to provide annual notice to the Commission regarding the industry standards utilized. These standards consist of information technology practices that are widely available to information technology professionals in the financial sector and issued by a widely recognized organization.

643 The two exempt clearing agencies may also be subject to the EU Regulation, the Digital Operational Resilience Act (DORA), which went into effect in 2015: *See* Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595.

644 *See* Commission Regulation No. 909/2014 of July 23, 2014, on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, art. 45, 2014 O.J. (L 257) 47, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0909.

645 *See* Commission Delegated Regulation 2017/392, Supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with Regard to Regulatory Technical Standards on Authorization, Supervisory and Operational Requirements for Central Securities Depositories. 65 Off. J. Eur. Union 48 (2017) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0392&from=EN.

identifying operational risks;[646] methods to test, address and minimize operational risks;[647] IT systems;[648] and business continuity.[649]

Furthermore, each of these two exempt clearing agencies publish disclosure framework reports[650] that purport to describe the policies and procedures[651] with respect to the operational risk framework of the Principles for Financial Market Infrastructures (PFMI) published by CPSS and IOSCO.[652]

### 2. Existing SCI Entities:

#### a. Affected Parties

In addition to these proposed new SCI entities, Regulation SCI has applied to entities that facilitate several different markets, including the market for trading services, the market for listing services, the market for regulation and surveillance services, the market for clearance and settlement services, and the market for market data.[653] As of this writing, there are 47 SCI entities. These include 35 SCI SROs (including 24 exchanges, 9 registered clearing agencies, FINRA, and the MSRB), 7 SCI ATSs (including 5 NMS stock ATSs and 2 non-NMS stock ATSs), 2 plan processors, and 3 exempt clearing

---

646 *Id.* art. 45:1.

647 *Id.* art. 45:2.

648 *Id.* art. 45:3.

649 *Id.* art. 45:4.

650 *See infra* notes 683-684.

651 The respective disclosure documents have not been reviewed by the Commission and its staff for accuracy and may or may not demonstrate implementation/compliance with international standards.

652 Bank for International Settlements (BIS), *Principles for Financial Market Infrastructures: Disclosure Framework and Assessment Methodology* (Dec. 2012), *available at* https://www.bis.org/cpmi/publ/d106.pdf.

653 17 CFR 242.1000 (definitions of "SCI systems" and "critical SCI systems").

agencies subject to ARP.[654] All of them are already required to comply with Regulation SCI, and, as discussed in section V.B.2.b, subsets of these entities also have other specific rules that apply to them.

The general characteristics of the markets in which the existing SCI entities operate are described in the SCI Proposing Release[655] and SCI Adopting Release.[656] There are, however, broad changes to these markets—as they pertain to Regulation SCI—that should be noted. The markets have changed in at least four important ways. First, the total trading volumes have increased across all types of securities.[657] Second, there is an increased reliance on technology and automation among financial institutions, a trend which accelerated due to the COVID-19 pandemic.[658] Third, and relatedly, financial institutions have become increasingly dependent on third parties—including

---

654 In 2021, the Commission amended Regulation SCI to add competing consolidators that exceed a 5% consolidated market data gross revenue threshold over a specified time period as SCI entities. Currently, no competing consolidators have registered with the Commission. *See* Market Data Infrastructure Adopting Release, *supra* note 24.

655 *See* SCI Proposing Release, *supra* note 14, at section V. *See also* Market Data Infrastructure Adopting Release, *supra* note 24, for a description of competing consolidator market characteristics.

656 *See* SCI Adopting Release, *supra* note 1, at section VI.

657 *See, e.g.*, *SIFMA Insights: Electronic Trading Market Structure Primer*, *supra* note 3 (summarizing electronic trading history and trends in different markets); SEC, *Staff Report on Equity and Options Market Structure Conditions in Early 2021* (Oct. 14, 2021), *available at* https://www.sec.gov/files/staff-report-equity-options-market-struction-conditions-early-2021.pdf; *see also* U.S. House Committee on Financial Services, *Game Stopped: How the Meme Stock Market Event Exposed Troubling Business Practices, Inadequate Risk Practices, and the Need for Legislative and Regulatory Reform* (June 2022), *available at*: https://democrats-financialservices.house.gov/uploadedfiles/6.22_hfsc_gs.report_hmsmeetbp.irm.nlrf.pdf.

658 *See, e.g.*, Henning Soller, et al., *Innovative Technologies in Financial Institutions: Risk as a Strategic Issue*, McKinsey Digital (Sep. 25, 2020), *available at*: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/innovative-technologies-in-financial-institutions-risk-as-a-strategic-issue ("The current COVID-19 crisis has significantly accelerated the need for financial institutions to adopt innovative technologies.").

cloud service providers—to operate their businesses and provide their services.[659] This is, in fact, a general trend among all global companies, and this trend, too, has been driven in part by the COVID-19 pandemic.[660] Fourth, cybersecurity events have grown in both number and sophistication.[661] These developments in the market have significantly increased the negative externalities that may flow from systems failures.

Current SCI entities are required to report systems intrusions, either immediately or on a quarterly basis, rather than immediately if de miminis in impact. However, current SCI entities have not been reporting attempted intrusions, as they were not required to do so.

**b. Regulatory Baseline**

The common regulatory baseline for current SCI entities is Regulation SCI which was adopted in 2014. Regulation SCI requires, among other things, that these entities establish, maintain, and enforce written policies and procedures reasonably designed to ensure that their SCI 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 and the rules and regulations thereunder and the entity's rules and

---

659 *See, e.g.*, Noah Kessler, *Cloud Is on the Rise in Financial Services and Regulators Are Taking Note*, ABA Risk and Compliance (Sept. 29, 2021), *available at* https://bankingjournal.aba.com/2021/09/cloud-is-on-the-rise-in-financial-services-and-regulators-are-taking-note/.

660 *See, e.g.*, Deloitte, *2021 Global Shared Services and Outsourcing Survey Report* 3, *available at* https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Process-and-Operations/gx-2021-global-shared-services-report.pdf ("[T]here's an increasing shift to leverage global, multifunctional, and virtual or remote models, especially driven by learnings from COVID-19").

661 *See, e.g.*, Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know*, Forbes.com (June 3, 2022), *available at* https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=2429c57e7864.

governing documents, as applicable, and specifies certain minimum requirements for such policies and procedures. As a policies and procedures based rule, and one that employs a risk-based approach, Regulation SCI provides flexibility to allow each SCI entity to determine how to best meet the requirements in Rule 1001(a).

In addition, 17 CFR 242.613 ("Rule 613") of Regulation NMS requires national securities exchanges and national securities associations (FINRA) to jointly develop and submit to the Commission a Consolidated Audit Trail National Market System (CAT NMS) Plan.[662]

Under the Commission-approved CAT NMS Plan, the national securities exchanges and FINRA (the Participants) conduct the activities related to the CAT through a jointly owned limited liability company, Consolidated Audit Trail, LLC ("Company").[663] FINRA CAT, LLC—a wholly-owned subsidiary of FINRA—has entered into an agreement with the Company to act as the plan processor for the CAT. However, the Participants remain ultimately responsible for the performance of the CAT and its compliance with any statutes, rules, and regulations.[664] The Plan Processor must develop three sets of policies and procedures: (1) the CAT information security program

---

662 17 CFR 242.613.

663 Consolidated Audit Trail, LLC, *CAT NMS Plan, secs. 1.1, 3.1, 4.1* (July 2020), *available at* https://catnmsplan.com/sites/default/files/2020-07/LLC-Agreement-of-Consolidated-Audit-Trail-LLC-as-of-7.24.20.pdf; *see also* CAT NMS Plan Approval Order, *supra* note 393; Joint Industry Plan; Order Approving Amendment to the National Market System Plan Governing the Consolidated Audit Trail, Securities Exchange Act Release No. 89397 (July 24, 2020), 85 FR 45941 (July 30, 2020).

664 CAT NMS Plan, secs. 4.3, 5.1, 6.1. The Participants jointly own on an equal basis the Company. As such, the CAT's Central Repository is a facility of each of the Participants, and also an SCI system of each of the Participants. *See* SCI Adopting Release, *supra* note 1, at 72275 at n. 246; CAT NMS Plan Approval Order, *supra* note 393, at 84758.

and related data security policies and procedures; (2) user security and access policies and procedures; and (3) breach management policies and procedures.[665]

First, the Plan Processor must develop and maintain a comprehensive information security program, to be approved and reviewed at least annually by an operating committee, which contains certain specific requirements for the Company related to data security.[666] As part of this requirement, the Plan Processor is required to create and enforce policies, procedures, and control structures to monitor and address CAT data security, including reviews of industry standards and periodic penetration testing.[667] Second, both the Participants and the Plan Processor must implement user security and access policies and procedures that include safeguards to secure access and use of the CAT.[668] The Plan Processor must also review Participant information security policies and procedures related to the Company to ensure that such policies and procedures are comparable to those of the CAT system.[669] Finally, the Plan Processor must develop a cyber-incident response plan and document all information relevant to breaches.[670] In

---

665 CAT NMS Plan, secs. 6.12 and app. D. secs. 4.1 to 4.1.5. The Plan Processor is subject to certain industry standards with respect to its information security program, including, among others, NIST-800-23 (Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Test/Evaluated Products), NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), and NIST 800-115 (Technical Guide to Information Security Testing and Assessment). CAT NMS Plan, app D sec 4.2.

666 CAT NMS Plan, app. D sec. 4.1.

667 *Id*. sec. 6.2(b)(v) and app. D secs. 4.1 to 4.2.

668 Specifically, these safeguards must include: (1) restrictions on the acceptable uses of CAT Data; (2) role-based access controls; (3) authentication of individual users; (4) multifactor authentication and password controls; (5) implementation of information barriers to prevent unauthorized staff from accessing CAT Data; (6) separate storage of sensitive personal information and controls on transmission of data; (7) security-driven monitoring and logging; (8) escalation of non-compliance or security events; and (9) remote access controls. *Id*. at secs. 6.2(b)(v), 6.5(c)(i), 6.5(c)(iii) and (iv) and app. D secs. 4.1 to 4.1.4, 4.1.6, 8.1, 8.1.1, 8.1.3, 8.2, 8.2.2.

669 *Id*. sec. 6.2(b)(vii).

670 *Id*. app. D sec. 4.1.5.

addition to these policies and procedures requirements, the CAT NMS Plan requires several forms of periodic review of CAT, including an annual written assessment,[671] regular reports,[672] and an annual audit.[673] The Commission has proposed amendments to the CAT NMS Plan that are designed to enhance the security of the CAT through increased security requirements as well as limiting the scope of sensitive information required to be collected by the CAT.[674]

### 3. Current Market Practice

This section describes current and new SCI entities' market practices, as relevant to certain of the proposed and existing provisions. These market practices include entities' compliance efforts that exceed current regulatory baseline requirements, entities' adherence to voluntary standards and best practices, and business practices not directly related to compliance with a regulatory obligation that nevertheless overlap with the substantive or procedural requirements of the proposed rule. To the extent the entities' existing practices already comply with the requirements or proposed requirements of Regulation SCI, or to the extent those practices might facilitate such compliance, the benefits and costs of the proposal could be mitigated. The Commission requests comment

---

671 The Participants are required to provide the Commission with an annual written assessment of the Plan Processor's performance, which must include, among other things, an evaluation of potential technology upgrades and an evaluation of the CAT information security program. *Id*. secs. 6.2(a)(v)(G), 6.6(b).

672 The Plan Processor is required to provide the operating committee with regular reports on various topics, including data security issues and the Plan Processor. *Id*. secs. 6.1(o), 6.2(b)(vi), 6.2(a)(v)(E), 6.2(b)(vi).

673 The Plan Processor is required to create and implement an annual audit plan that includes a review of all Plan Processor policies, procedures, control structures, and tools that monitor and address data security. *Id*. secs. 6.2(a)(v)(B) and (C), app. D secs. 4.1.3, 5.3.

674 Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security, Release No. 89632 (Aug. 21, 2020), 85 FR 65990 (Oct. 16, 2020).

on how the new and existing SCI entities' current market practices affect the baseline against which the economic effects are measured.

#### a. Systems Classification and Lifecycle Management

Based on the experience of Commission most current SCI entities undertake some form of lifecycle management program that includes acquisition, integration, support, refresh and disposal of covered systems, as applicable, and the sanitization of end-of-life systems.

#### b. Third-Party Vendor Management and Oversight

Globally the end-user spending on public cloud services is estimated to grow 20.4% in 2022 to a total of $494.7 billion, up from $410.9 billion in 2021.[675] In terms of market concentration, as of Q1 2022, the three largest CSPs collectively have the market share of 65 percent global spending on cloud computing[676] and the eight largest CSPs have roughly 80 percent of the market.[677] SCI entities employ cloud service providers.

---

675 *See* Press Release, Gartner.com (Apr. 19, 2020), *available at* https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022.

676 *See* Synergy Research Group, *Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total*, PR Newswire (Apr. 28, 2022), *available at* https://www.prnewswire.com/news-releases/huge-cloud-market-still-growing-at-34-per-year-amazon-microsoft--google-now-account-for-65-of-the-total-301535935.html (estimating as of Q1 2022 that the breakdown is: Amazon Web Services (AWS): 33%; Microsoft Azure: 22%; Google Cloud: 10%).

677 *Id.*

Some of the largest cloud service providers appear to be familiar with the Regulation SCI requirements with which SCI entities are obliged to comply.[678]

Both new and existing SCI entities may have existing agreements with third-party providers that govern the obligations and expectations as between an SCI entity and a third-party provider it utilizes. These documents may not currently be consistent with the SCI entity's requirements under the proposed amendments Regulation SCI. Some SCI entities may currently rely on a third-party provider's standard contract or SLA, which may not been drafted with Regulation SCI's requirements in mind. Similarly, some existing agreements between the SCI entity and a third-party provider may provide the third-party provider with the contractual right to be able to make decisions that would negatively impact an SCI entity's obligations in the third-party provider's "commercially reasonable discretion." Likewise, existing agreements may include defined terms that differ from those under the proposed amendments.

Regardless of their size, SCI entities typically enter into contracts with third-party providers to perform a specific function for a given time frame at a set price. At the conclusion of a contract, it may be renewed if both parties are satisfied. Because prices typically increase over time, there may be some need to negotiate a new fee for continued service. Negotiations also occur if additional services are requested from a given third-party provider. In the instance where additional services are required mid-contract, for

---

678 For example, *see* Microsoft Azure, *Regulation Systems Compliance and Integrity (SCI) Cloud Implementation Guide* (2019), *available at* https://azure.microsoft.com/mediahandler/files/resourcefiles/microsoft-azure-regulation-systems-compliance-and-integrity-sci-cloud-implementation-guide/AzureRegSCIGuidance.pdf; or Google Cloud, *U.S. Securities & Exchange Commission Regulation Systems Compliance & Integrity (Regulation SCI)* (Dec. 2021), *available at* https://services.google.com/fh/files/misc/sec_regulation_sci_gcp_whitepaper.pdf.

example, due to increased regulatory requirements, the third-party provider may be able to separately bill for the extra work that it must incur to provide the additional service, particularly if that party is in a highly concentrated market for that service and can wield market power. Alternatively, the service provider may be forced to absorb the additional cost until the contract can be renegotiated. This may be the case because that condition is specified in the contract with the SCI entity.

**Request for comment**

95. The Commission requests that commenters provide relevant data on the number of third-party providers available to SCI entities by their types of services they offer or by the types of systems, such as critical SCI systems, SCI systems, and indirect SCI systems.

96. To what extent do third-party providers compete with each other for SCI entities?

**c. SCI Review**

With respect to business continuity and disaster recovery plan reviews, FINRA Rule 4370 requires a broker-dealer to conduct an annual review of its business continuity plan. FINRA has observed that some broker-dealers[679] engaged in annual testing to evaluate the effectiveness of their business continuity plans.[680] With respect to broker-dealer reporting to their boards regarding cybersecurity policies and procedures and cybersecurity incidents, the board reporting frequency ranged from quarterly to ad-hoc

---

679 FINRA did not disclose the number or identity of the firms but it is likely that larger firms have more robust systems and practices given their greater resources.

680 *See* FINRA, 2019 Report on Examination Findings and Observations: Business Continuity Plans (BCPs), *supra* note 600.

among the firms FINRA reviewed.[681] Approximately two-thirds of the broker-dealers (68%) examined in a 2015 survey had an individual explicitly assigned as the firm's CISO which might suggest extensive executive leadership engagement.

#### d. Current SCI Industry Standards

As of 2015, the majority of broker-dealers reported utilizing one or more frameworks with respect to cybersecurity[682] either mapping directly to the standard or using it as reference point. Some of the standards such as COBIT may have broad application to various areas of IT but it is unclear to what extent broker-dealers utilize such standards beyond cybersecurity.

Also, each of the two exempt clearing agencies (Euroclear Bank SA/NV, and Clearstream Banking, S.A.) publish disclosure framework reports[683,] that purport to describe the policies and procedures relating to the 24 principles and five responsibilities set forth in the Principles for Financial Market Infrastructures (PFMI) published by CPSS and IOSCO.[684] The PFMI establishes new international standards for financial market

---

681 *See Report on Cybersecurity Practices*, *supra* note 621. At a number of firms, the board received annual cybersecurity-related reporting while other firms report on a quarterly basis. A number of firms also provide ad hoc reporting to the board in the event of major cybersecurity events.

682 *See supra* note 622. Among the firms that were part of the FINRA sweep, nearly 90% used one or more of the NIST, ISO or ISACA frameworks or standards. More specifically, 65% of the respondents reported that they use the ISO 27001/27002 standard while 25% use COBIT. Some firms use combinations of these standards for various parts of their cybersecurity programs. The COBIT standard, for example, is focused more on information technology governance than cybersecurity per se. In addition, several firms underscored the utility of the PCI Standard as well as the SANS Top 20.

683 Clearstream, *Principles for financial market infrastructures: Disclosure Framework* (Dec. 23, 2020), *available at* https://www.clearstream.com/resource/blob/1386778/3458c1c468e5f40ddf5dc970e8da4af2/cpmi-iosco-data.pdf; Euroclear Bank, *Disclosure Framework CPMI IOSCO 2020* (June 2020), *available at* https://www.euroclear.com/content/dam/euroclear/About/business/PA005-Euroclear-Bank-Disclosure-Framework-Report.pdf.

684 Bank for International Settlements (BIS), *Principles for Financial Market Infrastructures: Disclosure Framework and Assessment Methodology* (Dec. 2012), *available at* https://www.bis.org/cpmi/publ/d106.pdf.

infrastructures (FMIs) including payment systems that are systemically important, central securities depositories, securities settlement systems, central counterparties and trade repositories and prescribes the form and content of the disclosures expected of financial market infrastructures. Most relevant, principle 17 on operational risk offers guidelines on policies and procedures to identify, monitor, and manage operational risks, vulnerabilities, and threats; capacity planning; stress testing; systems development and testing methodology; business continuity and disaster recovery planning and testing; vendor risk management; and board supervision of risk management, etc.

#### e. Penetration Testing

Current SCI entities are required to conduct penetration testing as part of its SCI review[685] once every three years.[686] Among the new SCI entities, two SBSDRs that are currently registered as SDRs are subject to CFTC's rules, which require conducting penetration testing of the systems with the scope of those rules at least once every year.

### 4. Other Affected Parties

In addition to new and existing SCI entities, the proposed amendments may indirectly affect other parties, namely third-party service providers to which SCI systems functionality is outsourced. As discussed in depth above, an SCI entity may decide to outsource certain functionality to, or utilize the support or services of, a third-party provider (which would include both affiliated providers as well as vendors unaffiliated with the SCI entity) for a variety of reasons, including cost efficiencies, increased

---

685 Specifically, paragraph (b)(1) of Rule 1003 currently requires that "[p]enetration test reviews of the network, firewalls, and production systems shall be conducted at a frequency of not less than once every three years…". Rule 1003(b)(1).

686 *See* SCI Adopting Release, *supra* note 1, at 72344.

automation, particular expertise, or functionality that the SCI entity does not have in-house. Based on Commission staff experience, the Commission believes that these third-party providers, play a growing role with respect to SCI systems and indirect SCI systems, and the Commission anticipates that third-party providers will likely arise to provide other types of functionality, service, or support to SCI entities that are not contemplated yet today.[687]

Due to data limitations, we are unable to quantify or characterize in much detail the structure of these various service provider markets.[688] The Commission lacks specific information on the exact extent to which third-party service providers are retained, the specific services they provide, and the costs for those services beyond the estimates discussed above for cloud service providers. We also do not have information about the market for these services, including the competitiveness of such markets. We request information from commenters on the services related to SCI systems and indirect systems provided by third parties to new and existing SCI entities, the costs for those services, and the nature of the market for these services.

---

687 It has long been recognized that the financial services industry is increasingly relying on service providers through various forms of outsourcing. *See, e.g.*, Bank for International Settlements, *Outsourcing in Financial Services* (Feb. 15, 2005), *available at* https://www.bis.org/publ/joint12.htm. Recent estimates suggest that the aggregate contract value of outsourcing in the financial services industry is on the order of $10 to $20 billion. *See, e.g.*, Business Wire, *Insights on the Finance and Accounting Outsourcing Global Market to 2026* (Jan. 14, 2022), *available at* https://www.businesswire.com/news/home/20220114005440/en/Insights-on-the-Finance-and-Accounting-Outsourcing-Global-Market-to-2026---Featuring-Accenture-Capgemini-and-Genpact-Among-Others---ResearchAndMarkets.com.

688 Although certain regulatory filings may shed a limited light on the use of third-party service providers, we are unaware of any data sources that provide detail on the overall picture for each of the new and existing SCI entities.

### C. Analysis of Benefits and Costs of Proposed Amendments

The proposed amendments both expand the scope of Regulation SCI to reach new entities and also strengthen existing requirements in Regulation SCI that would apply to both old and new entities. This section explores the benefits and costs of these changes. First, we discuss the general benefits and costs of the proposed amendments to Regulation SCI. Next, we discuss the expansion of Regulation SCI to certain new SCI entities and the rationale for it. Finally, we analyze the specific benefits and costs of applying each provision of amended Regulation SCI to each of the proposed new SCI entities and current SCI entities.[689] The Commission encourages commenters to identify, discuss, analyze, and supply relevant data, information, or statistics regarding the benefits and costs.

The Commission is providing both a qualitative assessment and quantified estimates, including ranges, of the potential economic effects of the proposal where feasible. The overall magnitude of the economic effects will depend, in part, on the extent to which the new and current SCI entities already have in place practices that are aligned with the requirements of Regulation SCI, including the proposed amendments. New SCI

---

[689] For purposes of measuring the benefits and costs of the proposed rule on both existing and new SCI entities, this analysis assumes that market participants are compliant with existing applicable Commission, FINRA, CFTC, and other applicable rules, including those requiring registration and the rules and regulations applicable to such registered entities. To the extent that some entities engaged in activities including crypto asset securities are not, but should be, FINRA or Commission registered entities, they may incur additional costs to comply with existing registration obligations that are distinct from the costs associated with the proposed rule amendments and are not discussed in this analysis. Similarly, any benefits from coming into compliance with existing registration obligations are also not discussed in this analysis. For such entities, we expect the benefits and costs specifically associated with the proposed rule amendments to be same as those described below for existing and new SCI entities that are currently registered.

entities' costs of implementing Regulation SCI could also differ with the number and size of their systems affected.

In many cases it is difficult to quantify the economic effects, particularly those beyond the costs estimated in the Paperwork Reduction Act analysis. As explained in more detail below, the Commission in certain cases does not have, and does not believe it can reasonably obtain, data or information necessary to quantify certain effects. For instance, the Commission finds it impracticable to quantify many of the benefits associated with amended Regulation SCI. Indeed, we lack information that would allow us to predict the reduction in frequency and severity of SCI events or the specific cost savings that might arise from avoiding the harm Regulation SCI is designed to prevent. Further, even in cases where the Commission has some data, quantification is not practicable due to the number and type of assumptions necessary to quantify certain economic effects, which render any such quantification unreliable. The Commission requests that commenters provide relevant data and information to assist the Commission in quantifying the economic consequences of proposed amendments to Regulation SCI.

### 1. General Benefits and Costs of Proposed Amendments

Regulation SCI promotes the capacity, integrity, resiliency, availability, and security of SCI systems, as well as transparency about systems problems when they do occur, and thereby promote investors' confidence in market transactions. SCI events can today have broad impacts because of the growth of electronic trading, which allows increased volumes of securities transactions in a broader range of asset classes, at increasing speed, by a variety of trading platforms;[690] changes in the way SCI entities

---

690 *See* section I and *supra* note 3.

employ technology, including the increasing importance of third-party service providers to ensure reliable, resilient, and secure systems;[691] a significant increase in cybersecurity events across all types of companies, including SCI entities;[692] and an evolution of the threat environment.[693] A joint report from the World Economic Form and Deloitte states that "new interconnections and collective dependencies on certain critical providers significantly contribute to the number of vulnerable nodes that could threaten and exploit the financial system's essential functions."[694]

Expanding Regulation SCI to new SCI entities will help to ensure that the core technology systems of these newly designated SCI entities are robust, resilient, and secure—especially for those entities that have not already adopted comparable measures on their own—and would also help to improve Commission oversight of the core technology of key entities in the U.S. securities markets.[695]

---

691 *See* sections III.B, III.B.2.a.

692 *See* section III.B.3.

693 *See id.*

694 *See* World Economic Forum, *Beneath the Surface: Technology-Driven Systemic Risks and the Continued Need for Innovation* (Oct. 28, 2021) at 14, *available at* https://www.weforum.org/reports/beneath-the-surface-technology-driven-systemic-risks-and-the-continued-need-for-innovation/; *see also* Henning Soller, et al., *Innovative Technologies in Financial Institutions: Risk as a Strategic Issue*, McKinsey Digital (Sep. 25, 2020), *available at*: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/innovative-technologies-in-financial-institutions-risk-as-a-strategic-issue.

695 For example, some expert views suggest that current SCI entities' compliance with Regulation SCI likely prepared those entities to be more resilient and more prepared to face times of increased volatility—beyond what their prudent business practices may have allowed. For example, one industry publication notes that even as financial firms "updated their [business continuity planning] after the Sept. 11, 2001, terrorist attacks and superstorm Hurricane Sandy in 2012, when these events exposed cracks in Wall Street's contingency plans," they were still "more prepared during COVID-19 thanks to Regulation SCI for Systems, Compliance and Integrity." *See, e.g.*, *Is*

The Commission is also proposing amendments to update Regulation SCI in order to strengthen its requirements. These amendments would benefit markets and market participants by reducing the likelihood, severity, and duration of market disruptions arising from systems issues, among both current and new SCI entities, whether such events may originate from natural disasters, third-party provider service outages, cybersecurity events, hardware or software malfunctions, or any other sources.[696] Decreasing the number of trading interruptions can improve price discovery and liquidity because such interruptions interfere with the process through which relevant information gets incorporated into security prices and, may thereby, temporarily disrupt liquidity flows.[697] Trading interruptions in one security can also affect securities trading in other

---

*Remote Trading Leading to a Paradigm Shift on the Trading Desk?*, *supra* note 2. Similarly, a senior executive at FINRA stated in an interview that he found most surprising the resiliency of the market during COVID-19 and said "a lot of credit goes to the SEC for [the market's resiliency] with respect to adopting [Regulation SCI]." FINRA, Podcast: *Market Structure & COVID-19: Handling Increased Volatility and Volumes*, at 24:38 - 25:08 (Apr. 28, 2020), *available at* https://www.finra.org/media-center/finra-unscripted/market-structure-covid19-coronavirus (featuring an interview with FINRA's then-Executive VP of Market Regulation and Transparency Services, Tom Gira).

696 For example, the Ponemon Institute's 2016 Cost of Data Center Outages report estimates the average cost per minute of an unplanned outage was $8,851 for the average data center the Institute surveyed in 2016. *See* Ponemon Institute, *2016 Cost of Data Center Outages* 14 (Jan. 19, 2016) *available at* https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf. Also, although it is difficult to estimate the total cost of a cyberattack at an SCI entity, a potential effect of a cyberattack involving an SCI entity is a data breach. According to the IBM's 2022 Cost of a Data Breach report, the average cost of a data breach in the United States is $9.44 million, and the report added that "[f]or 83% of companies, it's not if a data breach will happen, but when. Usually more than once." *See* IBM, *2022 Cost of a Data Breach*, *available at* https://www.ibm.com/reports/data-breach#:~:text=Average%20cost%20of%20a%20data,million%20in%20the%202020%20report. Relatedly, another study reports that in 2020 the average loss in the financial services industry was $18.3 million per company per incident. The average cost of a financial services data breach was $5.85 million. *See* Jennifer Rose Hale, *The Soaring Risks of Financial Services Cybercrime: By the Numbers, Diligent* (Apr. 9, 2021), *available at* https://www.diligent.com/insights/financial-services/cybersecurity/#.

697 *See* Osipovich, Alexander, *NYSE Glitch Causes Erroneous Prices in Hundreds of Stocks*, Wall St. J. (online edition) (Jan. 24, 2023), *available at* https://www.wsj.com/articles/dozens-of-nyse-stocks-halted-in-opening-minutes-after-wild-price-swings-11674585962 (retrieved from Factiva database).

markets. For example, an interruption in the market for index options and other securities that underlie derivatives securities could harm the price discovery process for derivatives securities, and liquidity flows between the stock market and derivatives markets could be restricted. For this reason, market-based incentives alone are unlikely to result in optimal provision of SCI-related services. In this context, having plans and procedures in place to prepare for and respond to system issues is beneficial,[698] and the proposed amendments to Regulation SCI would help ensure that the infrastructure of the U.S. securities markets remains robust, resilient, and secure. A well-functioning financial system is a public good.

The Commission recognizes that the proposed amendments to Regulation SCI would impose costs on SCI entities, as well as costs on certain members, participants, customers (in the case of SCI broker-dealers), or third-party providers of SCI entities. The majority of these costs would be direct compliance costs, which are discussed in detail below for each requirement of proposed Regulation SCI. For current SCI entities, these costs would relate to the areas of Regulation SCI that are being amended. For new SCI entities, the costs would relate to complying with the entirety of Regulation SCI, including the proposed amendments. For current SCI entities, these costs may be mitigated to the extent the SCI entity's current business practices are already consistent with the proposed requirements, and if, as a result of compliance, the SCI entity avoids

---

698 For example, according to the IBM Report, in the context of system issues arising from cybersecurity events, having an incident response plan and "testing that plan regularly can help [each firm] proactively identify weaknesses in [its] cybersecurity and shore up [its] defenses" and "save millions in data breach costs." *See 2022 Cost of a Data Breach*, *supra* note 696. *See also* Alex Asen et al., *Are You Spending Enough on Cybersecurity* (Feb. 19, 2020), *available at* https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity (noting "[a]s the world becomes ever more reliant on technology, and as cybercriminals refine and intensify their attacks, organizations will need to spend more on cybersecurity").

the costs associated with a systems failure or breach. Likewise, for new SCI entities, these costs may be mitigated to the extent the SCI entity's current business practices are already consistent with the requirements of Regulation SCI, including the proposed amendments, and if, as a result of compliance, the SCI entity avoids the costs associated with a systems failure or breach.

Some portion of compliance costs could be economic transfers. This may be the case if compliance with a particular provision entails making use of certain third-party providers, and the market for third-party provider services is not itself competitive.[699] In such a case, third-party providers would make economic profits from the services they offer and the fees they charge, and some of the services fees charged would be economic transfers from SCI entities to third-party providers.

The proposed amendments could have other potential costs. For example, entities covered by the proposed rule frequently would need to make systems changes to comply with new and amended rules and regulations under Federal securities laws and SRO rules. For entities that meet the definition of SCI entity, because they would need to comply with the proposed amendments when they make systems changes, the proposed amendments could increase the costs and time needed to make systems changes to comply with new and amended rules and regulations. The Commission requests comment on the nature of such additional costs and time.

**Request for Comment**

---

699 *See, e.g.*, Yoon-Ho Alex Lee, *SEC Rules, Stakeholder Interests, and Cost-Benefit Analysis*, 10 Mkts L.J. 311 (2015), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2541805 (retrieved from SSRN Elsevier database; Yoon-Ho Alex Lee, *The Efficiency Criterion of Securities Regulation: Investor Welfare or Total Surplus?*, 57 Ariz. L. Rev. 85 (2015), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2406032 (retrieved from SSRN Elsevier database.

The Commission requests comment on all aspects of the Overall Benefits and Costs of Proposed Amendments discussion. In addition, the Commission is requesting comment on the following specific aspects of the discussion:

97. For new SCI entities, what activities do you currently perform (either because you are required to or you have chosen to voluntarily) that are already consistent with the requirements of Regulation SCI?

98. For new SCI entities and current SCI entities, can compliance with Regulation SCI result in the benefits the Commission describes in the analysis?

99. Are commenters aware of any data that can be used to quantify any aspects of benefits?

100. The Commission seeks commenters' views regarding the prospective costs, as well as the potential benefits, of applying Regulation SCI to SBSDRs. Are there characteristics specific to SBSDRS or the SBS market that would make applying Regulation SCI broadly or any specific provision or proposed new provision Regulation SCI challenging for SBSDRs? How much time would an SBSDR reasonably need to come into compliance with Regulation as proposed? Commenters should quantify the costs of applying Regulation SCI to SBSDRs, to the extent possible. Commenters are urged to address specifically each requirement of Regulation SCI and note whether it would be reasonable to apply each such requirement to SBSDRs and what the benefits and costs of such application would be.

101. For current SCI entities, what activities do you currently perform that are already consistent with the proposed amendments that seek to strengthen the obligations of SCI entities?

102. Are the Commission's estimates of incremental compliance costs owing to these proposed reasonable? Please note that the Commission does not purport to estimate the total costs of all activities SCI entities will perform in promoting the capacity, integrity, resiliency, availability, and security of their automated systems. The Commission's estimates pertain only to the increase in costs that will arise directly as a result of having to comply with the specific provisions of the proposed rules to the extent the covered entity has not already been performing such activities on its own or pursuant to other relevant rules or regulations.

103. What activities do you currently perform that go beyond the proposed amendments to Regulation SCI?

104. For current SCI entities, will compliance with the proposed amendments to Regulation SCI result in performing activities that go significantly above and beyond their current approach to promoting the capacity, integrity, resiliency, availability, and security of their automated systems? In other words, will these new rules require a significant rearranging of their resources beyond what they are already complying with voluntarily?

105. What are the costs of Regulation SCI? Are commenters aware of any data that can be used to quantify any aspects of costs?

**2. Expansion to New SCI Entities**

The Commission proposes to expand the definition of SCI entity to encompass SBSDRs, certain broker-dealers, and additional clearing agencies exempted from registration. These entities are key market participants that play a significant role in the U.S. securities markets and, in the event of a systems issues, they have the potential to impact investors, the overall market, or the trading of individual securities. Under the

proposed amendments, the new SCI entities would become subject to all provisions of Regulation SCI, including the provisions that the Commission proposes to amend for SCI entities, as discussed in section III.C of this release. We discuss in this section the entities to which Regulation SCI would be extended, including the rationale for doing so. The benefits and costs associated with applying each of the Regulation SCI requirements to these entities are subsequently discussed in section V.D.3.

The Commission preliminarily estimates that as a result of the proposed amendments to the definition of "SCI entity" in Rule 1000, there would be a total of 21 new SCI entities that would become subject to the requirements of Regulation SCI. These include 2 SBSDRs, 17 SCI broker-dealers, and 2 exempt clearing agencies.[700] Generally, inclusion of these new SCI entities in the amended definition is expected to help ensure systems resiliency at such entities and reduce the potential for incidents at these entities to have broad, disruptive effects across the securities markets and for investors. Furthermore, applying Regulation SCI to these entities increases market protections by establishing these obligations under the Exchange Act so that the Commission may enforce them directly and examine for compliance and provides a uniform requirement for all SCI entities.

**a. SBSDRs**

Currently, two SBSDRs are registered with the Commission and are subject to Rule 13n-6. The SBSDRs registered with the Commission are also registered with the

---

700 The Commission is estimating 23 new SCI entities in the PRA section based on the PRA's forward-looking requirement to account for persons to whom a collection of information is addressed by the agency within any 12-month period. But for purposes of the Economic Analysis, this section analyzes the baseline of existing entities that will be new SCI entities and then predicts the cost to those entities if the rule were to be adopted. Accordingly the Economic Analysis assumes 21, rather than 23, new SCI entities.

CFTC as swap data repositories (SDRs) and accordingly, with respect to systems of concern to the CFTC, are subject to CFTC rules and regulations related to swap data repositories, including the CFTC's System Safeguards rule.

Systems failures at SBSDRs can limit access to data, call into question the integrity of data, and prevent market participants from being able to report transaction data, and receive transaction data, and thereby have a large impact on market confidence, risk exposure, and market efficiency. For example, were an SBSDR to experience a systems issue, market participants could be prevented from receiving timely information regarding accurate prices for individual SBSs – such as aggregate market exposures to referenced entities (instruments), positions taken by individual entities or groups, and data elements necessary for a person to determine the market value of the transaction.[701] This could contribute to market instability.

Having SBSDRs comply with Regulation SCI would reduce the risk of system issues at SBSDRs and allow continued transparency and access to data. As noted above in the baseline, SBSDRs are currently subject to Rule 13n-6, which requires an SBSDR to "establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its systems provide adequate levels of capacity, integrity, resiliency, availability, and security." However, as described in detail below, the requirements of Regulation SCI that go beyond those required in Rule 13n-6—such as policies and procedures that include specific elements for infrastructure planning, up-to-date system

---

701 *See* Access to Data Obtained by Security-Based Swap Data Repositories, Securities Exchange Act Release No. 78716 (Aug. 29, 2016), 81 FR 60585, 60594, 60605-6 (Sep. 2, 2016). In that release, the Commission estimates that approximately 300 relevant authorities may make requests for data from security-based swap data repositories.

development and testing methodology, regular systems reviews and testing, BC/DR planning, monitoring for SCI events, and standards to facilitate successful collection, processing, and dissemination of market data—should deliver benefits beyond those currently achieved through Rule 13n-6.

The coverage of SBSDRs under the proposed amendments to Regulation SCI would augment the current principles-based requirements for policies and procedures on operational risk with detailed, more specific requirements to help ensure that SBSDR market systems are robust, resilient, and secure and that policies and procedures in place at SBSDRs meet requirements necessary to maintain the robustness of critical systems.

**b. SCI Broker-Dealers**

The Commission proposes to include certain broker-dealers—to be referred to as "SCI broker-dealers"—in the definition of SCI entity. This expansion would be limited to broker-dealers that exceed one or more size thresholds. The first proposed threshold is a total assets test. This test scopes within Regulation SCI any broker-dealers with five percent (5%) or more of the total assets[702] of all security brokers and dealers during at least two of the four preceding calendar quarters ending March 31, June 30, September 30, and December 31. The second proposed threshold is a transaction activity test. This test scopes within Regulation SCI any broker-dealer that transacted ten percent (10%) or more of the total average daily dollar volume by applicable reporting entities during at least four of the preceding six calendar months in any of the following asset classes: NMS stocks, exchange-listed options contracts, Agency Securities, or U.S. Treasury Securities.

---

[702] *See supra* note 169.

The Commission proposes to limit the definition of "SCI systems" for an SCI broker-dealer that qualifies as an SCI entity that satisfies only one or more transaction activity thresholds.[703] Specifically, only those systems that relate to the asset class for which the trading activity threshold is met (*i.e.*, NMS stocks, exchange-listed options contracts, Treasury Securities, or Agency Securities) would be "SCI systems" or "indirect SCI systems."[704] Broker-dealers may have multiple business lines and transact in different types of securities, and the proposal reflects the Commission's preliminary conclusion that systems related to asset classes that do not meet the rule's transaction activity threshold are unlikely to pose risk to the maintenance of fair and orderly markets if the systems with respect to that type of security were unavailable (assuming the systems for the distinct asset class are separate) relative to the burden of complying with the regulation's more stringent requirements.

In contrast, no such limitation applies to an SCI broker-dealer that qualifies as an SCI entity because it satisfies the total assets threshold. In this case, broker-dealers that qualify as SCI entities due to the total assets threshold are subject to Regulation SCI requirements for all of its applicable systems, regardless of the asset classes such systems relate to.[705] As discussed in section III.A.2.b.iii, this approach with respect to the total

---

703 *See* section III.A.2.b(iv).

704 *See* section III.A.2.b(iv). As explained above in section III.A.2.b.v, although crypto asset securities are not a separately enumerated asset class for the volume threshold, the SCI systems and indirect SCI systems pertaining to crypto asset securities that are NMS stocks, exchange-listed options, U.S. Treasury Securities, or Agency securities would be subject to Regulation SCI, including as it is proposed to be amended, as discussed in section III. C, with respect to the asset class for which the SCI broker-dealer satisfies the threshold.

705 As explained above, any system of an SCI broker-dealer meeting the total asset threshold that pertains to any type of security, including crypto asset securities, that meets the definition of SCI systems or indirect SCI systems would be covered by Regulation SCI.

assets threshold takes into consideration the multiple roles that the largest broker-dealers play in the U.S. securities markets. Not only do some of the largest broker-dealers generate liquidity in multiple types of securities, but many also operate multiple types of trading platforms. Entities with assets at this level also take risks that they may seek to hedge across asset classes, in some cases using "central risk books" for that and other purposes, and engage in routing substantial order flow to other trading venues. For these reasons, the Commission believes that systems issues at firms having assets at this level could have the potential to impact investors, the overall market, and the trading of individual securities, following a systems failure in any market in which they operate.

The Commission estimates that there would be 17 SCI broker-dealers, five of which would satisfy both the total assets threshold and at least one of the transaction activity thresholds, and twelve others of which would satisfy at least one of the transaction activity thresholds.[706] As discussed in section V.B.1.b.i, figure 6 (Panel A) shows the distribution of all registered broker-dealer firms between Q4 2021 and Q3 2022 by level of total assets. Figure 6 (Panel B) represents the distribution of all registered broker-dealer firms by percentage of aggregate total assets.[707] It shows that five firms accounted for roughly half of broker-dealer aggregate total assets and thus each could pose a substantial risk to the maintenance of fair and orderly markets in the event of a systems issue. During all four quarters from Q4 2021 to Q3 2022, all five firms reported to the Commission, on Form X-17A-5 (§ 249.617), total assets in an amount that

---

706 *See* section III.A.2.b(iv).

707 Panel A and Panel B in figure 6 show the same information as in figure 1 in section V.B.1.b.i., but with 5% threshold lines added. The threshold line in Panel A shows the average of 5% of aggregate total assets in each quarter from Q4 2021 to Q3 2022.

equals five percent (5%) or more of the total assets of all security brokers and dealers.[708] Figures 7 through 10 represent the distribution by level of transaction activity as measured by average daily dollar volume[709] (Panel A) and the distribution of firms by percentage of transaction activity[710] (Panel B) for each of four asset classes including NMS stocks, exchange-listed options, U.S. Treasury Securities, and Agency Securities respectively.[711] These figures clearly show that a few firms consistently accounted for a significant percentage of transaction activity over the six month period and thus each could pose a substantial risk to the maintenance of fair and orderly markets in the event of a systems issue. During at least four months of the six month period, six NMS stocks trading firms, six exchange-listed options contracts trading firms, four U.S. Treasury Securities trading firms, and six Agency Securities trading firms transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar of the corresponding markets. Most of these firms transacted more than ten percent (10%) during all six months.[712]

These large broker-dealers, by virtue of the total assets or transaction activity each represents over a period of time, play a significant role in the orderly functioning of U.S.

---

708 Each of these firms would satisfy the proposed total assets thresholds for an "SCI broker-dealer". *See* section III.A.2.b.iii (discussing proposed thresholds for an "SCI broker-dealer").

709 These measures are described in more detail in section III.A.2.b.iii.

710 *Id.*

711 Panel A and Panel B in figures 7 through 10 show the same information as in figures 2 through 5 in section V.B.1.b.i., but with 10% threshold lines added. The threshold line in each Panel A shows the average of 10% of aggregate average daily dollar volume reported to the plan processors (SIPs) of the CTA/CQ Plans and Nasdaq UTP Plan, OPRA Plan, or FINRA TRACE in each respective asset class from Jan. 2022 to June 2022. The threshold line in each Panel B equals 10%.

712 Each of these firms would satisfy the proposed transaction activity thresholds for an "SCI broker-dealer". *See* section III.A.2.b.iii (discussing proposed thresholds for an "SCI broker-dealer").

securities markets. If such a broker-dealer was adversely affected by a system issue, then the impact could not only affect the broker-dealer's own customers, but also disrupt the overall market, by compromising or removing significant liquidity from the market, interrupting the price discovery process, or indirectly contributing to capacity issues at other broker-dealers.[713]

Application of Regulation SCI is expected to reduce the likelihood of system issues at these largest broker-dealers as well as mitigate the effects of any such event. While it is possible that these broker-dealers may have systems in place due to market-based incentives, there are reasons to believe that these incentives may be insufficient. First, as mentioned in section V.C.1, a well-functioning financial system is a public good.[714] Second, investment in SCI systems takes the form of a hidden-action problem. As such, due to principal-agent conflict, it may not be possible for customers or counterparties to observe the degree of investment in SCI systems and thus to provide market-based discipline from underinvestment. In this case, a broker-dealer's investment in SCI systems would offer benefits to customers and counterparties who might incur switching costs to find a different broker if a substantial systems issue occurred. These benefits are likely to be especially high for market participants who rely on a single counterparty (such as is sometimes the case in Treasury securities and prime brokerage relationships), and for retail investors who have invested in the relationship with a single retail broker.

---

713 *See* section III.A.2.b(iv).

714 Since broker-dealers are not compensated for the positive impact that their systems investments have on other entities, they lack sufficient incentives to invest on others' behalf. *See*, for instance, Mazaher Kianpour et al., *Advancing the concept of cybersecurity as a public good*, 116 SIMULATION MODELLING PRACTICE AND THEORY 102493 (2022).

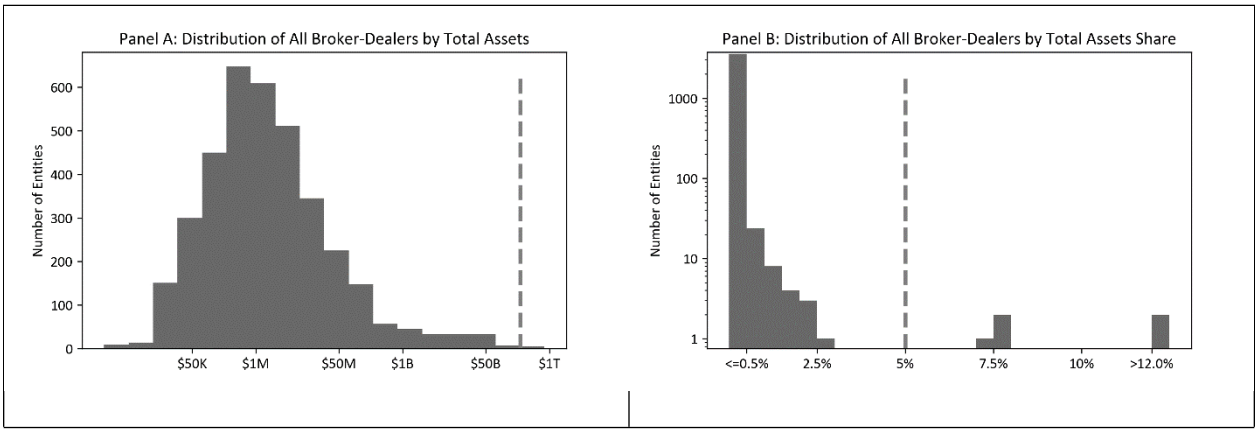



FIGURE 6. DISTRIBUTION OF BROKER-DEALERS BY TOTAL ASSETS (PANEL A) AND TOTAL ASSETS SHARE (PANEL B)

*Notes:* Panel (A): distribution of broker-dealers by average quarterly total assets. Panel (B): distribution of broker-dealers by average quarterly percentage of aggregate total assets. Data are from broker-dealer FOCUS Report Form X-17A-5 Schedule II filings from Q4 2021 to Q3 2022. Also for additional detail on the calculation of total assets of all security broker-dealers, *see supra* note 127.

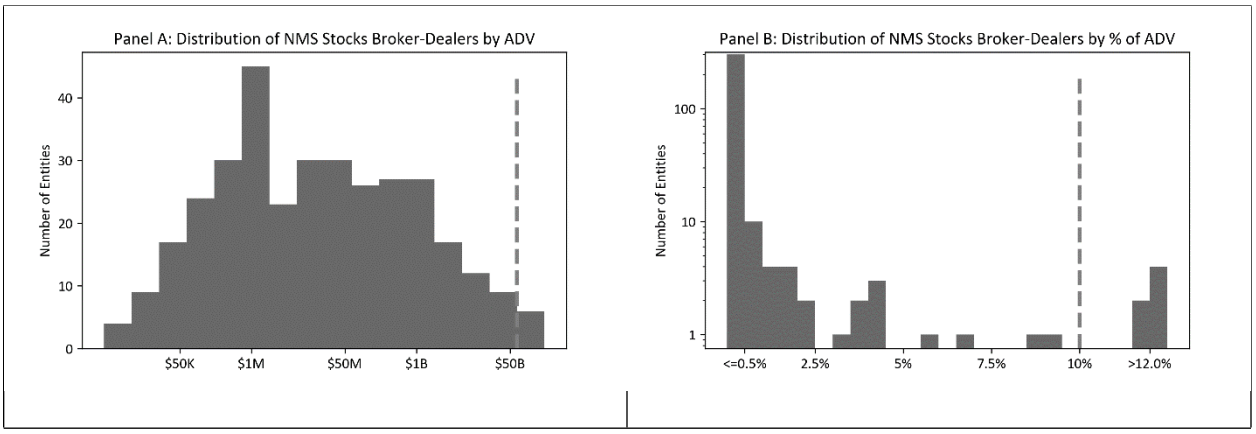



FIGURE 7. DISTRIBUTION OF BROKER-DEALERS, NMS STOCKS ASSET CLASS

*Notes:* Panel (A): distribution of broker-dealers by average of monthly average daily dollar volume. Panel (B): distribution of broker-dealers by average of monthly percentage of aggregate average daily dollar volume. Data are from Consolidated Audit Trail (CAT) data from Jan. 2022 to June 2022 and the plan processors (SIPs) of the CTA/CQ Plans and Nasdaq UTP Plan. CTA Plan, available at https://www.ctaplan.com; Nasdaq UTP Plan, available at https://www.utpplan.com.

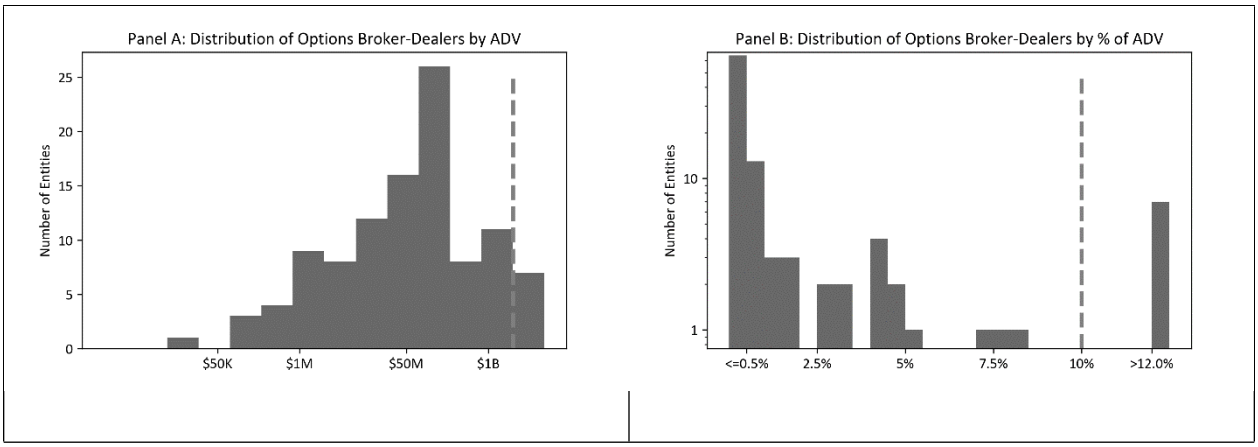



FIGURE 8. DISTRIBUTION OF BROKER-DEALERS, EXCHANGE-LISTED OPTIONS ASSET CLASS

*Notes:* Panel (A): distribution of broker-dealers by average of monthly average daily dollar volume. Panel (B): distribution of broker-dealers by average of monthly percentage of aggregate average daily dollar volume. Data are from Consolidated Audit Trail (CAT) data from Jan. 2022 to June 2022 and Options Price Reporting Authority (OPRA) data.

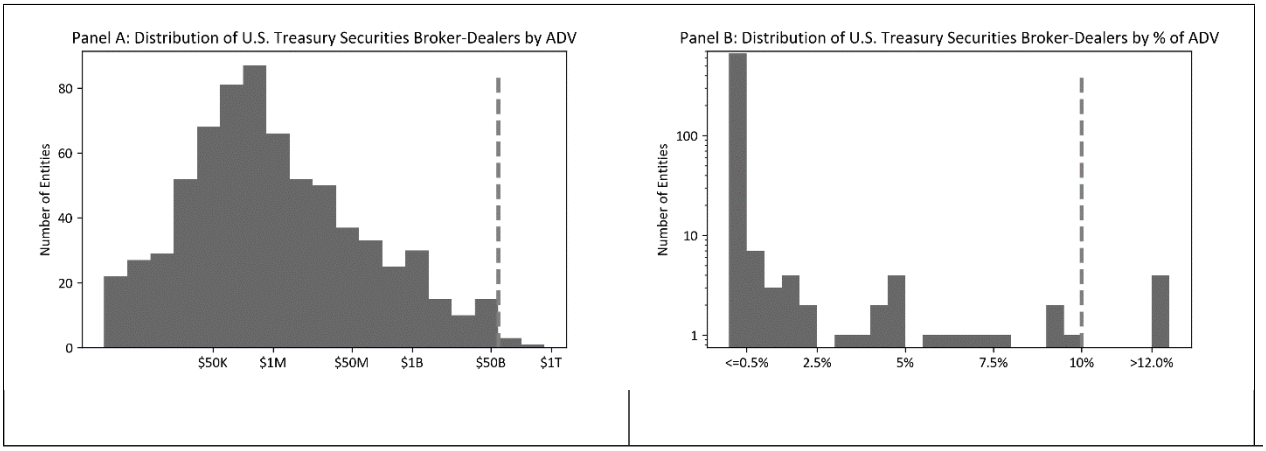



FIGURE 9. DISTRIBUTION OF BROKER-DEALERS, U.S. TREASURY SECURITIES ASSET CLASS

*Notes*: Panel (A): distribution of broker-dealers by average of monthly average daily dollar volume. Panel (B): distribution of broker-dealers by average of monthly percentage of aggregate average daily dollar volume. Data are from TRACE for Treasury Securities data from Jan. 2022 to June 2022 and FINRA TRACE.

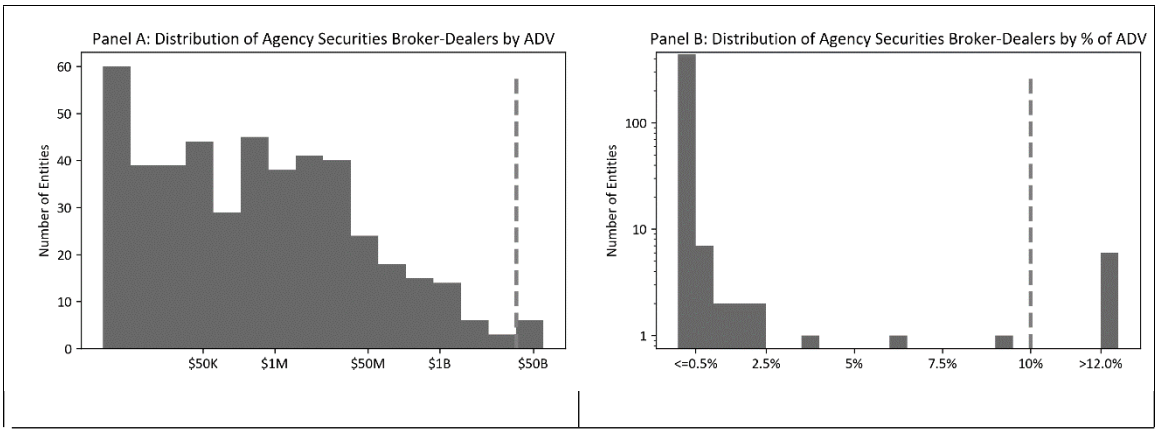



FIGURE 10. DISTRIBUTION OF BROKER-DEALERS, AGENCY SECURITIES ASSET CLASS

*Notes*: Panel (A): distribution of broker-dealers by average of monthly average daily dollar volume. Panel (B): distribution of broker-dealers by average of monthly percentage of aggregate average daily dollar volume. Data are from regulatory TRACE data from Jan. 2022 to June 2022 and FINRA TRACE.

### c. Additional Exempt Clearing Agencies

The proposed amendments would expand the scope of exempt clearing agencies covered by Regulation SCI to include two new exempt clearing agencies: Euroclear Bank SA/NV and Clearstream Banking, S.A. These exempt clearing agencies are not currently subject to Regulation SCI because Regulation SCI was initially limited to those exempt clearing agencies that were "subject to ARP" and these exempt clearing agencies are not subject to ARP. At the time it adopted Regulation SCI, the Commission stated it was taking a measured approach in applying requirements primarily to entities already covered under the ARP Inspection Program.[715]

The exempt clearing agencies not subject to ARP that the Commission proposes to scope into Regulation SCI provide CSD functions for transactions in U.S. securities between U.S. and non-U.S. persons using similar technologies as registered clearing

[715] SCI Adopting Release, *supra* note 1, at 72259.

agencies that are subject to Regulation SCI.[716] The technology systems that underpin operations of these exempt clearing agencies are critical systems that centralize and automate clearance and settlement functions for the global financial markets.[717] Such systems concentrate risk in the clearing agency.[718] A disruption to a clearing agency's operations, or failure on the part of a clearing agency to meet its obligations, could therefore serve as a source of contagion, resulting in significant costs not only to the clearing agency itself and its participants but also to other market participants across the U.S. financial system.[719] For example, an SCI event could cause a delay or disruption in

---

716 *See* section III.A.2.c.

717 *See* section III.A.2.c.

718 *See generally* Albert J. Menkveld & Guillaume Vuillemey, *The Economics of Central Clearing*, 13 Ann. Rev. Fin. Econ. 153 (2021), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3957021 (retrieved from SSRN Elsevier database). *See also* Paolo Saguato, Financial Regulation, Corporate Governance, and the Hidden Costs of Clearinghouses, 82 Ohio St. L.J. 1071, 1074-75 (2022), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269060 (retrieved from SSRN Elsevier database) ("[T]he decision to centralize risk in clearinghouses made them critical for the stability of the financial system, to the point that they are considered not only too-big-to-fail, but also too-important-to-fail institutions.").

719 *See generally* Dietrich Domanski, et al., *Central Clearing: Trends and Current Issues*, BIS Q. Rev. (Dec. 2015), *available at* https://www.bis.org/publ/qtrpdf/r_qt1512g.pdf (describing links between CCP financial risk management and systemic risk); Darrell Duffie, et al., *Policy Perspectives on OTC Derivatives Market Infrastructure*, Fed. Res. Bank N.Y. Staff Rep. No. 424, at 9 (Mar. 2010), *available at* https://ssrn.com/abstract=1534729 (retrieved from SSRN Elsevier database) ("If a CCP is successful in clearing a large quantity of derivatives trades, the CCP is itself a systemically important financial institution. The failure of a CCP could suddenly expose many major market participants to losses. Any such failure, moreover, is likely to have been triggered by the failure of one or more large clearing agency participants, and therefore to occur during a period of extreme market fragility."); Craig Pirrong, *The Inefficiency of Clearing Mandates*, Policy Analysis No. 655, at 11-14, 16-17, 24-26 (July 2010), *available at* https://www.cato.org/pubs/pas/PA665.pdf (stating, among other things, that "CCPs are concentrated points of potential failure that can create their own systemic risks," that "[a]t most, creation of CCPs changes the topology of the network of connections among firms, but it does not eliminate these connections," that clearing may lead speculators and hedgers to take larger positions, that a CCP's failure to effectively price counterparty risks may lead to moral hazard and

the settlement process with respect to certain securities, leading to a decrease in liquidity. Trading firms could be unwilling or unable to enter into new positions should prior trades suffer settlement timing delays requiring posting of additional margin at clearing agencies and the assumption of additional risk by trading firms.

Notably, Euroclear Bank SA/NV and Clearstream Banking, S.A. are already subject to Europe's CSDR, which has Operational Risk rules (Article 45) that includes many requirements that may align with those in Regulation SCI.[720] Additionally, the Commission exemptive order for one of the exempt clearing agencies requires certain provisions that are consistent with those in Regulation SCI.

### 3. Specific Benefits and Costs of Regulation SCI Requirements for All SCI Entities

#### a. Rule 1001—Policies and Procedures

Rule 1001(a) through (c) sets forth requirements relating to the written policies and procedures that SCI entities are required to establish, maintain, and enforce. New SCI entities will need to comply with these requirements for the first time. In addition, the

---

adverse selection problems, that the main effect of clearing would be to "redistribute losses consequent to a bankruptcy or run," and that clearing entities have failed or come under stress in the past, including in connection with the 1987 market break); Glenn Hubbard et al., *Report of the Task Force on Financial Stability* 96, Brookings Inst.(June 2021), *available at* https://www.brookings.edu/wp-content/uploads/2021/06/financial-stability_report.pdf ("In short, the systemic consequences from a failure of a major CCP, or worse, multiple CCPs, would be severe. Pervasive reforms of derivatives markets following 2008 are, in effect, unfinished business; the systemic risk of CCPs has been exacerbated and left unaddressed."); Froukelien Wendt, *Central Counterparties: Addressing their Too Important to Fail Nature* (IMF Working Paper No. 15/21, Jan. 2015), *available at* https://www.imf.org/external/pubs/ft/wp/2015/wp1521.pdf (assessing the potential channels for contagion arising from CCP interconnectedness); Manmohan Singh, *Making OTC Derivatives Safe—A Fresh Look* (IMF Working Paper No. 11/66, Mar. 2011), at 5-11, *available at* https://www.imf.org/external/pubs/ft/wp/2011/wp1166.pdf (retrieved from SSRN Elsevier database) (addressing factors that could lead central counterparties to be "risk nodes" that may threaten systemic disruption).

720 The two exempt clearing agencies may also be subject to the EU Regulation, the Digital Operational Resilience Act (DORA), which went into effect in 2015: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595.

Commission is proposing to amend portions of Rule 1001(a), which will affect existing SCI entities as well. We discuss the benefits and costs of applying existing provisions to new SCI entities, as well as the benefits and costs of the amendments for both new and existing entities, below. We also discuss below the economic effects of these changes specific to the new SCI entities.

**i. Benefits**

*1) Provisions Applicable Only to New SCI Entities*

Rule 1001 requires certain policies and procedures for SCI entities. We consider here the provisions under Rule 1001 that we are not amending and therefore will only have an impact on SCI entities, relative to the baseline. We separately consider the provisions that we propose to amend in the following section, for both new and existing SCI entities.

*(i) Capacity, Integrity, Resiliency, Availability, and Security (Rule 1001(a)(1), (a)(2)(i) through (iv), (vi), and (vii))*

Rule 1001(a)(1) requires that each SCI entity 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)(i) through (iv), (vi), and (vii) prescribe certain minimum requirements for an SCI entity's policies and procedures. The Commission is not amending paragraphs (a)(1) and (a)(2)(i) through (iv), (vi), or (vii), and therefore current SCI entities will not be

affected whereas new SCI entities will become subject to these provisions for the first time.

Generally, the requirements to establish policies and procedures in Rule 1001(a)(1) should help ensure more robust systems that help reduce the risk and incidence of systems issues affecting the markets by imposing requirements on new entities that are not currently subject to Regulation SCI and by covering systems and events that are not currently within the scope of existing regulations and current practices.[721] In addition, the required policies and procedures may help new SCI entities recover more quickly from SCI events that do occur.

Application of Rule 1001(a)(2)(i) through (iv), (vi), and (vii) to the new SCI entities is expected to benefit securities markets and market participants by leading to the establishment, maintenance, and enforcement of policies and procedures for these entities related to current and future capacity planning; periodic stress testing; systems development and testing methodology; and reviews and testing to identify vulnerabilities; standards for market data collection, processing, and dissemination; and monitoring to identify potential systems problems. These requirements should reduce the risk and incidence of systems issues, such as systems disruptions and systems intrusions. This, in turn, could reduce interruptions in the price discovery process and liquidity flows. Systems issues that directly inhibit execution facilities, order matching, and dissemination of market data could cause slow executions or delayed orders, or cause inoperability of an SCI entity for a period of time. If executions were delayed by a

---

[721] The potential adverse effects of systems failures are described in section V.C.2. for each type of new SCI entity. Benefits to new SCI entities from a reduction in the risk and incidents of systems issues would arise from a reduction in these adverse effects.

systems disruption in an SCI system related to a trading, order routing, clearance and settlement, or market data system, given the magnitude of the transaction activity in which SCI entities consistently engage, the delay could have cascading effects disruptive to the broader market.[722]

In addition, Rule 1001(a)(2)(vi) provides that an SCI entity's policies and procedures must include standards that result in systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data. Rule 1001(a)(2)(vi) is expected to help ensure that timely and accurate market data are made available by new SCI entities. Market participants rely on market data in a variety of ways, including for making markets, formulating trading algorithms, and placing orders, among others. Although new SCI entities currently facilitate the successful collection, processing, and dissemination of market data, improvements in timeliness and accuracy of the generation of market data inputs would help further ensure pricing efficiencies and uninterrupted liquidity flows in markets.

Similarly, by requiring policies and procedures for monitoring systems to identify potential SCI events, Rule 1001(a)(2)(vii) may help ensure that new SCI entities identify potential SCI events, which could allow them to prevent some SCI events from occurring or to take timely appropriate corrective action after the occurrence of SCI events. As discussed above, reducing the frequency and duration of SCI events or reducing the duration of SCI events that disrupt markets would reduce pricing inefficiencies and promote price discovery and liquidity.

---

[722] *See supra* note 197.

In general, setting forth policies and procedures with regard to capacity planning, stress testing, systems development and testing methodology, and reviews and testing to identify vulnerabilities could yield benefits to market participants and new SCI entities, including a potential reduction in the likelihood, duration, or severity of SCI events, thus helping to contain losses from these events, as described above.[723] Capacity planning and stress testing are necessary to help an SCI entity determine its systems' ability to process transactions in an accurate, timely, and efficient manner, and thereby help ensure market integrity. Development and testing systems are important in ensuring the reliability and resiliency of SCI systems. The potential adverse effects of systems failures are described in section V.C.2. for each type of new SCI entity. More reliable and resilient systems should help reduce the occurrence of SCI events and improve systems uptime for the new SCI entities, and thus possibly result in a reduction in losses due to SCI events and a reduction in these adverse effects. Furthermore, the use of inadequately tested software in production could result in substantial losses to market participants if it does not function as intended. For instance, if software malfunctions, it might not execute or route orders as intended and also could have unintended effects on quoted prices and the actual prices at which orders execute. Additionally, if a system's capacity thresholds are improperly estimated, it may become congested, resulting in higher indirect transaction costs due to lower execution quality (*e.g.*, decrease in order fill rates).

The Commission recognizes that the new SCI entities are subject to existing policies and procedures obligations as discussed in the baseline. Pursuant to those obligations, the new SCI entities may already engage in practices that are similar to

---

723 *See* section V.D.1.

certain requirements under Regulation SCI. To the extent that the existing policies and procedures are similar to those reflected in Regulation SCI, the magnitude of the costs and benefits discussed above that stem from the application of those policies and procedures will be correspondingly reduced. However, costs and benefits that arise from obligations under Regulation SCI that differ from those existing obligations, such as reporting to the Commission will be maintained.

While some of the existing regulations that apply to the proposed new SCI entities may be consistent with or similar to the policy and procedure requirements of Regulation SCI discussed in this section, the Commission believes it is nevertheless appropriate to apply these policy and procedure requirements to the new SCI entities and doing so would benefit participants in the securities markets in which these entities operate. Applying Regulation SCI to these entities increases market protections by establishing these obligations under the Exchange Act so that the Commission may enforce them directly and examine for compliance and provides a uniform mandatory requirement that will ensure their continued application.

In addition, some new SCI entities may already be voluntarily implementing policies and procedures consistent with the requirements of Regulation SCI. The magnitude of the benefits (and associated costs, as discussed below) from the policy and procedure requirements in Rule 1001(a)(1) and (a)(2)(i) through (iv), (vi), and (vii) for the new SCI entities (and the costs, as discussed below), will therefore depend on the extent to which their current operations already align with the rule's requirements, given both existing regulation and current practice. However, the Commission believes the application of Regulation SCI is still necessary. For example, while SBSDRs that also

function as SDRs in the swap markets, may currently apply the CFTC rules to their securities-based swap markets as well as their swaps markets, the CFTC rules only apply to their swap market SDR systems. Therefore, applying Regulation SCI to SBSDRs would help to ensure that the systems relevant to the securities markets are subject to a requirement to 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 are subject to enhanced Commission oversight.

Additionally, with respect to SBSDRs, the requirements of Regulation SCI are more specific and comprehensive than the principles-based requirements of Rule 13n-6. The requirements of Regulation SCI would thus exist and operate in conjunction with Rule 13n-6, helping ensure that SBSDR market systems are robust, resilient, and secure and enhancing Commission oversight of the these systems.

Similarly, application of Regulation SCI to broker-dealers would complement existing requirements and enhance the policies and procedures already in place for these entities. For example, the Market Access Rule prescribes specific controls and procedures around a broker-dealer entering orders on an exchange or ATS, but the policy and procedure requirements of Regulation SCI are broader in scope and are designed to ensure that the key technology pervasive and important to the functioning of the U.S. securities markets is robust, resilient, and secure. Further, the SCI review requirement obligates an SCI entity to assess the risks of its systems and effectiveness of its technology controls at least annually, identify weaknesses, and ensure compliance with the safeguards of Regulation SCI. In addition, with respect to the requirements concerning the collection, processing, and dissemination of market data, Regulation SCI

extends beyond existing requirements to include SCI systems directly supporting proprietary market data, which will provide additional benefits to market participants. Further while Rule 17a-3 has a notification requirement when a broker-dealer fails to make and keep current the records required by that Rule, Regulation SCI more directly addresses mitigating the impact of technology failures with respect to SCI systems and indirect SCI systems (which include systems that are not used to make and keep current the records required by Rule 17a-3) and requires notifications to the Commission for a different set of events—systems intrusions, systems compliance issues, and systems disruptions—than the notification requirements of 17 CFR 240.17a-11 ("Rule 17a-11").

Likewise, while FINRA Rule 4370 requires broker-dealers to maintain business contingency and disaster recovery plans, it does not include the requirement that the business continuity and disaster recovery plans be reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption, nor does it require the functional and performance testing and coordination of industry or sector-testing of such plans, which are instrumental in achieving the goals of Regulation SCI with respect to SCI entities.

Finally, with respect to the exempt clearing agencies not subject to ARP, subjecting these entities to the policy and procedure requirements of Regulation SCI will ensure that uniform, minimum requirements regarding capacity, integrity, resiliency, availability, and security applies to all exempt clearing agencies. Although some of the conditions underlying the exemptive orders for the two exempt clearing agencies that would be subject to Regulation SCI under the proposed amendments may be consistent with Regulation SCI's policy and procedure requirements, the conditions vary across the

agencies and in their similarity to the Regulation SCI requirements. As these exempt clearly agencies and other entities that they interact with become more technologically innovative and interconnected, applying a uniform, minimum set of requirements will improve the Commission's oversight and better ensure the resiliency of the markets in which they operate.

Overall, applying the specific and comprehensive requirements set forth in Rule (a)(2)(i) through (iv), (vi), and (vii) of Regulation SCI to the new SCI entities would create a uniform, mandatory framework under the Commission's oversight thereby furthering the goals of Regulation SCI to strengthen the technology infrastructure of the U.S. securities markets and improve its resilience.

*(ii) Systems Compliance (Rule 1001(b))*

Rule 1001(b)(1) requires each SCI entity to establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Exchange Act and the rules and regulations thereunder, and the entity's rules and governing documents, as applicable. Rule 1001(b)(2)(i) through (iv) provides that an SCI entity's policies and procedures under Rule 1001(b)(1) must include, at a minimum: (i) testing of all SCI systems and any changes to SCI systems prior to implementation; (ii) a system of internal controls over changes to SCI systems; (iii) a plan for assessments of the functionality of SCI systems designed to detect systems compliance issues, including by responsible SCI personnel and by personnel familiar with applicable provisions of the Exchange Act and the rules and regulations thereunder and the SCI entity's rules and governing documents; and (iv) a plan of coordination and communication between regulatory and other personnel of the

SCI entity, including by responsible SCI personnel, regarding SCI systems design, changes, testing, and controls designed to detect and prevent systems compliance issues.

These provisions remain unchanged and do not create any new requirement for current SCI entities. New SCI entities, however, would become subject to these provisions for the first time. The Commission recognizes that new SCI entities currently take various measures to ensure that their systems operate in a manner that complies with relevant laws and rules. The specific requirements of Rule 1001(b) will further ensure that new SCI entities operate their SCI systems in compliance with the Exchange Act and relevant rules. For example, the tests under Rule 1001(b)(2)(i) should help new SCI entities to identify potential compliance issues before new systems or systems changes are implemented; the internal controls under 17 CFR 242.1001(b)(2)(ii) ("Rule 1001(b)(2)(ii)") should help to ensure that new SCI entities remain vigilant against compliance challenges when changing their systems and resolve potential noncompliance before the changes are implemented; and the systems assessment plans under 17 CFR 242.1001(b)(2)(iii) ("Rule 1001(b)(2)(iii)") and the coordination and communication plans under Rule 1001(b)(2)(iv) should help technology, regulatory, and other relevant personnel of new SCI entities to work together to prevent compliance issues, and to promptly identify and address compliance issues if they occur.[724] To the extent that new SCI entities operate market regulation and market surveillance systems, and to the extent

---

[724] *See* SCI Adopting Release, at 72422.

that compliance with Rule 1001(b) reduces the occurrence of systems compliance issues, Rule 1001(b) should advance investor protection.[725]

*(iii) Responsible SCI Personnel (17 CFR 242.1001(c)(1) ("Rule 1001(c)(1)"))*

Rule 1001(c)(1) requires an SCI entity to establish, maintain, and enforce reasonably designed written policies and procedures that include the criteria for identifying responsible SCI personnel, the designation and documentation of responsible SCI personnel, and escalation procedures to quickly inform responsible SCI personnel of potential SCI events. This provision remains unchanged and does not create any new requirement for current SCI entities. New SCI entities, however, will become subject to this provision for the first time.

Requiring policies and procedures to identify and designate responsible SCI personnel and to establish escalation procedures to quickly inform such personnel of potential SCI events should help to effectively determine whether an SCI event occurred and what appropriate actions should be taken without unnecessary delay. As such, Rule 1001(c)(1) is expected to reduce the duration of SCI events as new SCI entities become aware of them and take appropriate corrective actions more quickly. The reduction in the duration of SCI events would benefit markets and their participants as it would promote pricing efficiency and price discovery.

---

[725] *See id.* at 72410 and 72422; *see also* section III.A.2.b.ii (policies and procedures, including those for system compliance, are expected to strengthen broker-dealers' operational capabilities independent of any specific SCI event affecting their technology supporting trading, clearance and settlement, order routing, market data, market regulation, and market surveillance).

The Commission recognizes that the new SCI entities currently have certain regulatory obligations that may align with certain requirements of Rule 1001(c)(1), as described in the baseline, and in addition the new SCI entities may already be voluntarily implementing policies and procedures that may align with certain requirements of Rule 1001(c)(1). For example, SBSDRs and exempt clearing agencies may have policies and procedures that identify roles and responsibilities for key personnel as well as appropriate escalation procedures including designation and documentation of responsible personnel as noted above.[726] Likewise, as discussed above,[727] broker-dealers may have policies and procedures for designating employees with specific roles and responsibilities and escalation procedures documented in their incident response plans. As discussed above, the extent of these benefits (and related costs, as discussed below) would depend in part on how closely the existing policies and procedures of the new SCI entities align with the specific requirements of Rule 1000(c)(1).

*(iv) Periodic Reviews of Policies and Procedures and Prompt Remedial Actions (Rule 1001(a)(3), (b)(3), (c)(2))*

Rule 1001(a)(3), (b)(3), and (c)(2) require each SCI entity to periodically review the effectiveness of the policies and procedures required under Rule 1001(a) through (c) related to capacity, integrity, resiliency, availability, and security; systems compliance; and responsible SCI personnel, respectively, and to take prompt action to remedy deficiencies in such policies and procedures. These provisions remain unchanged since

---

726 *See* sec. V.B.1.a.ii and V.B.1.c.ii.

727 *See* section V.B.1.b.ii.

the adoption of Regulation SCI in 2014, but new SCI entities will become subject to them for the first time.

Requiring periodic review of the policies and procedures and remedial actions to address any deficiencies in the policies and procedures would help to ensure that new SCI entities maintain robust policies and procedures and update them when necessary so that the benefits of Rule 1001(a) through (c) as discussed in section V.C.1 should continue to be realized. For example, Rule 1001(a)(3), (b)(3), and (c)(2) should help to decrease the number of trading interruptions due to system issues in new SCI entities. It should lead to fewer interruptions in the price discovery process[728] and liquidity flows, thus, may result in fewer periods with pricing inefficiencies. Further, because interruptions in liquidity flows and the price discovery process in one security can affect securities trading in other markets, reducing trading interruptions could have broad effects.

As with the other requirements of Regulation SCI previously discussed, the Commission acknowledges that the new SCI entities are subject to existing regulations, and the extent of the benefits (and costs, as discussed below) will depend on how closely their current policies and procedures align with the requirements for review and remedial action under Rule 1001(a)(3), (b)(3), and (c)(2). The SBSDRs registered with the Commission are registered with the CFTC as swap data repositories (SDRs) and, with respect to systems of concern to the CFTC, are subject to CFTC's rules that require these entities to conduct periodic reviews of automated systems and business continuity-

---

[728] The price discovery process involves trading—buyers and sellers arriving at a transaction price for a specific asset at a given time. Thus, generally, any trading interruptions would interfere with the price discovery process.

disaster recovery capabilities.[729] While such entities may apply the CFTC rules to the entirety of their repositories, the CFTC rules do not apply to the SBSDR and its security-based swap related systems. Therefore, applying Rule 1001(a)(3), (b)(3), and (c)(2) to SBSDRs would ensure periodic reviews of the effectiveness of policies and procedures specifically related to SCI systems and create a uniform, mandatory framework under the Commission's oversight.

Similarly, SCI broker-dealers also are required under FINRA Rule 4370 to conduct an annual review of the business continuity and disaster recovery plans.[730] Further, as noted above, the two exempt clearing agencies are required to report at least on an annual basis to the competent authority regarding their compliance with CSDR, including on their operational risk management framework and systems and their information security framework.[731] The exempt clearing agencies must also periodically test and review the operational arrangements and policies and procedures with users. Additionally, the exemptive order for one of the exempted clearing agencies requires a review of policies and procedures and reporting on the status of policies and procedures to the Commission. To the extent that that the broker-dealers and the exempt clearing agencies increase the scope of the review of their policies and procedures related to capacity, integrity, resiliency, availability, and security; systems compliance; and responsible SCI personnel, and take prompt action to remedy deficiencies, the exempt clearing agencies, broker-dealers and their customers will benefit from application of

---

729 *See* 17 CFR 49.24(j); 17 CFR 49.24(m); 17 CFR 49.24(b)(3).

730 *See* sec. V.B.1.b.ii.

731 *See* sec. V.B.1.c.ii.

Rule 1001(a)(3), (b)(3), and (c)(2) and create a uniform, mandatory framework under the Commission's oversight.

*2) Amended Provisions Applicable to Current and New SCI entities*

The Commission is proposing to amend Rule 1001(a)(2)(v) – to add to that provision a requirement that business continuity and disaster recovery plans be reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity without which there would be a material impact on any of its critical SCI systems – and add several new provisions in Rule 1001(a)(2), including proposed Rule 1001(a)(2)(viii) (systems classifications and lifecycle management programs); proposed Rule 1001(a)(2)(ix) (third-party provider management program); proposed Rule 1001(a)(2)(x) (a program to prevent the unauthorized access to such systems and information residing therein); and proposed Rule 1001(a)(2)(xi) (identification of the relevant current industry standard claimed as a safe harbor, if any). In addition, we are proposing to amend Rule 1001(a)(4) to clarify that policies and procedures that are consistent with current SCI industry standards provide a safe harbor with respect to the requirement that such policies and procedures be reasonably designed. These amendments would impact both new and existing SCI entities.

*(i) Business Continuity and Disaster Recovery Plans (Rule 1001(a)(2)(v))*

Rule 1001(a)(2)(v) currently requires SCI entities' policies and procedures to set forth 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. The Commission is proposing to also require that such plans are reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity, without which there would be a material impact on any of its critical SCI systems.

With respect to the existing requirements that will remain unchanged, these would only affect new SCI entities and not create any new requirement for current SCI entities. Requiring business continuity and disaster recovery plans increases the likelihood that the markets in which they participate will continue to function, and SCI systems can resume operation in a timely manner, even when there are significant outages to SCI systems. Rule 1001(a)(2)(v), among other things, is expected to help ensure prompt resumption of all critical SCI systems, which in turn is expected to help minimize interruptions in trading and clearance and settlement after a wide-scale disruption. Notably, in the case of a wide-scale disruption, multiple SCI entities may be affected by the same incident at the same time. Given that U.S. securities market infrastructure is concentrated in relatively few areas, such as New York City, New Jersey, and Chicago, maintaining backup and recovery capabilities that are geographically diverse could facilitate resumption in trading and critical SCI systems following wide-scale market disruptions.[732] Reducing the frequency and duration of trading interruptions would promote pricing efficiency, price discovery, and liquidity flows in markets.

---

[732] As discussed in section III.C.2, the geographic diversity of data center sites is an important consideration even where an SCI entity uses CSPs as its business continuity and disaster recovery service providers.

With respect to the new requirement on the unavailability of third-party providers, both new and current SCI entities will be affected. Financial institutions, including SCI entities, have become increasingly dependent on third parties—such as cloud service providers—to operate their businesses and provide their services.[733] The proposed requirement for business continuity and disaster recovery plans to address the unavailability of any third-party provider would help ensure that SCI entities are appropriately prepared for contingencies relating to a third-party provider with respect to critical SCI systems., including the potential for an extended outage, if, for example the third-party provider goes into bankruptcy or dissolves, or if it breaches its contract and decides to suddenly, unilaterally, and/or permanently cease to provide the SCI entity's critical SCI systems with functionality, support, or service.

The Commission understands that some new SCI entities are already subject to similar requirements and may already have policies and procedures that may align with Rule 1001(a)(2)(v),[734] while others may need to make more significant changes to their current policies, procedures and practices. As discussed above, the extent of the benefits (and costs, as discussed below) will depend on how closely the new SCI entities' current policies and procedures align with the requirements of 1001(a)(2)(v), including the proposed amendment. With respect to SBSDRs, which are also registered as SDRs with the CFTC, the CFTC's System Safeguard rule sets forth requirements for swap data repositories to establish and maintain emergency procedures, geographically diverse[735]

---

733 *See supra* sec. V.B.4. and note 687.

734 *See* sections III.A.2.a.ii, III.A.2.b.ii, III.A.2.c.i., V.B.1.a.ii, V.B.1.b.ii, and V.B.1.c.ii.

735 SDRs deemed critical by the CFTC require geographically diverse backup facilities and staff.

backup facilities, and a business continuity-disaster recovery plan that allows for the timely recovery and resumption of next day operations following the disruption. While such entities may apply the CFTC rules to the entirety of their repositories, the CFTC rules do not apply to the SBSDR and its security-based swap related systems. Therefore, Rule 1001(a)(2)(v) would help ensure SBSDR's have in place for their SCI systems business continuity and disaster recovery plans that meet the minimum requirements set forth in the rule and create a uniform, mandatory framework under the Commission's oversight. The proposed amendment would ensure that these plans specifically address the unavailability of any third-party provider that provides functionality, support, or service to the SBSDR's SCI systems, without which there would be a material impact on any of its critical SCI systems.

SCI broker-dealers are likewise required to create and maintain a written business continuity plan under FINRA Rule 4370.[736] Currently required business continuity public disclosure statements[737] generally indicate that some backup systems are geographically diverse, but limited information is disclosed with respect to a specific timeline for resumption of service in the event of a disruption. Similarly, these required business continuity public disclosure statements generally do not provide information on specific BC/DR plans to address the unavailability of any third-party provider, as would be required under the proposed amendment. Applying the requirements of Rule 100(a)(2)(v) to broker-dealers may reduce the frequency and duration of trading interruptions, which

---

736 *See* section V.B.1.b.ii.

737 While broker-dealers are required to provide a brief summary disclosure statement regarding their BCPs to customers, they do not disclose the actual BCP. Based on a review of 2021 and 2022 BCP disclosure statements, firms often do not provide any detail on operational capacity to meet demand surges or any specific timeframes for resumption of service.

would promote pricing efficiency, price discovery, and liquidity flows in markets. Further, the proposed amendment to Rule 1001(a)(2)(v) would help ensure broker-dealers have business continuity and disaster recovery plans in place to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI systems.

Finally, as discussed above, the exempt clearing agencies are currently required to maintain a business continuity policy and disaster recovery plan that ensures two hour resumption of critical operations and geographically diverse backup systems and monitor and test it at least annually.[738] The exempt clearing agencies are also required to address the unavailability of any critical third-party provider.[739] Application of Rule 1000(a)(2)(v), including the proposed amendment, would help ensure exempt clearing agencies have business continuity and disaster recovery plans in place to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI systems and thus would likely incrementally reduce the frequency and duration of trading interruptions and promote pricing efficiency, price discovery, and liquidity flows in markets.

*(ii) Systems Classification and Lifecycle Management (Proposed Rule 1001(a)(2)(viii))*

Proposed Rule 1001(a)(2)(viii) provides that an SCI entity's policies and procedures must provide for the maintenance of a written inventory and classification of

---

738 *See* sec. V.b.1.e.ii.

739 *Id.*

all SCI systems, critical SCI systems, and indirect SCI systems as such, and a program with respect to the lifecycle management of such systems, including the acquisition, integration, support, refresh, and disposal of such systems, as applicable. This is a new provision and applies to both current SCI entities and new SCI entities.

A foundational and essential step for an SCI entity to be able to meet its obligations under Regulation SCI is to be able to clearly identify the different types of its systems that are subject to differing obligations under Regulation SCI. Reasonably designed systems classification and lifecycle management policies and procedures, which include vulnerability and patch management, reduce the risk of SCI system defects and operational issues. The systems classification requirement would promote more efficient and timely compliance with the remaining provisions of Regulation SCI. The lifecycle management requirement would also ensure that sensitive information (including software configuration info, middleware, etc.) is not inadvertently revealed, potentially compromising the security of an SCI entity's data and network—and would further enhance the systems' integrity, resiliency, and security. The Commission understands that one of the first steps many current SCI entities would take to comply with Regulation SCI is to develop a classification of their systems in accordance with the definitions of each type of system in SCI, but not all SCI entities maintain such a list. Accordingly, the extent of the benefits described above will depend on whether existing entities have taken such steps and how closely they align with the proposed requirements.

With respect to new SCI entities, broker-dealers are required to maintain policies and procedures per Regulation S-P and S-ID, as discussed above.[740] In two Commission

---

740 *See* sec. V.B.1.b.ii.

exam sweeps, the Commission staff observed that most broker-dealers already inventory, catalog, and classify the risks of their systems and had a process in place for ensuring regular system maintenance, including the installation of software patches to address security vulnerabilities.[741] Furthermore, identification of mission critical systems is required by FINRA rule 4370. Accordingly, there would be an incremental benefit (and cost) from applying this particular provision of Regulation SCI to the broker-dealers. Additionally, the practice of inventorying and classifying systems might also encourage the firm to invest in supplemental security measures to reduce the number of indirect SCI systems, which would result in an incremental and upfront or short-term cost.

As discussed in section V.B.1.c.ii, exempt clearing agencies are required by CSDR to prepare a list with all the processes and activities that contribute to the delivery of the services they provide; and identify and create an inventory of all the components of their IT systems that support the processes and activities. This likely would represent an incremental benefit (and cost). Additionally, the practice of inventorying and classifying systems might also encourage the firm to invest in supplemental security measures to reduce the number of indirect SCI systems to reduce the long-time compliance burden which would result in an incremental and upfront or short-term cost.

*(iii) Third-Party Provider Management (Proposed Rule 1001(a)(2)(ix))*

Proposed Rule 1001(a)(2)(ix) concerns policies and procedures for effective third-party provider management and would newly apply to both existing and new SCI entities. As discussed above, financial institutions have been increasingly outsourcing parts of

---

741 *Id*.

their services.[742] When a market participant chooses to outsource a particular component of its operation to a third-party vendor, the vendor may offer components of services (of certain quality) at a cheaper rate than the market participant can supply on its own or where the market participant may lack the expertise or ability to provide them. If this is done properly and with full information, it can result in an efficient outcome without compromising the service quality below what is required under Regulation SCI.

But in some cases, if there is information asymmetry—especially with respect to service quality—market dynamics among SCI entities result on the provision of sub-optimal services. This may be the case for a number of reasons, including imperfect communication between the SCI entity and its third-party provider. First, a third-party provider providing its service to an SCI entity may lack the knowledge of the level of resiliency and capacity the SCI entity must maintain. Second, an SCI entity may lack the knowledge of the robustness of the third-party provider's operation. Third, the market for these services may not be competitive, and an SCI entity looking to outsource these services may not have other comparable choices. Failure to ensure that policies and procedures are adequate to reduce these risks may result in unidentified security weaknesses, the inability to analyze potential security events, and delayed business continuity and disaster recovery.

Proposed Rule 1001(a)(2)(ix) would require each SCI entity to have a program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for its SCI systems and, for purposes of security standards, its indirect SCI systems. Each SCI entity would be required to undertake a risk-based

---

[742] *See supra* sec. V.B.4. and note 687.

assessment of each third-party provider's criticality to the SCI entity, including analyses of third-party provider concentration, of key dependencies if the third-party provider's functionality, support, or service were to become unavailable or materially impaired, and of any potential security, including cybersecurity, risks posed. The Commission believes that specifically requiring each SCI entity to undertake a risk-based assessment of each of its third-party providers' criticality to the SCI entity will help it more fully understand the risks and vulnerabilities of utilizing each third-party provider, and provide the opportunity for the SCI entity to better prepare in advance for contingencies should the provider's functionality, support, or service become unavailable or materially impaired.

Again, the extent of these benefits may depend on whether an SCI entities' existing practices, and applicable regulations, are consistent with the requirements of proposed Rule 1001(a)(2)(ix). As noted above, SBSDRS that are dually registered as SDRs with the CFTC are also subject to the CFTC System Safeguards rule, which requires a SDR to undertake program of risk analysis and oversight of outsourcing and vendor management affecting its operations and automated systems.[743] A dual-registered entity's outsourced systems for processing SDR data might also be SCI systems if such systems also process SBSDR data. Accordingly, an SDR's adherence to the System Safeguard Rule's provision for vendor management and outsourcing is reasonably likely to reduce the benefit (and the cost, as discussed below) of complying with proposed Rule 1001(a)(2)(ix).

Similarly, as discussed above, broker-dealers are already subject to general vendor management obligations in accordance with FINRA Rule 3110 and obligations

---

[743] 17 CFR 49.24(b)(6).

under Regulation S-P[744]and thus some of their current practices may be consistent with some of the requirements of Rule 1001(a)(ix). However, those rules are different in scope and purpose than the proposed amendment to Regulation SCI.[745] For example, while FINRA rules already require initial and ongoing due diligence, third-party provider contract review and ongoing third-party risk assessment, proposed Rule 1001(a)(2)(ix) also requires an additional risk-based assessment of each third-party provider's criticality to the SCI entity. Accordingly, proposed Rule 1001(a)(2)(ix) may restrict usage of particular third-party providers, if and when they are unwilling or unable to comply with Regulation SCI's third-party provider requirements.

Finally, as discussed in V.B.1.c.ii, the two exempt clearing agencies are required by CSDR to have arrangements for the selection and substitution of IT third-party service providers and proper controls and monitoring tools which seems within the scope of proposed Rule 1001(a)(2)(ix) initial and ongoing due diligence provisions. The exempt clearing agencies are also required to identify critical utilities providers and critical service providers that may pose risks to tier operations due to dependency on them which seems within the scope of ongoing third-party risk assessment. In light of the existing requirements for exempt clearing agencies discussed in the baseline, any benefits (and associated costs, as discussed below) from the proposed amendment are likely to be relatively small with respect to critical service providers. However, the benefit would likely be larger with respect to non-critical service providers where the requirements are less specific.

---

744 *See supra* sec. V.B.1.b.ii.

745 *See* sec. III.A.2.b.ii. and III.D.

*(iv) Security (Proposed Rule 1001(a)(2)(x))*

Since the adoption of Regulation SCI in 2014, the financial system has become more digitized and consequently cybersecurity has become a significant concern for financial firms, investors, and regulatory authorities.[746] In addition, the COVID-19 pandemic and accelerated move to working from home increased the demand for digital services and reliance of SCI entities on third-party providers including CSPs. Moving the majority of activities to the online or digitized environment has increased the risk of cybersecurity events.[747] According to the Bank for International Settlements, the financial sector had the second-largest share of COVID-19-related cybersecurity events between March and June 2020.[748] The Commission is proposing a new paragraph (a)(2)(x) of Rule 1001 that would require policies and procedures of SCI entities include a program to prevent the unauthorized access to SCI systems and, for purposes of security standards, indirect SCI systems and information residing therein. This would be a new provision and would apply to both current SCI entities and new SCI entities.

The Commission anticipates that the primary benefit of the proposed rule would be to ensure that all SCI entities, including the new SCI entities, have policies and procedures to enhance their preparedness against cybersecurity threats. The proposed requirements to develop policies and procedures that are specifically designed to prevent the unauthorized access to SCI systems and information residing therein, would better

---

746 *See supra* sec. III.C.3.

747 Iñaki Aldasoro et al., *COVID-19 and Cyber Risk in the Financial Sector*, BIS Bull. No. 37 (Jan. 14, 2021), *available at* https://www.bis.org/publ/bisbull37.pdf.

748 *Id*. The health sector is ranked first in term of the cyberattacks.

protect SCI entities against cybersecurity threats. Such policies and procedures can strengthen the security surrounding their information systems and the data contained within, aiding in the prevention of unauthorized access; minimizing the damage from cybersecurity events; and improving incident recovery time.

Another significant benefit is that any such unauthorized access should be reported to the Commission. Thus, this rule, together with the Commission notification requirement in Rule 1002(b), as amended, will help the Commission better understand which entities are most affected by cybersecurity events, what the current trends may be, and provide the Commission with information that may aid in subsequent guidance or rulemaking to further strengthen the affected entities from future cybersecurity events and disruptions to their business operations. Indeed, as we stated in section B.2.a, it is the Commission's understanding that current SCI entities have been reporting de minimis system intrusions on a quarterly basis, rather than immediately, as permitted under the current requirements of Regulation SCI. Current SCI entities are not required to report attempted intrusions.

The extent of these benefits will depend on how consistent the existing policies and procedures of both current and new SCI entities are with the requirements of proposed Rule 1001(a)(2)(x). The Commission believes that many existing SCI entities already have most or all of such policies and procedures in place as part of their security protocols; thus the benefits (and the associated costs) of applying the proposed Rule 1001(a)(2)(x) may be reduced.

Among new SCI entities, both registered SBSDRs have stated they have policies and procedures addressing access management.[749] To the extent that SBSDRs already have access management policies and procedures that are aligned with the requirements of proposed Rule 1001(a)(2)(x), the proposed rule would offer limited benefits. Further, as discussed in section V.B.1.b.ii, broker-dealers are required to maintain policies and procedures addressing security issues per Regulation S-P and S-ID, although those regulations and the required policies and procedures are different in scope and purpose. The extent of the benefits of proposed Rule 1001(a)(2)(x) would thus depend on how consistent the broker-dealer's current policies and procedures are with the requirements of the proposed Rule.

As discussed in section V.B.1.c.ii, the two exempt clearing agencies are required to maintain information security frameworks describing mechanisms to detect and prevent cyber-attacks and a plan in response to cyber-attacks. The information security framework includes among other requirements access controls to the system and adequate safeguards against intrusions and data misuse. Therefore, proposed Rule 1001(a)(2)(x) may offer only limited incremental benefits.[750]

---

749 17 CFR 49.24(b)(2). *See* Security-Based Swap Data Repositories; ICE Trade Vault, LLC; Notice of Filing of Application for Registration as a Security-Based Swap Data Repository, *available at* https://www.sec.gov/rules/other/2021/34-91331.pdf; Security-Based Swap Data Repositories; DTCC Data Repository (U.S.), LLC; Notice of Filing of Application for Registration as a Security-Based Swap Data Repository, *available at* https://www.sec.gov/rules/other/2021/34-91071.pdf.

750 *See* section V.B.1.c.ii.

*(v) Current SCI Industry Standards (Proposed Rule 1001(a)(2)(xi)) and Safe Harbor for Policies and Procedures Consistent with SCI Industry Standards (Rule 1001(a)(4))*

Proposed Rule 1001(a)(2)(xi) would provide that an SCI entity's policies and procedures must include an identification of the current SCI industry standard(s) with which each such policy and procedure is consistent, if any. This requirement would be applicable if the SCI entity is taking advantage of the safe harbor provision, Rule 1001(a)(4). We are also proposing to amend the text of Rule 1001(a)(4), which deems an SCI entity's policies and procedures under Rule 1001(a) to be reasonably designed if they are consistent with current SCI industry standards, to make clear that its reference to and definition of "current SCI industry standards" provides a safe harbor for SCI entities with respect to their Rule 1001(a) policies and procedures. Proposed Rule 1001(a)(2)(xi) and the amendment to Rule 1001(a)(4) would apply to both current SCI entities and new SCI entities.

Rule 1001(a)(4) specifically states that compliance with current SCI industry standards is not the exclusive means to comply with the requirements of Rule 1001(a). Therefore, Rule 1001(a)(4) provides flexibility to allow each SCI entity to determine how to best meet the requirements in Rule 1001(a), taking into account, for example, its nature, size, technology, business model, and other aspects of its business. SCI entities can choose the technology standards that best fit with their business, promoting efficiency. The ability of SCI entities to rely on widely recognized technology standards,

if they choose to do so, will provide guidance to SCI entities on policies and procedures that would meet the articulated standard of being "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."

In addition, the flexibility of this requirement leaves room for industry-wide innovation, while encouraging each SCI entity to conform to an industry standard that is most appropriate for itself given the entity's scope of operation and particular characteristics. These standards currently in place may require protocols that go beyond the level that would have been chosen by an entity that is driven by profit-maximizing or cost-saving motives. Furthermore, as industry standards continue to evolve, Regulation SCI helps to ensure that SCI entities are motivated to adhere to the changing standards that reflect the changes in market conditions and technology. The Commission understands that many existing SCI entities rely on industry standards, typically by adhering to a specific industry standard or combination of industry standards for a particular technology area or by using industry standards as guidance in designing policies and procedures. Thus, overall benefits and costs to existing SCI entities will be incremental, and the benefits and costs are likely to be greater for entities that do not already rely on industry standards and lesser for entities that already adhere closely to industry standards.

Among new entities, both SBSDR entities are also registered with the CFTC as SDRs, and as such are subject to the CFTC's System Safeguard rule in their capacity as SDRs. The System Safeguard rule requires SDRs to follow generally accepted standards

and best practices with respect to the development, operation, reliability, security, and capacity of automated systems.[751] While not required, it is likely that dual-registered SDRs/SBSDRs are following these requirements for SBSDRs given the CFTC requirements for SDRs. Therefore, it is likely that SBSDRs already have policies and procedures consistent with existing industry standards.

As discussed above, broker-dealers are required to have certain policies and procedures pursuant to Regulation S-P and S-ID.[752] The 2015 FINRA report on cybersecurity practices observed that broker-dealers reported relying on industry standards with respect to cybersecurity requirements, typically by adhering to a specific industry standard or combination of industry standards or by using industry standards as a reference point for designing policies and procedures.[753] To the extent that any broker-dealers do not rely on industry standards or only selectively, applying Rule 1001(a)(4) and proposed Rule 1001(a)(2)(xi) will likely increase broker-dealer adherence to industry standards and improve overall compliance with Rule 1001.

As discussed in section V.B.1.c.ii, the two exempt clearing agencies are required by CSDR to rely on internationally recognized technical standards and industry best practices with respect to its IT systems. As such, it is likely that they already have policies and procedures that are consistent with one or more industry standards. The proposed amendment may have some incremental benefit and improve overall compliance with Rule 1001.

---

751 *See* 17 CFR 49.24.

752 *See* sec. V.B.1.b.ii.

753 *See* section V.B.1.b.ii.

### ii. Costs

The policies and procedures requirements of Regulation SCI would impose certain compliance costs on new SCI entities, which are expected to change at least some of their current practices to comply. In addition, the proposed amendments to certain provisions in Rule 1001 would impose additional costs on new and existing SCI entities. We discuss these costs below.

#### *1) Compliance Costs for New SCI Entities*

Some of the new SCI entities are already subject to existing regulatory requirements that are similar to the requirements in Rule 1001, including the proposed amendments. To the extent these entities already have policies and procedures that are consistent with the Rule 1001 requirements, they could incur lower costs to comply with the requirements of Rule 1001 than entities without such existing policies and procedures. Similarly, the compliance costs associated with Rule 1001 may vary across SCI entities depending on the degree to which their current voluntary practices are already consistent with the requirements of Rule 1001.The compliance costs of Rule 1001 may further depend on the complexity of SCI entities' systems (*e.g.*, the compliance costs will be higher for SCI entities with more complex systems). They may also depend, to a large extent, on the scale as well as the relative criticality of a given SCI entity's systems. We discuss below the costs for new SCI entities to comply with Rule 1001, including the proposed amendments; this includes PRA costs as well as additional compliance costs.

First, with respect to PRA costs, the Commission estimates total initial costs of approximately $13.4 million and annual costs of approximately $3.5 million for all new

SCI entities.[754] In addition to the compliance costs estimated as part of the PRA analysis, the Commission acknowledges there may, in some cases, be other compliance costs. In the SCI Adopting Release, the Commission formed estimates of non-PRA compliance costs for complying with Rule 1001(a) and (b),[755] which are instructive for determining such costs now for the new SCI entities. The Commission believed then, and continues to do so now, that the costs of complying with Rule 1001(c) are fully captured in the PRA cost estimates. The Commission's estimates then were based on extensive discussions with industry participants as well as information contained in the comment letters submitted during the rulemaking process. After carefully considering all comments, the Commission concluded that to comply with all requirements underlying the policies and procedures required by Rule 1001(a) and (b), other than paperwork burdens, on average, each SCI entity will incur an initial cost of between approximately $320,000 and $2.4 million and an ongoing annual cost of between approximately $213,600 and $1.6 million.[756] Adjusted for inflation since 2014, the initial cost would be between

---

754 *See* section IV.D.7. These are the estimated costs to comply with Rule 1001(a) through (c). For purposes of this Economic Analysis, there are two fewer entities than under the PRA analysis, lowering these estimated costs. *See supra* note 700.

755 According to the 2014 adopting release, these non-PRA compliance costs include, for example, establishing current and future capacity planning estimates, capacity stress testing, reviewing and keeping current systems development and testing methodology, regular reviews and testing to detect vulnerabilities, testing of all SCI systems and changes to SCI systems prior to implementation, implementing a system of internal controls, implementing a plan for assessments of the functionality of SCI systems, implementing a plan of coordination and communication between regulatory and other personnel of the SCI entity, including by responsible SCI personnel, designed to detect and prevent systems compliance issues, and hiring additional staff. *See* SCI Adopting Release, *supra* note 1, at 72416 n. 1939.

756 *Id*.

approximately $407,000 and $3.1 million, and the ongoing annual cost would be between approximately $272,000 and $2.0 million.[757]

In the 2014 adopting release, the Commission acknowledged that its cost estimates reflect a high degree of uncertainty because the compliance costs may depend on the complexity of SCI entities' systems (*e.g.*, the compliance costs will be higher for SCI entities with more complex systems). The initial compliance costs associated with Rule 1001 could also vary across SCI entities depending on the degree of that their current practices are already consistent with the requirements of Rule 1001.[758] The Commission explained the difficulty of gauging the degree to which an SCI entity was already taking measures consistent with Regulation SCI, which would affect the compliance costs with respect to Rule 1001. These considerations continue to apply to the Commission's estimate of any non-PRA costs for new SCI entities, which span multiple markets and vary a great deal in terms of the services they provide and the operations they perform. These new SCI entities face different baselines depending on the applicable

---

757 SEC inflation calculations are based on annual GDP price index data from Table 1.1.4. in the National Income and Product Accounts from the Bureau of Economic Analysis, and on inflation projections from *The Budget and Economic Outlook: 2023 to 2033*, published by the Congressional Budget Office in February 2023.

758 These estimates in the SCI Adopting Release were in turn based on the preliminary estimates included in the SCI Proposing Release, *supra* note 14, at 18171. However, one important assumption the SCI Proposing Release made was to assume that certain SCI entities "already [had or had] begun implementation of business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse to ensure next business day resumption of trading and two-hour resumption of clearance and settlement services following a wide-scale disruption." *Id.* at note 633. In the SCI Adopting Release, however, in order to accommodate the cost considerations of those SCI entities that did not already have geographically diverse backup facilities, the Commission estimated the average cost to be approximately $1.5 million annually for such SCI entities. *See* SCI Adopting Release, *supra* note 1, at 72420. In the section discussing Rule 1001(a)(2)(v) below, the Commission estimates the comparable estimate to be between $1.5 million and $1.8 million. This additional estimate range only applies to SCI entities that do not already have geographically diverse backup facilities and would be in addition to the non-paperwork burden estimates discussed in the current section.

regulatory requirements that they are subject to and the market practices each SCI entity has been following.

Given these considerations, the Commission believes that the estimates from 2014 are still appropriate estimates for the non-PRA costs associated with Rule 1001(a) and (b) of Regulation SCI without the proposed amendments for the new SCI entities. There are reasons to believe that these ranges should be increased for inflation[759] and technological changes since 2014, such as greater interconnectivity, that have expanded the scope for testing, leading to greater costs. However, there are also reasons to believe that as of 2023 these ranges may have come down.

First, some components of costs may be lower in 2023 because of technological improvements since 2014.[760] Second, the experience of the current 47 SCI entities complying with Regulation SCI since 2014 has likely generated a useful industry knowledge base for new SCI entities, including common practices, industry standards, and cost-saving measures. From this perspective, the cost of learning would be lower,

---

759 For example, GDP Price Index data from the Bureau of Economic Analysis (BEA) and projections from the Congressional Budget Office show that, economy-wide, prices increased by about 27% from 2014 to 2023.

760 *See* Matt Rosoff, *Why is Tech Getting Cheaper?,* weforum.org (Oct. 16, 2015), *available at* https://www.weforum.org/agenda/2015/10/why-is-tech-getting-cheaper/. For example, price has been dropping for cloud computing services over the last years. *See* Jean Atelsek, et al., *Major Cloud Providers and Customers Face Cost and Pricing Headwinds*, spglobal.com (May 10, 2022), *available at* https://www.spglobal.com/marketintelligence/en/news-insights/research/major-cloud-providers-and-customers-face-cost-and-pricing-headwinds; *see also* David Friend, *The Coming Era of Simple, Fast, Incredibly Cheap Cloud Storage*, Cloudtweaks.com (Nov. 15, 2022, 9:12 a.m.), *available at* https://cloudtweaks.com/2018/02/fast-incredibly-cheap-cloud-storage/ (describing the significant price drop for cloud storage as of 2018, and explaining that "the prices for cloud storage are heading in the same direction."). These trends may be reversing. *See* Jean Atelsek, et al., ("Rising energy costs and supply chain woes threaten to push up costs for the cloud hyperscalers in building and operating their data centers; therefore, cloud infrastructure prices are poised to increase."); Frederic Lardinois, *Google Cloud Gets More Expensive*, TechCrunch+ (Mar. 14, 2022, 11:54 p.m.), *available at* https://techcrunch.com/2022/03/14/inflation-is-real-google-cloud-raises-its-storage-prices/.

including the start-up cost. Third, the Commission understands that many financial institutions that are not subject to Regulation SCI have voluntarily begun to conform to one or more industry standards and adopted written policies and procedures related to ensuring capacity, integrity, resiliency, availability, and security of their systems. Indeed, the Commission understands—based on the Commission's discussions with industry participants—that the changes in the market—including greater automation and interconnectivity and an overall need to expand the scope of testing—have already incentivized many SCI entities to improve their internal protocols and to increase their technology expenditures. For example, the growing risk of cybersecurity events has already led many corporate executives to significantly increase their cybersecurity budgets.[761] From this perspective, although the overall security and IT spending may have increased manifold for SCI entities over the years, the Commission estimates that the magnitude of compliance costs owing to the adoption of Regulation SCI for new SCI entities, over and above their current expenses, may not necessarily have increased significantly as a result since 2014.

Taking these varied considerations into account, the Commission estimates that, adjusted for inflation since 2014, the 2014 figures remain reasonable ranges for non-PRA costs associated with Rule 1001(a) and (b) in 2023, without accounting for the proposed amendments in Rule 1001(a). In other words, the Commission estimates that a new SCI entity in 2023 will incur an initial non-PRA cost of between approximately $407,000 and

---

[761] For example, according to one source, as of 2020, "55% of enterprise executives [were planning] to increase their cybersecurity budgets in 2021 and 51% are adding full-time cyber staff in 2021." Louis Columbus, *The Best Cybersecurity Predictions for 2021 Roundup*, Forbes.com (Dec. 15, 2020), *available at* https://www.forbes.com/sites/louiscolumbus/2020/12/15/the-best-cybersecurity-predictions-for-2021-roundup/?sh=6d6db8b65e8c.

$3.1 million and an ongoing annual non-PRA cost of between approximately $272,000 and $2.0 million to comply with the original provisions of Regulation SCI from 2014.

To account for the proposed amendments, the Commission preliminarily estimates that, based on staff experience with current SCI entities' compliance practices, the non-PRA cost of complying with the amended provisions could be up to approximately 20% of the estimated non-PRA cost for complying with the original (*i.e.*, unamended) Rule 1001(a). Accordingly, the Commission estimates that a new SCI entity would incur an additional initial cost of between approximately $81,000 and $611,000 and an additional ongoing annual cost of between approximately $54,000 and $407,000 to comply with the amended provisions of Rule 1001(a).[762] Combined with the non-PRA costs estimates above for complying with the rest of Rule 1001(a) and (b), a new SCI entity will incur an additional initial non-PRA cost of between approximately $489,000 and $3.7 million[763] and an additional ongoing annual non-PRA cost of between approximately $326,000 and $2.4 million, plus the PRA costs estimated above.[764] The Commission estimates that, in the aggregate, all new SCI entities will incur a total initial non-PRA cost of between approximately $10.3 million and $77.0 million to comply with the policies and procedures required by Rule 1001(a) and (b).[765] In addition, the

---

762 These figures are 20% of the range from the Regulation SCI Adopting Release, adjusted for inflation from 2014 to 2023.

763 These figures are 120% of the range from the Adopting Release of Regulation SCI, adjusted for inflation since 2014.

764 These figures are approximately 120% of the range from the Adopting Release of Regulation SCI, adjusted for inflation since 2014.

765 The Commission currently estimates there are 23 new SCI entities, two of which are excluded from the economic analysis as explained above. The range of $10.3 million and $77.0 million represents 21 times the per-entity initial cost range from the Regulation SCI Adopting Release, adjusted for inflation since 2014.

Commission estimates that, in the aggregate, new SCI entities will incur total annual ongoing non-PRA cost of between approximately $6.9 million and $51.3 million.[766] Depending on the price-sensitivity of their customers and the availability of alternative providers, new SCI entities may pass on some of these costs to their customers.[767]

In addition, with respect to the periodic reviews required by Rule 1001(a)(3), (b)(3), and (c)(2), there may be additional indirect costs if an SCI entity takes prompt or unplanned remedial action following the discovery of deficiencies in its policies and procedures. Specifically, the new SCI entities may need to delay or shift their resources away from profitable projects and reallocate their resources towards taking prompt or unplanned remedial actions required by the rules. It is nevertheless difficult to assess such indirect costs imposed on SCI entities because the Commission lacks information necessary to provide a reasonable estimate and such indirect costs will be circumstance-specific.

*2) Compliance Costs for Existing SCI Entities*

Existing SCI entities should incur new costs only to comply with the proposed amendments to Rule 1001(a). With respect to PRA costs, the Commission estimates total initial costs of approximately $8.2 million and annual costs of approximately $1.1 million

---

766 The range of $6.9 million and $51.3 million represents 21 times the per-entity ongoing annual cost range from the Regulation SCI Adopting Release, adjusted for inflation since 2014.

767 *See, e.g.,* Jonathan Baker, Orley Ashenfelter, David Ashmore & Signe-Mary McKernan, *Identifying the Firm-Specific Cost Pass-Through Rate*, Federal Trade Commission. Bureau of Economics 1 (1998), *available at* https://www.ftc.gov/sites/default/files/documents/reports/identifying-firm-specific-cost-pass-through-rate/wp217.pdf.

for all current SCI entities.[768] For non-PRA costs associated with these amendments, the Commission estimates that the non-PRA cost of complying with the amended provisions could be up to approximately 20% of the estimated non-PRA cost for complying with the original (*i.e.*, unamended) Rule 1001(a), as explained above. Accordingly, the Commission estimates that an existing SCI entity would incur an additional initial non-PRA cost of between approximately $81,000 and $611,000 and an additional ongoing annual non-PRA cost of between approximately $54,000 and $407,000 to comply with the amended provisions of Rule 1001(a).[769] The Commission in turn estimates that, in the aggregate, current SCI entities will incur a total initial non-PRA cost of between approximately $3.8 million and $28.7 million to comply with the policies and procedures required by Rule 1001(a) and (b).[770] In addition, the Commission estimates that, in the aggregate, current SCI entities will incur total annual ongoing non-PRA cost of between approximately $2.6 million and $19.1 million.[771]

*3) Other Costs for all SCI Entities and other Affected Parties*

Proposed Rule 1001(a)(2)(ix) could raise costs of third-party service providers insofar as they may have to renegotiate contracts and change the terms of their services to accommodate the requirements of SCI entities. SCI entities could also incur costs in

---

768 *See* section IV.D.7. These include costs for existing entities to comply only with Rule 1001(a), and for new entities to comply with Rule 1001(a) through (c).

769 These figures are 20% of the range from the Regulation SCI Adopting Release, adjusted for inflation since 2014.

770 The Commission currently estimates there are 47 current SCI entities. The range of $3.8 million and $28.7 million represents 47 times the per-entity cost range from the SCI Adopting Release, adjusted for inflation since 2014.

771 The range of $2.6 million and $19.1 million represents 47 times the per-entity cost range from the SCI Adopting Release, adjusted for inflation since 2014.

enforcing their third-party provider management program. In particular, to the extent that accommodating the terms and conditions that would be demanded by SCI entities under proposed Rule 1001(a)(2)(ix) would be costly to third-party service providers, SCI entities could face higher prices from third-party providers, though any change in prices would also depend upon market conditions (such as the level of competition amongst third-party service providers for the type of services sought after by the SCI entity, the relative bargaining power of the SCI entity in negotiations with third-party service providers, new entry into the market for third-party services, and willingness of service providers to absorb costs or pass costs to other customers).

**Request for Comment**

106. For current SCI entities, do you agree that the Commission's specified ranges reasonably capture the non-paperwork burden costs owing to Rule 1001(a) and (b) that you have incurred above and beyond amounts you were already spending to ensure your SCI systems' capacity, integrity, resiliency, availability, and security under the existing requirements of Regulation SCI?

107. For new SCI entities, do you agree that the Commission's specified ranges reasonably capture the non-paperwork burden costs owing to Rule 1001(a) and (b) that you expect to incur above and beyond the amounts you were already spending to ensure your SCI systems' capacity, integrity, resiliency, availability, and security under the existing requirements of Regulation SCI?

108. For current and new SCI entities, do you agree that the Commission's specified ranges for the non-paperwork cost of complying with the proposed amendments to Rule 1001(a) and (b), at 20 percent of the specified ranges for Rule 1001(a) and (b),

reasonably capture such costs that you expect to incur, above and beyond amounts you are already spending to ensure your SCI systems' capacity, integrity, resiliency, availability, and security owing to the proposed amendments?

109. If you are a current SCI entity and currently inventory and classification of all SCI systems, critical SCI systems, and indirect SCI systems, how does your activity differ from the requirements of the rule proposal? What have been the benefits and costs of this activity?

110. If you are a current SCI entity and have a program with respect to the lifecycle management of SCI systems, does it address the acquisition, integration, support, refresh, and disposal of such systems, as applicable? How does your activity differ from the requirements of the rule proposal? What have been the benefits and costs of this activity?

111. If you are a current SCI entity and you currently have a third-party provider management program to ensure that your SCI systems contractors perform their work in accordance with the requirements of Regulation SCI, how does your activity differ from the requirements of the rule proposal? What have been the benefits and costs of this activity?

112. If you are a current SCI entity and you currently require an initial and periodic review of contracts with service providers for consistency with your obligations under Regulation SCI, how does your activity differ from the requirements of the rule proposal? What have been the benefits and costs of this activity?

113. If you are a current or proposed SCI entity and you currently conduct a risk-based assessment of each third-party provider's criticality, to your operations, how does

your activity differ from the requirements of the rule proposal? What have been the benefits and costs of this activity?

114. If you are a current SCI entity and your policies and procedures include a program to prevent the unauthorized access to SCI systems and information residing therein, how does your activity differ from the requirements of the rule proposal? What have been the benefits and costs of this activity?

115. The Commission requests that commenters provide relevant data and analysis to assist us in determining the economic consequences of the proposed amendments related to third-party providers' management. In particular, the Commission requests data and analysis regarding the costs SCI entities and third-party providers may incur, and benefits they may receive, from the proposed amendments.

116. Do you agree with the Commission's analysis of the benefits of the proposed amendments related to third-party providers' management? Why or why not? Please explain in detail.

117. Do you agree with the Commission's analysis of the costs of the proposed amendments related to third-party providers' management? Why or why not? Please explain in detail.

**b. Rule 1002—Corrective Action, Commission Notification, and Information Dissemination**

Regulation SCI requires SCI entities to take appropriate corrective actions in response to SCI events (Rule 1002(a)), notify the Commission of SCI events (Rule 1002(b)), and disseminate information regarding certain major SCI events to all members or participants of an SCI entity and certain other SCI events to affected members or participants (Rule 1002(c)). Rule 1000, in turn, defines SCI events to include systems

disruptions, systems compliance issues, and systems intrusions. The Commission is proposing two amendments that affect these provisions. First, it is proposing to expand the definition of systems intrusion in Rule 1000. Second, it is proposing to amend Rule 1002(b)(5) to eliminate the exception to the reporting requirement for de minimis systems intrusions and instead require the reporting of all systems intrusions, whether de minimis or not, within the time frames specified in paragraphs (b)(1) through (4).

New SCI entities will need to comply with these requirements of Rules 1000 and 1002, and their proposed amendments, for the first time. Existing SCI entities will need to apply the new definition of systems intrusion in Rule 1000 to the requirements of Rule 1002, including the amendments to Rule 1002(c). We discuss below the benefits and costs of these provisions and amendments for new and existing SCI entities.

**i. Benefits**

*1) Rule 1000 – Definition of SCI Events*

In general, the definition of SCI event (and its component parts) in Rule 1000 circumscribe the scope of the substantive requirements in Rule 1002. Therefore, many of the costs and benefits associated with the definitions are incorporated in the discussion of the substantive requirements. The benefits associated with scoping the substantive requirements for Rule 1002 through the specific definitions of systems disruption, systems compliance issue, and systems intrusion are discussed at length in the 2014 SCI Adopting Release[772] and would apply to the new SCI entities. We summarize those benefits here and discuss the benefits for both new and current SCI entities resulting from expanding the definition of systems intrusion.

---

[772] *See* SCI Adopting Release, *supra* note 1, at 72423-27.

**Systems Disruption.** Rule 1000 of Regulation SCI currently defines a "systems disruption" as an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system. This definition would remain unchanged. As the Commission noted in 2014, the definition sets forth a standard that SCI entities can apply in a wide variety of circumstances to determine in their discretion whether a systems issue should be appropriately categorized as a systems disruption. The inclusion of systems disruptions in the definition of SCI event, along with the requirements Rule 1002 should help effectively reduce the severity and duration of events for new SCI entities that harm pricing efficiency, price discovery, and liquidity and help Commission oversight of the securities markets.

**Systems Compliance Issues.** Under Rule 1000, a systems compliance issue is an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable. The Commission stated in 2014 that inclusion of systems compliance issues in the definition of SCI event and the resulting applicability of the Commission reporting, information dissemination, and recordkeeping requirements are important to help ensure that SCI systems are operated by SCI entities in compliance with the Exchange Act, rules thereunder, and their own rules and governing documents.

**System Intrusion.** Rule 1000 of Regulation SCI currently defines a "systems intrusion" as any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity. The Commission is proposing to expand the definition of systems intrusions to include any cybersecurity attack that disrupts, or significantly degrades, the normal

operation of an SCI system. This revision includes cybersecurity events that cause disruption on an SCI entity's SCI systems or indirect SCI systems, whether or not the event resulted in an entry into or access to such systems. In addition, the proposed revised definition would include any significant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria. This revision is intended to capture unsuccessful, but significant, attempts to enter an SCI entity's SCI systems or indirect SCI systems. The definition, including the proposed amendments, will apply to new SCI entities for the first time while the proposed amendments will apply to existing SCI entities.

In the SCI Adopting Release, the Commission discussed the benefits of including a system intrusion in the definition of an SCI event for which the requirements of Rule 1002 apply. These same benefits extend to the new SCI entities. Specifically, the Commission stated that unauthorized access, destruction, and manipulation of SCI systems and indirect SCI systems could adversely affect the markets and market participants because intruders could force systems to operate in unintended ways that could create significant disruptions in securities markets. Therefore, the inclusion of systems intrusions in the definition of SCI events can help reduce the risk of such adverse effects for new SCI entities.

The proposed changes, which would apply to new and current SCI entities, would update the definition to include additional types of incidents that are currently considered to be cybersecurity events that are not included in the current definition. If an incident meets the definition, it must then comply with the requirements for corrective action,

Commission notice, and information dissemination in Rule 1002. The proposed changes to the definition would thus ensure that the Commission and its staff are made aware when an SCI entity is the subject of a significant cybersecurity threat, including those that may be ultimately unsuccessful, which would provide important information regarding threats that may be posed to other entities in the securities markets, including other SCI entities. Because such cybersecurity events can cause serious harm and disruption to an SCI entity's operations, the Commission believes that the definition of systems intrusion should be broadened to include cybersecurity events that may not entail actually entering or accessing the SCI entity's SCI systems or indirect SCI systems, but still cause disruption or significant degradation, as well as significant attempted unauthorized entries. By requiring SCI entities to submit SCI filings for these new types of systems intrusions, the Commission believes that the revised definition of systems intrusion would also provide the Commission and its staff more complete information to assess the security status of the SCI entity, and also assess the impact or potential impact that unauthorized activity could have on the security of the SCI entity's affected systems as well on other SCI entities and market participants.

*2) Rule 1002—Corrective Action, Commission Notice, Information Dissemination*

As noted, Rule 1002 prescribes certain required actions for SCI entities upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. The requirements of Rule 1002(a) and (c) remain substantively unchanged from current Regulation SCI except additional events are scoped into the Rules for existing SCI entities through the proposed expanded definition of systems intrusion. These

provisions will therefore primarily affect new SCI entities. We discuss generally the benefits of the expanded definition above and do not repeat those here.[773]

**Corrective Action (Rule 1002(a)).** Rule 1002(a) requires an SCI entity to begin to take appropriate corrective action upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. Rule 1002(a) also requires corrective action to include, at a minimum, mitigating potential harm to investors and market integrity resulting from the SCI event, and devoting adequate resources to remedy the SCI event as soon as reasonably practicable. Thus, it would not be appropriate for an SCI entity to delay the start of corrective action once its responsible SCI personnel have a reasonable basis to conclude that an SCI event has occurred, and the SCI entity would be required to focus on mitigating potential harm to investors and market integrity resulting from the SCI event and devoting adequate resources to remedy the SCI event as soon as reasonably practicable. This provision remains unchanged for existing SCI entities, except to the extent they must comply with the requirements for additional events scoped in under the expanded definition of systems intrusion, as noted above. For both current and new SCI entities, the benefits of expanding the definition to include certain types of systems intrusions that are not covered by Regulation SCI would include a potential reduction in the length or severity of systems disruptions caused by these types of

---

773 The SCI Adopting Release considered the benefits and costs of the specific definitions for each type of SCI event. *See* SCI Adopting Release, *supra* note 1, at 72404-08. Those costs and benefits remain the same for new SCI entities to which these definitions would apply and are not repeated here, except with respect to the definition of systems intrusions, which the Commission proposes to amend. To the extent that the primary effect of these definitions is realized through the requirements in Rule 1002 to take corrective action, notify the Commission, and disseminate information, we discuss the effects of applying those requirements on new SCI entities below.

intrusions and would thus reduce the negative effects of those interruptions on the SCI entity and on market participants.

The corrective action requirement of Regulation SCI will likely reduce the length of systems disruptions, systems compliance issues, and systems intrusions, and thus reduce the negative effects of those interruptions on the SCI entity and market participants. Additionally, to the extent that corrective action could involve wide-scale systems upgrades, some SCI entities may potentially seek to accelerate capital expenditures, for example, by updating their systems with newer technology earlier than they might have otherwise to comply with Regulation SCI. As such, Rule 1002(a) could further help ensure that SCI entities invest sufficient resources as soon as reasonably practicable to address systems issues.

New SCI entities will become subject to Rule 1002(a) for the first time. The Commission believes that new SCI entities already have a variety of procedures in place to take corrective actions when system issues occur. However, Rule 1002(a) may require modifications to those existing practices in part because the rule specifies the timing and enumerates certain goals for corrective action.[774]

**Commission Notification (Rule 1002(b)).** Rule 1002(b) requires an SCI entity to notify the Commission of the SCI event immediately upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. Within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, an SCI entity is required to submit to the Commission a more detailed written notification, on a good faith, best efforts basis, pertaining to the SCI event. Until

---

[774] *See* SCI Adopting Release, *supra* note 1, at 72423.

such time as the SCI event is resolved and the SCI entity's investigation of the SCI event is closed, the SCI entity is required to provide updates regularly, or at such frequency as requested by a representative of the Commission. The SCI entity is also required to submit a detailed final written notification after the SCI event is resolved and the SCI entity's investigation of the event is closed (and an additional interim written notification, if the SCI event is not resolved or the investigation is not closed within a specified period of time). Finally, paragraph (b)(5) currently provides an exception to the reporting requirements of paragraphs (b)(1) through (4) for de minimis SCI events, and SCI entities are currently required to submit a summary to the Commission with respect to systems disruptions and systems intrusions only on a quarterly basis. The Commission is proposing to amend this provision to require SCI entities to exclude systems intrusions from this exception so that SCI entities will need to report systems intrusions, whether de minimis or not, within the time frames specified in paragraphs (b)(1) through (4). This would eliminate quarterly reporting for de minimis systems intrusions. Thus, for current SCI entities, the difference concerns the time frame for, and manner of, reporting de minimis systems intrusions while new SCI entities will be subject to the entire Commission notification regime for the first time.

For the new SCI entities, Rule 1002(b) as a whole would enhance the effectiveness of Commission oversight of the operation of these entities. For example, SCI events notification results in greater transparency for the Commission, including ensuring that the Commission has a view into problems at particular SCI entities for regulatory purposes as well as perspective on the effect of a single problem to the market

at-large.[775] Further, the requirements of submitting notifications pertaining to the SCI events to the Commission, set forth by Rule 1002(b), could help prevent systems failures from being dismissed as momentary issues, because notification would help focus the SCI entity's attention on the issue and encourage allocation of SCI entity resources to resolve the issue as soon as reasonably practicable.

Both new and current SCI entities would be subject to the new reporting requirements under the proposed revisions to Rule 1001(b)(5). These revisions eliminate the need for entities to determine if an intrusion (which should be rare and also may be difficult to assess) meets the de minimis threshold before it notifies the Commission, and instead would require reporting to the Commission for all systems intrusions at the time of the event, which will provide more timely information to the Commission. This may result in more frequent reporting for systems intrusions while also eliminating quarterly reporting of systems intrusions, as compared to the baseline.

**Information Dissemination (Rule 1002(c)).** Rule 1002(c) currently requires an SCI entity to disseminate information regarding certain major SCI events to all of its members or participants and certain other SCI events to affected members or participants. Specifically, promptly after any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, an SCI entity is required to disseminate certain information regarding the SCI event. When certain additional information becomes known, the SCI entity is required to promptly disseminate such information to those members or participants (or, as proposed, in the case of an SCI broker-dealer, customers) of the SCI entity that any responsible SCI personnel has reasonably estimated may have

---

[775] *See* SCI Adopting Release, *supra* note 1, at 72424 (citing letter by David Lauer).

been affected by the SCI event. Until the SCI event is resolved, the SCI entity is required to provide regular updates on the required information. In the case of a major SCI event, where the impact is most likely to be felt by many market participants, dissemination of information to all members, participants, or customers, as applicable, of the SCI entity is required. A major SCI event is defined to mean an SCI event that has any impact on a critical SCI system or a significant impact on the SCI entity's operations or on market participants.

The information dissemination requirement currently does not apply to SCI events to the extent that they relate to market regulation or market surveillance systems and de minimis SCI events. The Commission is proposing to add to these exceptions for the information dissemination requirement, a systems intrusion that is a significant attempted unauthorized entry into the SCI systems or indirect SCI systems. Accordingly, Rule 1002(c) remains mostly unchanged for existing SCI entities, except to the extent they must comply with the requirements for additional events scoped in under the expanded definition of systems intrusion (the benefits of which are discussed above) and except for systems intrusions that are significant attempted unauthorized entries, which are exempted from the information dissemination requirements. New SCI entities, however, will become subject to the information dissemination requirements for the first time.

Rule 1002(c) is expected to help market participants—specifically the members, participants, or customers, as applicable of new SCI entities estimated to be affected by an SCI event and, in the case of major SCI events, all members, participants, or customers of a new SCI entity—to better evaluate the operations of SCI entities by requiring certain information about the SCI event to be disclosed. Furthermore, increased

awareness of SCI events through information disseminated to members, participants, or customers, as applicable, should provide new SCI entities additional incentives to maintain robust systems and minimize the occurrence of SCI events. More robust SCI systems and the reduction in the occurrence of SCI events at new SCI entities could reduce interruptions in price discovery processes and liquidity flows. For example, in 2014, a commenter stated that sharing information about hardware failures, systems intrusions, and software glitches will alert others in the industry about such problems and help reduce system-wide costs of diagnosing problems, as well as result in improved responses to technology problems.[776]

With respect to the new exception for significant attempted unauthorized entries, which impacts new and existing SCI entities, the Commission is concerned that disseminating information about unsuccessful attempted entries to members or participants of an SCI entity would create unnecessary distractions, particularly since the SCI entity's security controls were able, in fact, to repel the cybersecurity event. In addition, disseminating information regarding unsuccessful intrusions could result in the threat actors being unnecessarily alerted that they have been detected, which could make it more difficult to identify the attackers and halt their efforts on an ongoing, more permanent basis.

The Commission recognizes that many of the new SCI entities are currently subject to other regulatory requirements to maintain policies and procedures that address the provisions required by these rules, as discussed in detail above.[777] Similarly, some

---

[776] *See* SCI Adopting Release, *supra* note 1, at 72426 n. 931 (citing letter from James Angel).

[777] *See* sections III.A.2.a.ii, III.A.2.b.ii, III.A.2.c.i., V.B.1.a.ii, V.B.1.b.ii, and V.B.1.c.ii.

existing SCI entities engage in current market practices consistent with the expanded definition of systems intrusion.

The benefits from the policy and procedure requirements in Rule 1002(a) through (c) for the new SCI entities (and the costs, as discussed below), will therefore depend on the extent to which their current operations already align with the rule's requirements, given both existing regulation and current practice.

While some of the existing regulations that apply to the proposed new SCI entities may be consistent with or similar to the policy and procedure requirements of Regulation SCI discussed in this section, the Commission believes it is nevertheless appropriate to apply these policy and procedure requirements to the new SCI entities and that doing so would benefit participants in the securities markets in which these entities operate.

Overall, applying the specific and comprehensive requirements set forth in Rule 1002(a) through (c) of Regulation SCI to the new SCI entities would enhance and build on any existing policies and procedures, thereby furthering the goals of Regulation SCI to strengthen the technology infrastructure of the U.S. securities markets and improve its resilience.

**ii. Costs**

We discuss below the costs of complying with the requirements of Rule 1002, applying the definitions in Rule 1000, including the amended definition of systems intrusion. Because the definitions themselves have no associated costs, all of the costs associated with the amended definition flow through the substantive requirements. New SCI entities will need to comply with these requirements for the first time whereas costs for the existing SCI entities are attributed to the expanded definition of systems intrusion and the amendment to Rule 1002(b)(5). Relative to the current practice and baseline, the

proposed rule expansion of the definition of the intrusion would likely result in more frequent reporting by the SCI entities to the Commission, which is reflected in the costs estimates below.

**Corrective Action (Rule 1002(a)).** Rule 1002(a) could impose modestly higher costs for new SCI entities in responding to SCI events relative to their current practice. In the PRA analysis, the Commission estimates those costs as approximately $1.2 million in initial and $0.4 million in annual costs.[778] Furthermore, if Regulation SCI reduces the frequency and severity of SCI events in the future, the cost of corrective action could similarly decline over time. Nevertheless, the Commission lacks data regarding the degree to which Regulation SCI will reduce the frequency and severity of SCI events at new SCI entities.

In addition, if a new SCI entity is required to take corrective action sooner than it might have without the requirements of Regulation SCI, this may impose indirect costs (*i.e.,* opportunity costs) to such SCI entities because they may have to delay or reallocate their resources away from profitable projects and direct their resources toward taking corrective action required by the rule. It is difficult to assess indirect costs imposed on new SCI entities without having comprehensive and detailed information on the value of the potential foregone projects of those SCI entities. The facts and circumstances of each specific SCI event will be different.

Existing SCI entities may incur new costs associated with corrective action for additional systems intrusions scoped in under the expanded definition. The Commission

---

[778] *See* section IV.D.7. For purposes of this Economic Analysis, there are two fewer entities than under the PRA analysis, lowering these estimated costs. *See supra* note 700.

estimates a one-time total cost of approximately $0.5 million for all existing SCI entities to update their procedures to account for additional types of systems intrusions.[779]

To the extent new SCI entities currently undertake correction action consistent with the Rule 1002(a) requirements, they could incur lower PRA costs to comply with the requirements of Rule 1002(a) than entities without such existing requirements. Similarly, to the extent many existing SCI entities currently undertake corrective action consistent with the expanded definition of systems intrusion, they could incur lower PRA costs to comply with the amended requirements of Rule 1002(a) than entities without such existing requirements.

**Notification of SCI Events (Rule 1002(b)).** The compliance costs associated with Rule 1002(b) are attributed to the paperwork burden of Commission notifications of SCI events, including recordkeeping and submission of quarterly reports with respect to de minimis SCI events, as applicable. For new SCI entities, these costs include costs to comply with the notification requirements, as amended, for the first time. Existing SCI entities would incur costs complying with the amendment to Rule 1002(b)(5) as well as the costs associated with notification for new events scoped in under the expanded definition of systems intrusions. These are discussed in detail in section IV.

For Rule 1002(b)(1), the Commission estimates approximately $0.1 million in initial and annual costs for existing and new SCI entities alike.[780] For Rule 1002(b)(2), the Commission estimates approximately $1.3 million in initial and annual costs for

---

[779] *See* section IV.D.2.b, IV.D.7.

[780] *See* section IV.D.7; *see also supra* note 700.

existing SCI entities and $1.5 million in initial and annual costs for new SCI entities.[781] For Rule 1002(b)(3), the Commission estimates approximately $0.2 million in initial and annual costs for existing SCI entities and $0.2 million in initial and annual costs for new SCI entities.[782] For Rule 1002(b)(4), the Commission estimates approximately $2.0 million in initial and annual costs for existing SCI entities and $2.3 million in initial and annual costs for new SCI entities.[783] Finally, for Rule 1002(b)(5), the Commission estimates a savings for existing SCI entities, as noted above, and approximately $1.2 million in initial and annual costs for new SCI entities.[784]

To the extent new SCI entities currently provide notification consistent with the Rule 1002(b) requirements, they could incur lower PRA costs to comply with the requirements of Rule 1002(b) than entities without such existing practices.

**Information Dissemination (Rule 1002(c)).** While some new SCI entities currently provide their members or participants and, in some cases, market participants or the public more generally, with notices of certain systems issues (*e.g.*, system outages), Rule 1002(c) may impose new requirements that they have not currently implemented. As such, the requirements of Rule 1002(c) will impose costs—which are attributed to paperwork burdens—on new SCI entities with respect to preparing, drafting, reviewing, and making the information available to members or participants, or, in the case of an SCI broker-dealer, customers. For new SCI entities the Commission estimates approximately $1.3 million in costs, initially and annually, for disseminating information

---

781 *See id.*

782 *Id*.

783 *Id*.

784 *Id*.

about SCI events and systems affected, as required by Rule 1002(c)(1).[785] For new entities, the Commission also estimates approximately $1.6 million in initial costs and $0.4 million in annual costs to develop processes to identify the nature of a critical system, major SCI event, or a *de minimis* SCI event for purposes of disseminating this information.[786]

Existing SCI entities may incur new costs associated with information dissemination for additional systems intrusions scoped in under the expanded definition. The Commission estimates approximately $0.7 million in initial and annual PRA costs for existing SCI entities, and $0.4 million in initial and annual costs for new SCI entities, for disseminating information about system intrusions as required by the proposed revisions to Rule 1002(c)(2).[787] These costs are discussed in more detail in section IV.

To the extent new SCI entities currently disseminate information consistent with the Rule 1002(c) requirements, they could incur lower PRA costs to comply with the requirements of Rule 1002(c) than entities without such existing requirements. Similarly, to the extent many existing SCI entities currently disseminate information consistent with the expanded definition of systems intrusion, they could incur lower PRA costs to comply with the amended requirements of Rule 1002(c) than entities without such existing practices.

**Identification of Nature of System or Event.** To comply with the requirements of Rule 1002, SCI entities need to identify certain types of events and systems issues,

---

785 *See* section IV.D.7. For purposes of this Economic Analysis, there are two fewer entities than under the PRA analysis, lowering these estimated costs. *See supra* note 700.

786 *See* section IV.D.2.d, IV.D.7; s*ee also supra* note 700.

787 *See* section IV.D.7; *supra* note 700.

including whether the event is de minimis. Current SCI entities would already have such processes in place to comply with the existing requirements of Regulation SCI. The Commission understands that many new SCI entities likely already have some internal procedures for determining the severity of a systems issue.

As a new SCI entity must determine whether an SCI event has occurred and whether it is a de minimis SCI event, Rule 1002 may impose one-time implementation costs on new SCI entities associated with developing a process or modifying its existing process to ensure that they are able to quickly and correctly make such determinations, as well as ongoing costs in reviewing the adopted process. As explained in detail in section IV, we estimate new SCI entities would incur an initial PRA cost of $1,641,024 and an ongoing annual PRA cost of $362,418 to develop these processes.

To the extent new SCI entities currently have a process in place for identifying certain types of events and system issues consistent with the relevant Rule 1002 requirements, they could incur lower PRA costs to comply with the relevant requirements of Rule 1002 than entities without such existing requirements.

**c. Rule 1003—Material Systems Changes and SCI Review**

**i. Reports to the Commission (Rule 1003(a))**

Rule 1003(a)(1) requires an SCI entity to provide quarterly reports to the Commission describing completed, ongoing, and planned material systems changes to its SCI systems and the security of indirect SCI systems, during the prior, current, and subsequent calendar quarters. Rule 1003(a)(1) also requires an SCI entity to establish reasonable written criteria for identifying a change to its SCI systems and the security of its indirect SCI systems as material. Rule 1003(a)(2) requires an SCI entity to promptly submit a supplemental report to notify the Commission of a material error in or material

omission from a previously submitted report. These requirements remain unchanged. New SCI entities, however, will become subject to them for the first time. We discuss the benefits and costs of applying these provisions to new SCI entities below.

*1) Benefits*

The notification requirement would be beneficial because it permits the Commission and its staff to have up-to-date information regarding an SCI entity's systems development progress and plans, to aid in understanding the operations and functionality of the systems, and any material changes thereto, without requiring SCI entities to submit a notification to the Commission for each material systems change.[788]

The Commission recognizes that some of the new SCI entities are currently subject to other material systems change notification requirements and that most, if not all, new SCI entities have some internal processes for documenting systems changes as discussed in detail above.[789] Accordingly, the Commission notification requirements in Rule 1003(a) would be new for most but not all of the new SCI entities.

The benefits from the policy and procedure requirements in Rule 1003(a) for the new SCI entities (and the costs, as discussed below), will therefore depend on the extent to which their current operations already align with the rule's requirements, given both existing regulation and current practice.

While some of the existing regulations that apply to the proposed new SCI entities may be consistent with or similar to the policy and procedure requirements of Regulation SCI discussed in this section, the Commission believes it is nevertheless appropriate to

---

788 *See* SCI Adopting Release, *supra* note 1, at 72337-38.

789 *See* sections III.A.2.a.ii, III.A.2.b.ii, III.A.2.c.i., V.B.1.a.ii, V.B.1.b.ii, and V.B.1.c.ii.

apply these policy and procedure requirements to the new SCI entities and doing so would benefit participants in the securities markets in which these entities operate. Overall, applying the specific and comprehensive requirements set forth in Rule 1003(a) of Regulation SCI to the new SCI entities would complement any existing requirements and enhance any reporting of material systems changes already in place for these entities.

Costs

The compliance costs of Rule 1003(a) primarily entail costs associated with preparing and submitting Form SCI in accordance with the instructions thereto. The initial and ongoing PRA cost estimates associated with preparing and submitting Form SCI with regard to material systems changes under Rule 1003(a)(1) and (2) are discussed in detail in section V. The Commission does not expect Rule 1003(a) would impose significant costs on SCI entities other than those discussed in section IV. For new SCI entities, the Commission estimates approximately $1.0 million in initial PRA costs and $0.3 million in annual PRA costs to establish reasonable written criteria for identifying material changes to SCI systems and to the security of indirect SCI systems.[790] For new SCI entities, the Commission also estimates approximately $3.6 million initially and annually in PRA costs associated with material system change notices.[791] The Commission acknowledges that the actual cost for each new entity may differ depending on their existing processes for documenting system changes and whether the necessary information is readily available. The Commission does not expect Rule 1003(a) to impose significant costs on new SCI entities besides the costs discussed here. To the

---

790 *See* section IV.D.7. For purposes of this Economic Analysis, there are two fewer entities than under the PRA analysis, lowering these estimated costs. *See supra* note 700.

791 *Id*.

extent new SCI entities are currently subject to other material systems change notification regulatory requirements and have existing processes for documenting systems changes that align with the Rule 1003(a) requirements, they could incur lower costs to comply with the requirements of Rule 1003(a) than entities without such existing requirements.

**ii. Annual SCI Review (Rules 1000 and 1003(b))**

Rule 1003(b) requires SCI entities to conduct an annual SCI review and works in conjunction with the definition of "SCI review" from Rule 1000. Under the current definition, SCI review includes "(1) A risk assessment with respect to such systems of an SCI entity; and (2) An assessment of internal control design and effectiveness of its SCI systems and indirect SCI systems to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards."[792] Rule 1003(b)(1) then requires an annual SCI review, "provided, however, that (i) Penetration test reviews . . . shall be conducted at a frequency of not less than once every three years; and (ii) Assessment of SCI systems directly supporting market regulation or market surveillance shall be conducted at a frequency based upon the risk assessment conducted as part of the SCI review, but in no case less than once every three years."[793] Rule 1003(b)(2) and (3) require each SCI entity to submit its annual SCI review report to, respectively, "senior management of the SCI entity for review" and "to the Commission and to the board of director of the SCI entity, or the equivalent of such board" within specified time frames.[794]

---

792 17 CFR 242.1000.

793 17 CFR 242.1003(b)(1).

794 17 CFR 242.1003(b)(2) and (3).

The Commission proposes to make changes to the definition of "SCI review." Specifically, under the proposed amendment, "SCI review" would include, for both SCI systems and indirect SCI systems, an annual assessment, using appropriate risk management methodology, of risks related to capacity, integrity, resiliency, availability, and security, and internal control design and operating effectiveness, and annual penetration test reviews (increased from at least one review every three years), and a review of third-party provider management risks and controls. Rule 1003(b) would also be amended to require more specific information to be included in the SCI review report, including a list of the controls reviewed and a description of each such control; the findings of the SCI review, including, at a minimum, assessments of the risks described above; a summary, including the scope of testing and resulting action plan, of each penetration test review; and a description of each deficiency and weakness identified by the SCI review. In addition, the revisions would make mandatory that a response from senior management to the report is included when it is submitted to the Commission and board, whereas previously the language appeared permissive.

*1) Benefits*

The SCI review requirement would have SCI entities assess the relative strengths and weaknesses of their systems which may help, in turn, improve systems and reduce the number of SCI events. The reduction in occurrence of SCI events could reduce interruptions in the price discovery process and liquidity flows, as discussed above. In addition, the efficiency of the Commission's oversight (*e.g.*, inspection) of SCI entities' systems would be enhanced.

The proposed increase in the frequency of penetration testing reviews, which applies to both new and existing SCI entities, should better prepare SCI entities against cyber threats, which are increasing in numbers and becoming more sophisticated. For this reason, the proposed amendment is expected to further strengthen the security, integrity, and resilience of all SCI entities. Having an annual penetration testing requirement can help SCI entities reduce the likelihood of costly data breaches.[795] For instance, according to one industry source, RSI Security, a penetration test "can measure [the entity's] system's strengths and weaknesses in a controlled environment before [the entity has] to pay the cost of an extremely damaging data breach."[796]

The requirement to review third-party provider management risks and controls will work in conjunction with the proposed amendment to Rule 1001(a)(2) requiring inclusion of a third-party provider management. The additional benefit of requiring an annual review of third-party provider management risks and controls is to ensure the benefits provided by the amendment to Rule 1001(a)(2) are properly realized and further increasing the likelihood that third-party providers provide functionality, support or services that are consistent with the requirements of Regulation SCI.

The Commission understands that many existing SCI entities have already adopted practices that may align with some of the provisions of the proposed amendment to Rule 1003(b).

---

795 *See, e.g.*, Mirza Asrar Baig, *How Often Should You Pentest?*, Forbes.com (Jan. 22, 2021), *available at* https://www.forbes.com/sites/forbestechcouncil/2021/01/22/how-often-should-you-pentest/?sh=b667999573c6.

796 RSI Security, *What is the Average Cost of Penetration Testing?,* RSI Security Blog (Mar. 5, 2020), *available at* https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:~:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company.

The Commission also understands that many new SCI entities currently undertake annual systems reviews and that senior management and/or the board of directors or a committee thereof reviews reports of such reviews as discussed in detail above.[797] However, the scope of the systems reviews, and the level of senior management and/or board involvement in such reviews, can vary.

The benefits from the policy and procedure requirements in Rule 1003(b) for the new SCI entities (and the costs, as discussed below) and the benefits from the amended policy and procedure requirements in Rule 1003(b) for the existing SCI entities, will therefore depend on the extent to which their current operations already align with the rule's requirements, given both existing regulation and current practice.

For example, with respect to broker-dealers, prior Commission and FINRA exam results indicate that many if not most large broker-dealers conduct risk assessments of internal control design and effectiveness. Additionally, some broker-dealers provide annual cybersecurity reports to the board. The Commission understands that nearly all large broker-dealers conduct penetration testing[798] of systems considered critical although not all firms conduct such testing annually. Many of these current market practices align with the policy and procedure requirements of Regulation SCI discussed in this section.

While some of the existing regulations that apply to the proposed new SCI entities or current market practices may be consistent with or similar to some of the policy and

---

797 *See* sections III.A.2.a.ii, III.A.2.b.ii, III.A.2.c.i., V.B.1.a.ii, V.B.1.b.ii, and V.B.1.c.ii.

798 *Supra* note 619. According to FINRA's 2018 RCA, 100% of higher revenue firms include penetration testing as a component in their overall cybersecurity program. Other factors these firms consider in evaluating the relevance of penetration testing include the degree to which they manage or store confidential or critical data such as trading strategies, customer PII, information about mergers and acquisitions or confidential information from other entities (for example, in the case of clearing firms).

procedure requirements of Regulation SCI discussed in this section, the Commission believes it is nevertheless appropriate to apply these policy and procedure requirements to the new SCI entities and that doing so would benefit participants in the securities markets in which these entities operate.

Overall, applying the specific and comprehensive requirements set forth in Rule 1003(b) of Regulation SCI to the new SCI entities would enhance and build on any existing policies and procedures, thereby furthering the goals of Regulation SCI to strengthen the technology infrastructure of the U.S. securities markets and improve its resilience.

*2) Costs*

New SCI entities will incur costs to comply with the review requirements for the first time, and existing SCI entities will incur costs to comply with the amended provisions. The initial and ongoing paperwork burden associated with conducting an SCI review, submitting a report of the SCI review to senior management of the SCI entity for review, and submitting a report of the SCI review and the response by senior management to the Commission and to the board of directors of the SCI entity or the equivalent of such board is discussed in detail in section IV. For existing SCI entities, the Commission estimates approximately $7.4 million in initial and annual costs, while for new SCI entities the Commission estimates approximately $9.6 million in initial and annual costs.[799] The paperwork burden estimates provided here for new SCI entities include the costs of complying with the proposed amended versions of the Rule, namely

---

[799] *See* section IV.D.7. For purposes of this Economic Analysis, there are two fewer entities than under the PRA analysis, lowering these estimated costs. *See supra* note 700.

the proposed additional requirements for conducting the SCI review, the requirement that SCI entities include more specific information in their SCI review reports, and related recordkeeping.[800]

To the extent new SCI entities currently undertake annual systems reviews and that senior management and/or the board of directors or a committee thereof reviews reports of such reviews consistent with the Rule 1003(a) requirements, they could incur lower PRA costs to comply with the requirements of Rule 1003(a) than entities without such existing practices. Similarly, to the extent many existing SCI entities have already adopted practices that are consistent with some of the provisions of the proposed amendment to Rule 1003(b), they could incur lower PRA costs to comply with the requirements of Rule 1003(a) than entities without such existing practices.

With respect to the increased frequency for the penetration test review, this requirement will impose non-paperwork compliance costs in addition to those captured by the PRA estimates for both new and existing SCI entities. For example, RSI Security explains that penetration testing "can cost anywhere from $4,000-$100,000," and "[o]n average, a high quality, professional [penetration testing] can cost from $10,000-$30,000."[801] RSI Security, however, was clear that the magnitudes of these costs can vary with size, complexity, scope, methodology, types, experience, and remediation measures.[802] Another source estimates a "high-quality, professional [penetration testing to cost] between $15,000-$30,000," while emphasizing that "cost varies quite a bit based

---

800 *See* section IV.D.3.

801 *See* RSI Security, *supra* note 796.

802 *See id.*

on a set of variables."[803] This is in line with a third source, which states that "[a] true penetration test will likely cost a minimum of $25,000."[804] The Commission preliminarily believes that the cost of penetration testing will range between $25,000 and $100,000 for new and existing SCI entities, in light of the complexity and scope required, although the costs may be somewhat lower depending on the frequency with which such testing and review are currently conducted by new and existing SCI entities. The Commission acknowledges the non-paperwork costs of the proposed increase in the frequency of a penetration test review, and seeks feedback on these costs.

**Request for comment**:

118. For current and proposed SCI entities, how often do you (already) perform penetration testing and how much does it cost?

#### d. Rule 1004—Business Continuity and Disaster Recovery Plan Testing

Rule 1004(b) requires the testing of an SCI entity's business continuity and disaster recovery plans at least once every 12 months. Rule 1004(a) and (b) require participation in such testing by those members or participants that an SCI entity reasonably determines are, taken as a whole, the minimum number necessary for the maintenance of fair and orderly markets in the event of the activation of its BC/DR plans. Rule 1004(c) requires an SCI entity to coordinate such testing on an industry- or sector-

---

803 Gary Glover, *How Much Does a Pentest Cost?*, Securitymetrics Blog (Nov. 15, 2022, 8:36 a.m.), *available at* https://www.securitymetrics.com/blog/how-much-does-pentest-cost.

804 Mitnick Security, *What Should You Budget for a Penetration Test? The True Cost*, Mitnick Security Blog, (Jan. 29, 2021, 5:13 a.m.), *available at* https://www.mitnicksecurity.com/blog/what-should-you-budget-for-a-penetration-test-the-true-cost.

wide basis with other SCI entities.[805] The Commission is proposing to amend Rule 1004 to require that third-party providers also participate in such testing. Therefore, for current SCI entities, the difference is to include third-party providers in its testing. For new SCI entities, the entire provision is a new obligation. We discuss below the benefits and costs of applying this provision, including the proposed amendments, to new and existing SCI entities.

**i. Benefits**

As discussed above, requiring the new SCI entities to test their BC/DR plans would likely improve backup infrastructure and lead to fewer market-wide shutdowns, which should help facilitate continuous liquidity flows in markets, reduce pricing errors, and thus improve the quality of the price discovery process.[806] Moreover, Rule 1004 would help ensure fair and orderly markets in the event of the activation of BC/DR plans.

In addition, for both new and existing SCI entities, the proposed requirement to establish standards for the designation of third-party providers and their participation in the currently scheduled functional and performance testing of the operation of BC/DR plans will help those SCI entities ensure that their efforts to develop effective BC/DR plans are not undermined by a lack of participation by third-party providers that the SCI entity believes are necessary to the successful activation of such plans.

---

805 One avenue for coordinating such testing is through SIFMA's voluntary Industry-Wide Business Continuity Test. *See* SIFMA, *Industry-Wide Business Continuity Test* (Oct. 15, 2022), *available at* https://www.sifma.org/resources/general/industry-wide-business-continuity-test/.

806 *See* sec. V.C.1.; *see also* SCI Adopting Release, *supra* note 1, at 72429.

Although the Commission finds it impracticable to quantify these benefits in dollar terms,[807] the Commission believes it would be helpful to consider the cost of an unplanned outage. For example, the Commission considers a reduced occurrence of a potential outage as a benefit of complying with Regulation SCI. As discussed above, one source of cost estimates for an unplanned outage is the Ponemon Institute's 2016 Cost of Data Center Outages report.[808] According to the report, the total cost per minute of an unplanned outage was $8,851 for the average data center the Institute surveyed in 2016.[809] This implies a cost of $531,060 per hour of an unplanned outage at the time.[810] Moreover, outages themselves can also last far longer than one hour. For example, natural disasters, such as hurricanes, can often lead to lengthy outages lasting 200 to 400 hours.[811] Taken together, this data suggests potentially significant benefits to having an adequate policy and procedure in place to ensure business continuity and disaster relief plans for SCI entities.

The benefits from the BC/DR requirements in Rule 1004 for the current and new SCI entities (and the costs, as discussed below) will depend on the extent to which their current operations already align with the rule's requirements, given both existing regulation and current practice. Based on discussion with industry participants, the

---

807 As discussed in section V.D.1. multiple factors would affect the harm to the overall economy from an unplanned outage at an SCI entity.

808 *See supra* note 696.

809 *Id.* at 14.

810 The report also showed that this figure was increasing over time. The same figure was $5,617/min in 2010 and $7,908/min in 2013. *See id.*

811 *See* Data Foundry, *How Much Should You Spend On Business Continuity and Disaster Recovery* (Dec. 12, 2019), *available at* https://www.datafoundry.com/blog/much-spend-business-continuity-disaster-recovery.

Commission understands that some existing SCI entities already require third-party service provider participation in testing despite not being required to do so currently under Regulation SCI. For these SCI entities, there may be incremental benefits from making the third-party service provider participation a requirement under the Regulation and ensuring that they continue to include these parties in such testing going forward.

Some new SCI entities, either due to existing regulatory requirements or on their own volition, also already require some of their members or participants, as well as third-party providers, to participate in performance testing of BC/DR plans or offer the opportunity to do so on a voluntary basis, although such participation may be limited in nature (*e.g.*, testing for connectivity to backup systems). However, existing requirements for the new SCI entities may differ from the requirements of Rule 1004. For example, FINRA Rule 4370 does not require the functional and performance testing and coordination of industry or sector-testing of such plans.

With respect to SBSDRs, the requirements of Regulation SCI are more specific and comprehensive in terms of testing business continuity and disaster recovery plans than the principles-based requirements of Rule 13n-6. The requirements of Regulation SCI would thus exist and operate in conjunction with Rule 13n-6 and help ensure that SBSDR market systems are robust, resilient, and secure and enhance Commission oversight of the these systems. Moreover, to the extent the systems of SBSDRs that relate to the securities-based swap markets function separately (or could function separately in the future) from the systems of SDRs that relate to the swaps markets, applying Rule 1004 to these entities would help to ensure effective testing of BC/DR plans for the

specific systems relevant to the securities markets and would subject these systems to enhanced Commission oversight.

Similarly, the Commission recognizes that exempt clearing agencies that this rule proposal would newly scope into Regulation SCI are currently required to have BC/DR plans and test them at least annually with the participation of customers, critical utilities, critical service providers, other clearing agencies, other market infrastructures, and any other institution with which interdependencies have been identified in the business continuity policy. Overall, applying the specific and comprehensive requirements set forth in Rule 1004 would complement existing requirements and enhance the BC/DR plans tests already in place for these entities.

**ii. Costs**

The mandatory testing of SCI entity BC/DR plans, including backup systems, as required under amended Rule 1004, will result in costs to SCI entities. For current SCI entities, the increase in the cost would come from the requirement to include designated third-party providers in when testing their BC/DR plans—to the extent they have not been doing so. In addition, because the proposed requirements of Rule 1004 would require participation by various other parties, including designated members, participants, and other third parties, these parties may also bear costs of Rule 1004. We discuss these various costs below.

**Costs to New and Existing SCI Entities.** It is the Commission's understanding that some new SCI entities already engage with their members, participants or customers, as applicable, or third-party providers when testing BC/DR plans. Furthermore, as mentioned above, market participants, including new SCI entities, already coordinate certain BC/DR plans testing to an extent. However, Rule 1004 mandates participation in

testing for new SCI entities that do not currently participate, requires coordination when testing BC/DR plans, and requires their members, market participants, or their third-party providers participate.

In particular, Rule 1004 requires SCI entities to designate their members, participants, or third-party providers to participate in BC/DR plans testing and to coordinate such testing with other SCI entities on an industry- or sector-wide basis. The requirement of member, participant, or third-party provider designation in BC/DR plans testing under Rule 1004 may impose new costs even for those that currently have BC/DR plan testing, as an SCI would have to allocate resources towards initially establishing and later updating standards for the designation of its members and participants and third-party providers for testing. For example, systems reconfiguration for functional and performance testing and establishing an effective coordinated test script could be a complex process and result in additional costs, but it is an important first step in establishing robust and effective BC/DR plans testing. Furthermore, the requirement to coordinate industry- or sector-wide testing would impose additional administrative costs because an SCI entity would be required to notify its members, participants, or third-party providers and also organize, schedule, and manage the coordinated testing.

Many of the costs associated with Rule 1004 are costs estimated in the PRA in section IV. For existing SCI entities the Commission estimates approximately $1.4 million in initial costs and $0.5 million in annual costs, while for new SCI entities the Commission estimates approximately $3.2 million in initial costs and $1.1 million in

annual costs.[812] In addition to the PRA costs, the Commission believes that new SCI entity's may incur non-paperwork costs associated with the mandatory testing of BC/DR plans, including backup systems; however, the Commission finds it impracticable to provide a quantified estimate of these specific non-paperwork costs for new SCI entities because the Commission does not have detailed information regarding the current level of engagement by members or participants in BC/DR testing and the associated costs, or the details of the BC/DR testing that new SCI entities would implement pursuant to Rule 1004.

In addition, both new and existing SCI entities may incur costs beyond the PRA costs to comply with the requirement that third-party providers be included in the testing requirement. The Commission acknowledges that there will be significant variations in incremental cost for new and existing SCI entities beyond the costs of complying with the rest of the testing requirements, depending on the relationship of each SCI entity with the third-party provider and the need to revise any contractual agreement between them. But in any situation where a third-party provider is already required to provide a continuous service plan (such as 24/7 connectivity), the incremental cost of having the third-party provider participate in the BC/DR testing should be modest. To the extent existing and new SCI entities already have BC/DR plan testing that align with the Rule 1004 requirements, they could incur lower costs to comply with the requirements of Rule 1004 than entities without such existing BC/DR plan testing.

---

[812] *See* section IV.D.4. For purposes of this Economic Analysis, there are two fewer entities than under the PRA analysis, lowering these estimated costs. *See supra* note 700.

**Costs to SCI Entity Members, Participants, and Third-Party Providers.** Rule 1004 will also impose costs on SCI entity designated members, participants and third-party providers. Although members, participants, and third-party providers will incur costs as a result of Rule 1004, those that are likely to be designated to participate in business continuity and disaster recovery plans testing are those that conduct a high level of activity with the SCI entity or those that play an important role for the SCI entity and who are more likely to have already established connections to the SCI entity's backup site. It is the Commission's understanding that most of the larger members, participants, and third-party providers already have established connectivity with the SCI entity's backup site and already monitor and maintain such connectivity, and thus the additional connectivity costs imposed by Rule 1004 would be modest to these members or participants.[813] The Commission, however, finds it impracticable to provide a quantified estimate of the specific costs for SCI entity members, participants or third-party providers associated with the mandatory testing required by Rule 1004 as such data or information is not required to be provided by SCI entities to the Commission under Regulation SCI. Nevertheless, the Commission preliminarily believes, for similar reasons as provided in the section discussing non-paperwork burden estimates for Rule 1001(a) and (b), that the figures from 2014 remain reasonable approximations for new SCI entities in 2023, after adjusting for inflation since 2014.[814]

---

[813] *See* SCI Adopting Release, *supra* note 1, at 72430.

[814] After adjusting for inflation since 2014, the cost of BD/DR plan testing ranges from approximately $31,000 to $76,000 per year, per member or participant. The aggregate annual cost for designated members and participants to participate in BC/DR testing is approximately $84.0 million after adjusting for inflation since 2014.

Because SCI entities have an incentive to limit the imposition of the cost and burden associated with testing to the minimum necessary to comply with the rule, given the option, most SCI entities would likely, in the exercise of reasonable discretion, prefer to designate the fewest number of members, participants, or third-party providers to participate in testing and meet the requirements of the rule, than to designate more.

The Commission believes that the cost associated with Rule 1004 is unlikely to induce the designated members or participants to reduce the number of SCI entities through which they trade and adversely affect price competitiveness in markets. As noted above, the Commission also recognizes that costs to some SCI entity members, participants, or third-party providers associated with Rule 1004 could vary depending on the BC/DR plans being tested, and to the extent they participate. Based on industry sources, the Commission understands that most of the larger members or participants of SCI entities already maintain connectivity with the backup systems of SCI entities.[815] However, the Commission understands that there is a lower incidence of smaller members or participants maintaining connectivity with the backup sites of SCI entities. As such, the Commission believes that the compliance costs associated with Rule 1004 would be higher for those members, participants, or third-party providers that are designated for testing by SCI entities who would need to invest in additional infrastructure to participate in such testing.[816]

---

[815] SCI Adopting Release, *supra* note 1, at 72430.

[816] *Id*.

As discussed above, Rule 1001(a) does not require backup facilities of SCI entities fully duplicate the features of primary facilities.[817] Further as discussed in section IV.B.6, SCI entity members, participants, or third-party providers are not required by Regulation SCI to maintain the same level of connectivity with the backup sites of an SCI entity as they do with the primary sites. In the event of a wide-scale disruption in the securities markets, the Commission acknowledges that SCI entities and their members, participants, or third-party providers may not be able to provide the same level of service as on a normal trading day. However, when BC/DR plans are in effect due to a wide-scale disruption in the securities markets, the requirements of Rule 1004 should help ensure adequate levels of service and pricing efficiency, to facilitate trading and maintain fair and orderly markets without imposing excessive costs on SCI entities and market participants by requiring them to maintain the same connectivity with the backup systems as with the primary sites.[818]

**Request for comment:**

119. If you are a current or proposed SCI entity and you currently require any of your service providers to participate in your scheduled business continuity or disaster recovery testing, how does your activity differ from the requirements of the rule proposal? What have been the benefits and costs of this activity?

120. If you are a current or proposed SCI entity and your business continuity or disaster recovery plans address the unavailability of your third-party providers, how

---

[817] SCI Adopting Release, *supra* note 1, at 72353.

[818] *See id.*

does your activity differ from the requirements of the rule proposal? What have been the benefits and costs of this activity?

#### e. Rules 1005 through 1007—Recordkeeping and Electronic Filing

Rules 1005 through 1007 relate to recordkeeping requirements, filing and submission requirements, and requirements for service bureaus. SCI entities are required by Rule 1005 of Regulation SCI to make, keep, and preserve certain records related to their compliance with Regulation SCI.[819] Rule 1006 of Regulation SCI provides for certain requirements relating to the electronic filing on Form SCI, of any notification, review, description, analysis, or report to the Commission required to be submitted under Regulation SCI.[820] Rule 1007 of Regulation SCI requires a written undertaking when records are required to be filed or kept by an SCI entity under Regulation SCI, or are prepared or maintained by a service bureau or other recordkeeping service on behalf of the SCI entity.[821]

Rule 1005(c) currently requires that the recordkeeping period survives even if an SCI entity ceases to do business or ceases to be registered under the Exchange Act. The Commission proposes to amend Rule 1005(c) so that this record retention provision also applies to an SCI entity that remains in business as a registered entity but "otherwise [ceases] to be an SCI entity." Therefore, for existing SCI entities, this is the only difference from the current recordkeeping requirement in Rule 1005(c). For new SCI

---

819 *See* 17 CFR 242.1005. Rule 1005(a) of Regulation SCI relates to recordkeeping provisions for SCI SROs, whereas Rule 1005(b) relates to the recordkeeping provision for SCI entities other than SCI SROs.

820 *See* 17 CFR 242.1006.

821 *See* 17 CFR 242.1007.

entities, all of the requirements in Rules 1005 through 1007 are new obligations. We discuss below the benefits and costs of applying these provisions to new and existing SCI entities.

**i. Benefits**

The Commission believes that Rules 1005 and 1007 would allow Commission staff to inspect and examine the new SCI entities for their compliance with Regulation SCI, and would increase the likelihood that Commission staff can identify conduct inconsistent with Regulation SCI. Preserved information should provide the Commission with an additional source to help determine the causes and consequences of one or more SCI events and better understand how such events may have impacted trade execution, price discovery, liquidity, and investor participation. Consequently, the Commission believes that the requirements of Rules 1005 and 1007 would help ensure compliance of the new SCI entities with Regulation SCI and help realize the potential benefits (*e.g.*, better pricing efficiency, price discovery, and liquidity flows) of the regulation.

Rule 1006 requires SCI entities to electronically file all written information to the Commission on Form SCI.[822] Rule 1006 would provide a uniform manner in which the Commission receives—and SCI entities provide—written notifications, reviews, descriptions, analyses, or reports required by Regulation SCI. Rule 1006 should add efficiency for the new SCI entities in drafting and submitting the required reports, and for the Commission in reviewing, analyzing, and responding to the information provided.

---

[822] Except for notifications submitted pursuant to Rule 1002(b)(1) and (3).

The Commission recognizes that all of the new SCI entities are currently subject to the Commission and other regulatory recordkeeping requirements.[823] However, records relating to Regulation SCI may not be specifically addressed in the recordkeeping requirements of certain rules. The benefits from the recordkeeping requirements in Rules 1005 and 1007 for the new SCI entities (and the costs, as discussed below), will therefore depend on the extent to which their current operations already align with the rule's requirements, given both existing regulation and current practice.

The proposed amendment to Rule 1005(c) will apply to new and existing SCI entities. Although many SCI events may be resolved in a short time frame, there may be other SCI events that may not be discovered for an extended period of time after their occurrences, or may take significant periods of time to fully resolve. In such cases, having an SCI entity's records available after it has ceased to be an SCI entity or be registered under the Exchange Act would add to the scope of historical records available for review in the event of an SCI event. This is a particular issue for entities whose coverage under the rule might vary over time, depending on when the entities—or their systems—meet the rule's coverage thresholds. For these entities, uniform record retention periods will also facilitate comparative review of risk and compliance trends. These benefits will be limited if entities and systems of entities tend to continue meeting coverage requirements over time, without a break in coverage.

**ii. Costs**

The recordkeeping requirements of Rules 1005 and 1007 will impose additional costs, including a one-time cost to set up or modify an existing recordkeeping system to

---

[823] *See, e.g.*, 17 CFR 240.17a-3 and 240.17a-4, applicable to broker-dealers.

comply with Rules 1005 and 1007. The initial and ongoing compliance costs associated with the recordkeeping requirements are attributed to paperwork burdens, which are discussed in section IV above.[824]

With respect to Rule 1006, all costs associated with Form SCI are attributed to the paperwork burdens discussed in section IV. For existing SCI entities the Commission estimates approximately $21.0 million in initial costs and $12.0 million in annual costs, while for new SCI entities the Commission estimates approximately $41.7 million in initial costs and $25.8 million in annual costs.[825]

Every new SCI entity will be required to have the ability to electronically submit Form SCI through the EFFS system, and every person designated to sign Form SCI will be required to have an electronic signature and a digital ID. The Commission believes that this requirement will not impose an additional burden on new SCI entities, as these entities likely already prepare documents in an electronic format that is text searchable or can readily be converted into a format that is text searchable.

The Commission also believes that many new SCI entities currently have the ability to access the EFFS system and electronically submit Form SCI, such that the requirement to submit Form SCI electronically will not impose significant new

---

824 When monetized, the paperwork burden associated with all recordkeeping requirements would result in approximately $278,460 initially and $40,950 annually for all new SCI entities in the aggregate. The Commission estimates that a New SCI Entity other than an SCI SRO will incur a one-time cost of $900 for information technology costs for purchasing recordkeeping software, for a total of $18,900. *See* section IV.D.7. For purposes of this Economic Analysis, there is two fewer entities than under the PRA analysis, lowering these estimated costs. *See supra* note 700.

825 *See* section IV.D.7; *supra* note 700.

implementation or ongoing costs.[826] The Commission also believes that some of the persons who will be designated to sign Form SCI already have digital IDs and the ability to provide an electronic signature. To the extent that some persons do not have digital IDs, the additional cost to obtain and maintain digital IDs is accounted for in the paperwork burden, discussed in section IV above.[827]

### D. Efficiency, Competition, and Capital Formation Analysis

As previously discussed in section C, the proposed amendments to Regulation SCI would reduce the impact of market disruptions arising as a result of natural disasters, third-party provider service outages, cybersecurity events, hardware or software malfunctions. We expect that the proposed amendments will reduce the frequency, severity, and duration of systems issues that occur in the context of these events, and will thus decrease the number of trading interruptions. The proposed amendments will thus improve market efficiency, price discovery, and liquidity, because trading interruptions interfere with the process through which information gets incorporated into security prices. In addition, by reducing trading interruptions, the proposed amendments will have beneficial effects across markets, because of the interconnectedness of securities markets. For example, an interruption in the market for equity securities could harm the price discovery process in the options markets, reducing the flow of liquidity across markets. As a result, we expect the proposed amendments, if adopted, would improve price efficiency in securities markets.[828]

---

826 The initial and ongoing costs associated with various electronic submissions of Form SCI for the new SCI entities are discussed in the Paperwork Reduction Act section above. *See supra* section IV.D.6.

827 *See id.*

828 *See* sections V.D.1 and V.D.3.

Prices that accurately convey information about fundamental value improve the efficiency with which capital is allocated across projects and firms, thus promoting capital formation. In addition, we expect the proposed amendments to encourage capital formation by reinforcing investors' confidence in market transactions.

The proposed amendments to Regulation SCI could affect competition among SCI entities because the compliance costs could differ among SCI entities. For example, current SCI entities are expected to face smaller incremental compliance costs than new SCI entities. New SCI entities that have been subject to similar regulations could also face smaller incremental compliance costs than those who have not. Even among new SCI entities, certain provisions can be more costly for some than others. For example, the initial compliance costs of the systems resumption requirements could differ among new SCI entities. Specifically, as mentioned above, Rule 1004's BC/DR testing requirements may require greater incremental costs for smaller SCI entities that have not already been engaged in BC/DR testing. Lastly, some of the new SCI entities may already have practices that are aligned with at least some of the requirements under amended Regulation SCI compared to the baseline, reducing their incremental compliance costs.

In addition to competition among SCI entities, the compliance costs imposed by the proposed amendments to Regulation SCI could have an effect on competition where SCI entities and non-SCI entities compete, such as in the markets for trading services (*e.g.*, broker-dealers). Specifically, since non-SCI entities do not have to incur the compliance costs associated with Regulation SCI, SCI entities could find it difficult to pass on their own compliance costs to investors or customers without losing investors or customers to non-SCI entities. This would adversely affect the profits of SCI entities.

That said, by expanding the set of SCI entities, the proposed amendments would ensure that, where there is currently competition between existing SCI entities and the new entities under this proposed rule then these competing entities are subject to similar SCI compliance requirements.

The proposed threshold-based tests for scoping a broker-dealer into Regulation SCI could bring about a potential unintended effect of deterring growth among broker-dealers and discouraging potential benefits of scale economies. For example, to the extent a certain broker-dealer may take otherwise-unwanted steps to keep its trading volumes or asset level low, or spin off entities and not realize scale economies, all for the purpose of avoiding being subject to regulation, this can be inefficient for the economy. Likewise, the proposal to apply regulation SCI to all exempt clearing agencies would mean that any entity that seeks to become a clearing agency will automatically be subject to Regulation SCI and will thus bear the associated compliance cost.

The compliance costs associated with Rule 1004 could raise barriers to entry and affect competition among members or participants of SCI entities. Specifically, to the extent that members or participants could be subject to designation in BC/DR plan testing and could incur additional compliance costs, the member or participant designation requirement of Rule 1004 could raise barriers to entry. In addition, as discussed above, the compliance costs of the rule will likely be higher for smaller members or participants of SCI entities compared to larger members or participants of SCI entities. The adverse effect on competition may be mitigated to some extent, as the most likely members or participants to be designated for testing are larger members or participants who already maintain connectivity with an SCI entity's backup systems. Further, the adverse effect on

competition for smaller members or participants could be partially mitigated to the extent that larger firms, which are members of multiple SCI entities, could incur additional compliance costs as these larger member firms could be subject to multiple designations for business continuity and disaster recovery plan testing.[829]

### E. Reasonable Alternatives

In formulating our proposal, we have considered various alternatives. Those alternatives are discussed below and we have also requested comments on certain of these alternatives.

#### 1. Limiting the Scope of the Regulation SCI Provisions for New SCI Entities

The Commission has considered whether all of the obligations set forth in Regulation SCI should apply to the new SCI entities or whether only certain requirements should be imposed, such as those requiring written policies and procedures, notification of systems problems, business continuity and disaster recovery testing, and penetration testing.[830] For example, the Commission has considered if SBSDRs should be subject to full Regulation SCI requirements, similar to SCI plan processors, or should be subject to only some of the Regulation SCI requirements, given differing levels of automation and stages of regulatory development of the SBS market.

The Commission believes that these alternatives would reduce some of the benefits as well as some of the costs compared to the proposed rules. The lower costs

---

829 *Id*. at 72433.

830 Such an approach is similar to that taken regarding the competing consolidators in Market Data Consolidator rule. The Market Data Consolidator rule subjects competing consolidators that do not meet the earning thresholds to some, but not all, obligations that apply to competing consolidators. 17 CFR 242.614.

from limiting the Regulation SCI requirements, such as periodic reviews of policies and procedures or Commission notification, for some new entities could result in lower barriers to entry and could increase competition in the relevant markets compared to the proposed rules. However, taking into consideration the large size of the new SCI entities and, therefore, their externalities on some other SCI entities in case of system failure, the Commission believes these effects on the competition may not be significant enough to warrant forgoing benefits (such as timely notifications to the Commission) in addition to the reduced effectiveness of the regulation. Moreover, not requiring specific SCI requirements for certain new SCI entities would likely result in less uniform treatment across current and new SCI entities performing similar functions.[831]

### 2. Mandating Compliance with Current SCI Industry Standards

The Commission has considered the alternative of mandating compliance with current SCI industry standards. This alternative would require that the policies and procedures of SCI entities required under Rule 1001(a) comply with "current SCI industry standards" rather than simply making such compliance a safe harbor under Rule 1001(a)(4).[832] This alternative would ensure that an SCI entity have policies and procedures consistent with current SCI industry standards. These standards likely have the advantage of economy of scale as several entities in that industry adopted the standards and thus the standards benefit from more innovative efficiencies than in-house

---

831 *See supra* section III.A.2.

832 Proposed Rule 1000(a)(4) defines "current SCI industry standards" as "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."

standards. Moreover, mapping policies and procedures to the industry standard would help facilitate the Commission's inspection and enforcement capabilities.

Based on Commission staff experience, however, this alternative would not be an appropriate solution for all SCI entities. One reason is that given the differences exhibited by various SCI entities and the complexity of each SCI entity's operations, it may not be suitable for each one to find a current SCI industry standard that suits its needs without substantial modification and customization. To this extent, the Commission sees a great value in allowing each SCI entity to customize its policies and procedures to address the specific operational risks it faces. It is the Commission's understanding that a number of current SCI entities have developed and implemented policies and procedures largely based on industry standards, but they have also customized them based on the size, risks, and unique characteristics of SCI entities. For this reason, mandating compliance with a current SCI industry standard may be an inefficient approach. For the larger and more complex-structured SCI entities, losing flexibility to design systems or develop policies and procedures by mandating the industry standards could also result in less effective policies and procedures or adversely affect integrity, resiliency, availability, or security of SCI systems.

### 3. Requiring Diversity of Back-Up Plan Resources

With respect to critical SCI systems, the Commission has considered mandating multi-vendor backups. This alternative would require that SCI entities that utilize third-party providers to operate critical SCI systems have geographically diverse backup systems that are operated by a different third-party provider (*e.g.*, multi-cloud). As previously discussed, there can be significant advantages for an entity moving its systems from an on-premises, internally run data center to cloud service providers (CSPs), which

may include cost efficiencies, automation, increased security, and resiliency, and the ability to leverage the opportunity to reengineer or otherwise update their systems and applications to run more efficiently.[833]

However, each SCI entity is obligated to satisfy the requirements of Regulation SCI for systems operated on behalf the SCI entity by a third party. This necessarily requires an individualized assessment of the costs and risks associated with managing the CSP relationship, and determining that the CSPs' backup and recovery capabilities are sufficiently resilient, geographically diverse, and reasonably designed to achieve timely recovery following a wide-scale disruption.[834] Further, while reducing the risk of over-reliance on a single vendor and the chance of system failures–for example, due to the same vulnerabilities within a vendor—a multi-cloud strategy would add additional costs including negotiation, contract, deployment, and management costs; and it is the Commission's understanding that multi-cloud architecture could introduce more complexity and, accordingly, operational and cybersecurity risks into the SCI back-up systems.[835] In place of a prescriptive alternative of mandating multi-vendor backups, the Commission is proposing, in Rule 1001(a)(2)(v) and (ix), a more flexible approach under which each SCI entity must consider CSPs and other third-party providers as part of a risk-based assessment of the providers' criticality and their role in the entity's business continuity and disaster recovery planning.

---

833 *See* section III.C.2.

834 *See id*.

835 For example, security breach possibilities could increase because of the interconnection of SCI systems between multi cloud providers.

#### 4. Penetration Testing Frequency

With respect to the penetration testing frequency, the Commission has considered requiring longer (*e.g.*, every 2 years) or shorter (quarterly, every 6 months) frequencies for penetration testing, rather than the currently proposed annual (a reduction from the current rule of every three years). When the Commission adopted Regulation SCI in 2014, the Commission decided to require penetration test reviews "not less than once every three years in recognition of the potentially significant costs that may be associated with the performance of such tests."[836] Nevertheless, as mentioned above, markets have changed since the adoption of Regulation SCI. In particular, cybersecurity has become a more pervasive concern for all types of businesses, including SCI entities. In addition, the Commission understands that industry practices with respect to penetration testing has evolved such that tests occur on a much more frequent basis, as businesses confront the threat of cybersecurity events on a wider scale. To this extent, the Commission has considered whether penetration testing should be conducted at least once quarterly, every 6 months, or every 2 years.

The Commission understands industry practices generally tend to recommend at least one penetration test review a year. Requiring penetration test reviews more frequently could further strengthen security and reduce cybersecurity events at SCI entities. Nevertheless, the Commission believes that requiring all SCI entities to conduct such reviews more than once every year may be too much of a drain on the institution's resources, due to the estimated cost of $10,000 to $30,000 per test,[837] and given the wide

---

[836] SCI Adopting Release, *supra* note 1, at 72344.

[837] *See* section V.D.3.c.

scope of annual testing to be conducted as part of an annual review under proposed Rule 1003(b).[838] Moreover, while some entities may need to perform multiple tests each year on different components of their environment, for other entities a requirement for multiple tests may be counterproductive, if the testing cycle does not provide time to implement security investments.

### 5. Attestation for Critical SCI System Vendors

Given the importance of critical SCI systems and SCI entities' increasing reliance on third-party providers, the Commission has considered requiring attestation (such as by an SCI entity's chief executive officer or general counsel) that contracts with third-party providers for critical SCI systems comply with the SCI entity's obligations under Regulation SCI. Such an attestation requirement would further ensure that SCI entities are negotiating contract terms with third-party providers for critical SCI systems in a manner that is consistent with Regulation SCI's requirements. However, an attestation requirement for each such contract may have limited value, and may be overly time-consuming and resource-intensive, relative to the value of the attestation requirement.

The value of an attestation requirement will be limited, given that proposed Rule 1001(a)(2)(ix) would require each SCI entity to have a program to manage and oversee third-party providers, or to the extent that they already provide attestations to their customers (which, in turn, may vary to the degree that they are in competition with like entities). At the same time, an attestation requirement may have significant costs.

---

838 *See* proposed Rules 1000, 1001(a)(2)(iv) (penetration testing as part of an annual review under Rule 1003(b) must include testing of "network, firewalls, and production systems, including of any vulnerabilities of . . . SCI systems and indirect SCI systems," including vulnerabilities "pertaining to internal and external threats, physical hazards, and natural or manmade disasters").

For SCI entities these costs may include the direct costs of updating their oversight processes in order to ensure that their attestations are accurate and in compliance; training their in-house personnel on the third-party service provider's methods for operating critical IT systems; and conducting oversight of the service provider's subcontractors as well as oversight of the service provider itself. SCI entities may also incur costs if they move critical system functions in-house or consolidate vendors to reduce the risk or burden of the attestation requirement, which could result in lower-quality or less efficient services. Furthermore, requiring the attestation by SCI entity's senior officers could increase the due diligence cost of the attestation requirement. Senior officers making attestations may require additional liability insurance, higher compensation or lower incentive pay as a share of overall compensation. Finally, the service providers themselves may face increased costs as part of their efforts to help the SCI entity make the relevant attestation, including contract renegotiation costs, upgrading operations, and responding to information requests from the SCI entity. These costs, in turn, might be passed to the SCI entity and ultimately to its participants, members, or customers.

The Commission believes the additional costs could be disproportionate to the benefits of an attestation requirement. For these reasons, the Commission has decided against including an attestation requirement.

**6. Transaction Activity Threshold for SCI Broker-dealers**

With respect to the transaction activity threshold used to scope broker-dealers within Regulation SCI as discussed in section III.A.2.b, the Commission has considered as an alternative whether to set a higher (more limited) or lower (more expansive) threshold than the proposed 10% threshold. For example, the Commission has considered

if only broker-dealers with transaction activity thresholds above 15% should be included as SCI broker-dealers[839] but determined that this would fail to scope within Regulation SCI some of the largest and most significant broker-dealers that pose technological vulnerabilities and risks to the maintenance of fair and orderly markets. This would have the effect of decreasing costs moderately for broker-dealers no longer within the scope of Regulation SCI at the expense of a significant decrease in benefits otherwise associated with the improvements to fair and orderly markets, as described above.

Similarly, the Commission has also considered whether all broker-dealers with transaction activity thresholds above 5% should be included as SCI broker-dealers,[840] but determined that this would scope within Regulation SCI several broker-dealers that are not among the most significant broker-dealers that pose technological vulnerabilities and risks to the maintenance of fair and orderly markets. This would have the effect of

---

839 The Commission believes that the proposed threshold of 5% of total assets is a reasonable approach to identifying the largest broker-dealers. *See* section III.A.2.b.iii (discussing proposed thresholds for an "SCI broker-dealer"). The Commission has considered as an alternative to further scope in the broker-dealers with transaction activity thresholds above 15%. Regulation SCI would only be applicable to an estimated ten broker-dealers based on the analysis of data which include broker-dealer FOCUS Report Form X-17A-5 Schedule II filings from Q4 2021 to Q3 2022. Also for additional detail on the calculation of total assets of all security broker-dealers, *see supra* note 127. Data also include Consolidated Audit Trail (CAT) data from Jan. 2022 to June 2022, the plan processors (SIPs) of the CTA/CQ Plans and Nasdaq UTP Plan. CTA Plan, *available at* https://www.ctaplan.com; Nasdaq UTP Plan, *available at* https://www.utpplan.com, Options Price Reporting Authority (OPRA) data, TRACE for Treasury Securities data from Jan. 2022 to June 2022, regulatory TRACE data from Jan. 2022 to June 2022, and FINRA TRACE.

840 The Commission believes that the proposed threshold of 5% of total assets is a reasonable approach to identifying the largest broker-dealers. *See* section III.A.2.b.iii (discussing proposed thresholds for an "SCI broker-dealer"). The Commission has considered as an alternative to further scope in the broker-dealers with transaction activity thresholds above 5%. Regulation SCI would only be applicable to an estimated 29 broker-dealers based on the analysis of data which include broker-dealer FOCUS Report Form X-17A-5 Schedule II filings from Q4 2021 to Q3 2022. Also for additional detail on the calculation of total assets of all security broker-dealers, *see supra* note 127. Data also include Consolidated Audit Trail (CAT) data from Jan. 2022 to June 2022, the plan processors (SIPs) of the CTA/CQ Plans and Nasdaq UTP Plan. CTA Plan, *available at* https://www.ctaplan.com; Nasdaq UTP Plan, *available at* https://www.utpplan.com, Options Price Reporting Authority (OPRA) data, TRACE for Treasury Securities data from Jan. 2022 to June 2022, regulatory TRACE data from Jan. 2022 to June 2022, and FINRA TRACE.

increasing costs for marginal firms without a comparable increase in benefits associated with an improvement of fair and orderly markets.

In addition, with respect to the transaction activity threshold used to scope broker-dealers within Regulation SCI as discussed in section III.A.2.b, the Commission has also considered as an alternative whether to apply the proposed 10% threshold to principal trades only, rather than all transactions. Accordingly, the Commission considered whether to include as an SCI entity any registered broker-dealer that, irrespective of the size of its balance sheet, consistently trades for its own account at a substantially high level in certain enumerated asset classes, scaled as a percentage of total average daily dollar volume, as reported by applicable reporting organizations. Under the alternative, ten broker-dealer firms[841] would have been scoped in as "SCI broker-dealers," which are among the 17 "SCI broker-dealers" subject to the proposed Regulation SCI.

This alternative approach to the transaction activity threshold would identify those broker-dealers that generate significant liquidity in specified types of securities markets and could also be considered a proxy for those that also engage in substantial agency trading and other business. Because the alternative would also scope in fewer broker-dealers as SCI entities, this alternative would also impose fewer total costs compared to the proposed approach.

---

[841] The estimated ten broker-dealer firms are based on the analysis of data which include broker-dealer FOCUS Report Form X-17A-5 Schedule II filings from Q4 2021 to Q3 2022. Also for additional detail on the calculation of total assets of all security broker-dealers, *see supra* note 127. Data also include Consolidated Audit Trail (CAT) data from Apr. 2022 to Sept. 2022, the plan processors (SIPs) of the CTA/CQ Plans and Nasdaq UTP Plan. CTA Plan, *available at* https://www.ctaplan.com; Nasdaq UTP Plan, *available at* https://www.utpplan.com, Options Price Reporting Authority (OPRA) data, TRACE for Treasury Securities data from Apr. 2022 to Sept. 2022, regulatory TRACE data from Apr. 2022 to Sept. 2022, and FINRA TRACE.

However, the Commission preliminarily believes that limiting the extension of Regulation SCI to broker-dealers that engage in significant trading activity for their own account in one or more of the enumerated asset classes and generate significant liquidity on which fair and orderly markets rely would fail to acknowledge the substantial role that executing brokers acting as agents also play in the markets. Accordingly, the alternative approach would fail to scope within Regulation SCI some of the largest and most significant broker-dealers that pose technological vulnerabilities and risks to the maintenance of fair and orderly markets. In the Commission's view, using all transaction activity rather than limiting the analysis to principal trades is a more appropriate measure for estimating the significance of a broker-dealer's footprint in the markets and the effect that its sudden unavailability could have on the fair and orderly market functioning.

Thus, while the alternative would likely scope in fewer broker-dealers as SCI entities, and thus reduce the aggregate costs of extending Regulation SCI, compared to the proposal, it would also limit the extensive benefits, discussed above, associated with applying Regulation SCI to additional broker-dealers that play a critical role in the market.

#### 7. Limitation on Definition of "SCI Systems" for SCI Broker-Dealers

Additionally, the Commission considered leaving the original definition of "SCI systems" unrevised such that any broker-dealer that were to only meet or exceed the trading activity threshold of 10% for any asset class would have been subject to Regulation SCI requirements for all of its systems, not only those systems with respect to the type of securities for which an SCI broker-dealer satisfies the trading activity threshold. Leaving the definition unrevised would scope in SCI broker-dealer systems

with respect to classes of securities with a lower volume of trading, for which system unavailability is less likely to pose a risk to the maintenance of fair and orderly markets. This would have the effect of increasing costs for SCI broker-dealers with limited trading activity in one or more other cases of securities, while yielding a potential benefit in terms of risk reduction with respect to the maintenance of fair and orderly markets.

## VI. Regulatory Flexibility Act Certification

The Regulatory Flexibility Act ("RFA")[842] requires Federal agencies, in promulgating rules, to consider the impact of those rules on small entities. Section 603(a)[843] of the Administrative Procedures Act,[844] as amended by the RFA, generally requires the Commission to undertake a regulatory flexibility analysis of all proposed rules, or proposed rule amendments, to determine the impact of such rulemaking on "small entities."[845] Section 605(b) of the RFA states that this requirement shall not apply to any proposed rule or proposed rule amendment which, if adopted, would not have a significant economic impact on a substantial number of small entities.[846]

### A. "Small Entity" Definitions

For purposes of Commission rulemaking in connection with the RFA, a small entity includes an exchange that has been exempt from the reporting requirements of

---

842 5 U.S.C. 601 *et seq.*

843 5 U.S.C. 603(a).

844 5 U.S.C. 551 *et seq.*

845 Although section 601(b) of the RFA defines the term "small entity," the statute permits agencies to formulate their own definitions. The Commission has adopted definitions for the term "small entity" for purposes of Commission rulemaking in accordance with the RFA. Those definitions, as relevant to this proposed rulemaking, are set forth in 17 CFR 240.0-10 ("Rule 0-10").

846 *See* 5 U.S.C. 605(b).

Rule 601 under Regulation NMS, and is not affiliated with any person (other than a natural person) that is not a small business or small organization. A small entity also includes a broker-dealer with total capital (net worth plus subordinated liabilities) of less than $500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to 17 CFR 240.17a-5(d) ("Rule 17a–5(d)" under the Exchange Act),[847] or, if not required to file such statements, a broker-dealer with total capital (net worth plus subordinated liabilities) of less than $500,000 on the last business day of the preceding fiscal year (or in the time that it has been in business, if shorter); and is not affiliated with any person (other than a natural person) that is not a small business or small organization. Furthermore, a small entity includes a securities information processor that: (1) had gross revenues of less than $10 million during the preceding fiscal year (or in the time it has been in business, if shorter); (2) provided service to fewer than 100 interrogation devices or moving tickers at all times during the preceding fiscal year (or in the time that it has been in business, if shorter); and (3) is not affiliated with any person (other than a natural person) that is not a small business or small organization under 17 CFR 240.0-10.[848] A small entity additionally includes a clearing agency that (1) Compared, cleared and settled less than $500 million in securities transactions during the preceding fiscal year (or in the time that it has been in business, if shorter); (2) had less than $200 million of funds and securities in its custody or control at all times during the preceding fiscal year (or in the time that it has been in business, if shorter); and (3) is not

---

847 17 CFR 240.17a-5(d).

848 17 CFR 240.0-10(g).

affiliated with any person (other than a natural person) that is not a small business or small organization as defined in 17 CFR 240.0-10.[849]

### B. Current SCI Entities

Currently, SCI entities comprise SCI SROs, SCI ATSs, plan processors, SCI competing consolidators, and certain exempt clearing agencies. The Commission believes that none of these entities would be considered small entities for purposes of the RFA.

#### 1. SCI SROs

As discussed in section II.B.1 above, Regulation SCI currently applies to SCI SROs, which is defined as any national securities exchange, registered securities association, or registered clearing agency, or the Municipal Securities Rulemaking Board; *provided however*, that for purposes of 17 CFR 242.1000, the term SCI self-regulatory organization shall not include an exchange that is notice registered with the Commission pursuant to 15 U.S.C. 78f(g) or a limited purpose national securities association registered with the Commission pursuant to 15 U.S.C. 78*o*-3(k).[850] Currently, there are 35 SCI SROs.

Based on the Commission's existing information about the entities that are subject to proposed Regulation SCI, the Commission believes that SCI SROs would not fall within the definition of "small entity" as described above.

As stated, the Commission has defined a "small entity" as an exchange that has been exempt from the reporting requirements of Rule 601 of Regulation NMS and is not affiliated with any person (other than a natural person) that is not a small business or

---

[849] 17 CFR 240.0-10(d).

[850] *See* 17 CFR 242.1000.

small organization.[851] None of the national securities exchanges registered under section 6 of the Exchange Act that would be subject to the proposed rule and form is a "small entity" for purposes of the RFA.

There is only one national securities association (FINRA), and the Commission has previously stated that it is not a small entity as defined by 13 CFR 121.201.[852]

As stated, a small entity includes, when used with reference to a clearing agency, a clearing agency that: (1) compared, cleared, and settled less than $500 million in securities transactions during the preceding fiscal year; (2) had less than $200 million of funds and securities in its custody or control at all times during the preceding fiscal year (or at any time that it has been in business, if shorter); and (3) is not affiliated with any person (other than a natural person) that is not a small business or small organization.[853]

Based on the Commission's existing information about the clearing agencies currently registered with the Commission, the Commission preliminarily believes that such entities exceed the thresholds defining "small entities" set out above. While other clearing agencies may emerge and seek to register as clearing agencies, the Commission preliminarily does not believe that any such entities would be "small entities" as defined in Exchange Act Rule 0-10.

### 2. The MSRB

The Commission's rules do not define "small business" or "small organization" for purposes of entities like the MSRB. The MSRB does not fit into one of the categories

---

851 *See* paragraph (e) of Rule 0-10.

852 *See, e.g.*, Securities Exchange Act Release No. 62174 (May 26, 2010), 75 FR 32556, 32605 n.416 (June 8, 2010) ("FINRA is not a small entity as defined by 13 CFR 121.201.").

853 *See* paragraph (d) of Rule 0-10.

listed under the Commission rule that provides guidelines for a defined group of entities to qualify as a small entity for purposes of Commission rulemaking under the RFA.[854] The RFA in turn, refers to the Small Business Administration ("SBA") in providing that the term "small business" is defined as having the same meaning as the term "small business concern" under section 3 of the Small Business Act.[855] The SBA provides a comprehensive list of categories with accompanying size standards that outline how large a business concern can be and still qualify as a small business.[856] The industry categorization that appears to best fit the MSRB under the SBA table is Professional Organization. The SBA defines a Professional Organization as an entity having average annual receipts of less than $15 million. Within the MSRB's 2021 Annual Report the organization reported total revenue exceeding $35 million for fiscal year 2021.[857] The Report also stated that the organization's total revenue for fiscal year 2020 exceeded $47 million.[858] The Commission is using the SBA's definition of small business to define the MSRB for purposes of the RFA and has concluded that the MSRB is not a "small entity."

### 3. SCI ATSs

As discussed in section II.B.1 above, Regulation SCI currently applies to SCI ATSs (which are required to be registered as broker-dealers) that during at least four of

---

854 *See* Rule 0-10.

855 *See* 5 U.S.C. 601(3).

856 *See* 13 CFR 121.201. *See also* SBA, Table of Small Business Size Standards Marched to North American Industry Classification System Codes, *available at* https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf (outlining the list of small business size standards within 13 CFR 121.201).

857 *See* MSRB, 2021 Annual Report, 16, *available at* https://msrb.org/-/media/Files/Resources/MSRB-2021-Annual-Report.ashx.

858 *Id*.

the preceding six calendar months: (1) Had with respect to NMS stocks: (i) Five percent (5%) or more in any single NMS stock, and one-quarter percent (0.25%) or more in all NMS stocks, of the average daily dollar volume reported by applicable transaction reporting plans, which represents the sum of all reported bought and all reported sold dollar volumes; or (ii) One percent (1%) or more in all NMS stocks of the average daily dollar volume reported by applicable transaction reporting plans, which represents the sum of all reported bought and all reported sold dollar volumes; or (2) Had with respect to equity securities that are not NMS stocks and for which transactions are reported to a self-regulatory organization, five percent (5%) or more of the average daily dollar volume as calculated by the self-regulatory organization to which such transactions are reported. All NMS stock and non-NMS stock ATSs are required to register as broker-dealers.

There are seven SCI ATS currently. As stated, a small entity also includes a broker-dealer with total capital (net worth plus subordinated liabilities) of less than $500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to Rule 17a–5(d) under the Exchange Act,[859] or, if not required to file such statements, a broker-dealer with total capital (net worth plus subordinated liabilities) of less than $500,000 on the last business day of the preceding fiscal year (or in the time that it has been in business, if shorter); and is not affiliated with any person (other than a natural person) that is not a small business or small organization. Applying this test for broker-dealers, the Commission believes that none of the SCI ATSs currently trading were operated by a broker-dealer that is a "small entity."

---

[859] 17 CFR 240.17a-5(d).

*Plan Processors*

As discussed in section II.B.1 above, Regulation SCI currently applies to plan processors, which are "any self-regulatory organization or securities information processor acting as an exclusive processor in connection with the development, implementation and/or operation of any facility contemplated by an effective national market system plan."[860] Currently, there are two plan processors subject to Regulation SCI.

The current plan processors are SIAC a subsidiary of NYSE Group, Inc., and Nasdaq Stock Market LLC, a subsidiary of Nasdaq, Inc. In addition, even if other entities do become plan processors, the Commission preliminarily believes that most, if not all, plan processors would be large business entities or subsidiaries of large business entities, and that every plan processor (or its parent entity) would have gross revenues in excess of $10 million and provide service to 100 or more interrogation devices or moving tickers. Therefore, the Commission preliminarily believes that none of the current plan processors or potential plan processors would be considered small entities.

*SCI Competing Consolidators*

As discussed in section II.B.1 above, Regulation SCI currently applies to SCI competing consolidators. While no SCI competing consolidators have yet to register, as discussed in the adopting release for the Market Data Infrastructure rule, the Commission estimates, and continues to estimate, that up to 10 entities will register as competing consolidators.[861]

---

[860] *See* 17 CFR 242.1000; 17 CFR 242.600(b)(67).

[861] *See* Market Data Infrastructure Adopting Release, *supra* note 24, at 18808.

As discussed in the Market Data Infrastructure final rule, "based on the Commission's information about the 10 potential entities the Commission estimates may become competing consolidators, the Commission believes that all such entities will exceed the thresholds defining 'small entities' set out above."[862] The Commission continues to believe this analysis is accurate, and that "[c]ompeting consolidators will be participating in a sophisticated business that requires significant resources to compete effectively."[863] Accordingly, the Commission believes that any such registered competing consolidators will exceed the thresholds for "small entities" set forth in 17 CFR 240.0-10.

*Exempt Clearing Agencies*

As discussed in section II.B.1 above, Regulation SCI currently applies to certain clearing agencies, specifically, exempt clearing agencies subject to ARP. There are currently 3 exempt clearing agencies subject to Regulation SCI, and the Commission estimates that Regulation SCI will apply to two more if the proposed rules are finalized. The Commission believes that all the clearing agencies, both those to which Regulation SCI currently applies and those to which it will, exceed the thresholds defining 'small entities' set out above.

### C. Proposed SCI Entities

The proposed expansion of the definition of the term "SCI entity" would include SBSDRs and SCI broker-dealers, as well as additional clearing agencies exempted from registration. The Commission preliminarily believes that none of these would be considered small entities for purposes of the RFA.

---

862 *Id.*

863 *Id.* at 18808–09.

### 1. SBSDRs

As discussed in section III.A.2.a above, in 2015, the Commission established a regulatory framework for SBSDRs, under which SBSDRs are registered securities information processors and disseminators of market data in the SBS market. There are currently two registered SBSDRs that would be subject to Regulation SCI.

The two currently registered SBSDRs are subsidiaries of large business entities.[864] In addition, even if other entities do register as SBSDRs, for purposes of Commission rulemaking, the Commission believes that none of the SBSDRs will be considered small entities.[865]

### 2. SCI Broker-dealers

As discussed in section III.A.2.b above, the proposed definition of an SCI broker-dealer would be a broker or dealer registered with the Commission pursuant to section 15(b) of the Exchange Act which: (1) in at least two of the four preceding calendar quarters, ending March 31, June 30, September 30, and December 31, reported to the Commission, on Form X-17A-5 (§ 249.617), total assets in an amount that equals five percent (5%) or more of the total assets of all security brokers and dealers; or (2) during

---

[864] *See supra* note 111.

[865] *See* SBSDR Adopting Release, *supra* note 96, 80 FR 14548-49 (providing that in the Proposing Release, the Commission stated that it did not believe that any persons that would register as SBSDRs would be considered small entities. The Commission stated that it believed that most, if not all, SBSDRs would be part of large business entities with assets in excess of $5 million and total capital in excess of $500,000. As a result, the Commission certified that the proposed rules would not have a significant impact on a substantial number of small entities and requested comments on this certification. The Commission did not receive any comments that specifically addressed whether 17 CFR 240.13n-1 through 240.13n-12 ("Rules 13n-1 through 13n-12") and Form SBSDR would have a significant economic impact on small entities. Therefore, the Commission continues to believe that Rules 13n-1 through 13n-12 and Form SBSDR will not have a significant economic impact on a substantial number of small entities. Accordingly, the Commission hereby certifies that, pursuant to 5 U.S.C. 605(b), Rules 13n-1 through 13n-12, Form SBSDR will not have a significant economic impact on a substantial number of small entities.).

at least four of the preceding six calendar months: (i) with respect to transactions in NMS stocks, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the average daily dollar volume reported by or pursuant to applicable effective transaction reporting plans, provided, however, that for purposes of calculating its activity in transactions effected otherwise than on a national securities exchange or on an alternative trading system, the broker-dealer shall exclude transactions for which it was not the executing party; or (ii) with respect to transactions in exchange-listed options contracts, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the average daily dollar volume reported by an applicable effective national market system plan; or (iii) with respect to transactions in U.S. Treasury Securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume made available by the self-regulatory organizations to which such transactions are reported; or (iv) with respect to transactions in Agency securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume made available by the self-regulatory organizations to which such transactions are reported.[866]

The Commission preliminarily estimates that 17 entities would satisfy one or more of these thresholds. Applying the test for broker-dealers stated above, the Commission believes that none of the potential SCI broker-dealers would be considered small entities.

---

[866] Such broker-dealer would not be required to comply with the requirements of Regulation SCI until six months after the SCI broker-dealer satisfied either threshold for the first time.

### 3. Exempt Clearing Agencies

For the purposes of Commission rulemaking, a small entity includes, when used with reference to a clearing agency, a clearing agency that: (1) compared, cleared, and settled less than $500 million in securities transactions during the preceding fiscal year; (2) had less than $200 million of funds and securities in its custody or control at all times during the preceding fiscal year (or at any time that it has been in business, if shorter); and (3) is not affiliated with any person (other than a natural person) that is not a small business or small organization.[867]

Based on the Commission's existing information about the clearing agencies currently exempted from registration with the Commission, the Commission preliminarily believes that such entities exceed the thresholds defining "small entities" set out above. While other clearing agencies may emerge and seek to register as clearing agencies, the Commission preliminarily does not believe that any such entities would be "small entities" as defined in Exchange Act Rule 0-10.

## D. Certification

For the foregoing reasons, the Commission certifies that the proposed amendments to Rules 1000, 1001, 1002, 1003, 1004, and 1005, and Form SCI if adopted, would not have a significant economic impact on a substantial number of small entities for purposes of the RFA.

The Commission invites commenters to address whether the proposed rules would have a significant economic impact on a substantial number of small entities, and, if so,

---

[867] *See* paragraph (d) of Rule 0-10.

what would be the nature of any impact on small entities. The Commission requests that commenters provide empirical data to support the extent of such impact.

**Statutory Authority**

Pursuant to the Exchange Act, 15 U.S.C. 78a *et seq*., and particularly, sections 2, 3, 5, 6, 11A, 13, 15, 15A, 17, 17A, and 23(a) thereof (15 U.S.C. 78b, 78c, 78e, 78f, 78k-1, 78m, 78o, 78o-3, 78q, 78q-1, and 78w(a)), the Commission proposes amendments to Regulation SCI under the Exchange Act and Form SCI under the Exchange Act, and to amend Regulation ATS under the Exchange Act, and 17 CFR parts 242 and 249.

**List of Subjects in 17 CFR Parts 242 and 249**

Brokers, Reporting and recordkeeping requirements, Securities.

For the reasons stated in the preamble, title 17, chapter II of the Code of Federal Regulations is proposed to be amended as follows:

**PART 242 – REGULATIONS M, SHO, ATS, AC, NMS, AND SBSR AND CUSTOMER MARGIN REQUIREMENTS FOR SECURITY FUTURES**

1. The authority citation for part 242 continues to read as follows:

**Authority**: 15 U.S.C. 77g, 77q(a), 77s(a), 78b, 78c, 78g(c)(2), 78i(a), 78j, 78k-1(c), 78l, 78m, 78n, 78o(b), 78o(c), 78o(g), 78q(a), 78q(b), 78q(h), 78w(a), 78dd-1, 78mm, 80a-23, 80a-29, and 80a-37.

2. Amend § 242.1000 by:

a. Adding in alphabetical order the definitions of "Agency Security" and "Exempt clearing agency";

b. Removing the definition of "Exempt clearing agency subject to ARP";

c. Adding in alphabetical order the definitions of "Registered security-based swap data repository" and "SCI broker-dealer";

d. Revising the definitions of "SCI entity", "SCI review", "SCI systems", and "Systems intrusion"; and

e. Adding in alphabetical order the definition of "U.S. Treasury Security".

The additions and revisions read as follows:

**§242.1000 Definitions.**

* * * * *

*Agency Security* means a debt security issued or guaranteed by a U.S. executive agency, as defined in 5 U.S.C. 105, or government-sponsored enterprise, as defined in 2 U.S.C. 622(8).

* * * * *

*Exempt clearing agency* means an entity that has received from the Commission an exemption from registration as a clearing agency under section 17A of the Exchange Act.

* * * * *

*Registered security-based swap data repository* means any security-based swap data repository, as defined in 15 U.S.C. 78c(a)(75), that is registered with the Commission pursuant to 15 U.S.C. 78m(n) and § 240.13n-1 of this chapter.

* * * * *

*SCI broker-dealer* means a broker or dealer registered with the Commission pursuant to section 15(b) of the Exchange Act, which:

(1) In at least two of the four preceding calendar quarters, ending March 31, June 30, September 30, and December 31, reported to the Commission, on Form X-17A-5 (§ 249.617 of this chapter), total assets in an amount that equals five percent (5%) or more

of the total assets of all security brokers and dealers. For purposes of this paragraph (1), *total assets of all security brokers and dealers* shall mean the total assets, as calculated and made publicly available by the Board of Governors of the Federal Reserve, or any subsequent provider of such information, for the associated preceding calendar quarter; or

(2) During at least four of the preceding six calendar months:

(i) With respect to transactions in NMS stocks, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the average daily dollar volume reported by or pursuant to applicable effective transaction reporting plans, provided, however, that for purposes of calculating its activity in transactions effected otherwise than on a national securities exchange or on an alternative trading system, the broker-dealer shall exclude transactions for which it was not the executing party;

(ii) With respect to transactions in exchange-listed options contracts, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the average daily dollar volume reported by an applicable effective national market system plan;

(iii) With respect to transactions in U.S. Treasury Securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume made available by the self-regulatory organizations to which such transactions are reported; or

(iv) With respect to transactions in Agency Securities, transacted average daily dollar volume in an amount that equals ten percent (10%) or more of the total average daily dollar volume made available by the self-regulatory organizations to which such transactions are reported.

(3) Provided, however, that such SCI broker-dealer shall not be required to comply with the requirements of Regulation SCI until six months after the end of the quarter in which the SCI broker-dealer satisfied paragraph (1) of this definition for the first time or six months after the end of the month in which the SCI broker-dealer satisfied paragraph (2) of this definition for the first time.

* * * * *

*SCI entity* means an SCI self-regulatory organization, SCI alternative trading system, plan processor, exempt clearing agency, SCI competing consolidator, SCI broker-dealer, or registered security-based swap data repository.

* * * * *

*SCI review* means a review, following established and documented procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems, and which review, using appropriate risk management methodology, contains:

(1) With respect to each SCI system and indirect SCI system of the SCI entity, assessments performed by objective personnel of:

(i) The risks related to the capacity, integrity, resiliency, availability, and security;

(ii) Internal control design and operating effectiveness, to include logical and physical security controls, development processes, systems capacity and availability, information technology service continuity, and information technology governance, consistent with industry standards; and

(iii) Third-party provider management risks and controls; and

(2) Penetration test reviews performed by objective personnel of the network, firewalls, and production systems, including of any vulnerabilities of its SCI systems and indirect SCI systems identified pursuant to § 242.1001(a)(2)(iv);

(3) *Provided, however,* that assessments of SCI systems directly supporting market regulation or market surveillance shall be conducted at a frequency based upon the risk assessment conducted as part of the SCI review, but in no case less than once every three years.

* * * * *

*SCI systems* means all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance; *provided, however,* that with respect to an SCI broker-dealer that satisfies only the requirements of paragraph (2) of the definition of "SCI broker-dealer," such systems shall include only those systems with respect to the type of securities for which an SCI broker-dealer satisfies the requirements of paragraph (2) of the definition.

* * * * *

*Systems intrusion* means any:

(1) Unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity;

(2) Cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system; or

(3) Significant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria.

*U.S. Treasury Security* means a security issued by the U.S. Department of the Treasury.

3. Amend § 242.1001 by revising paragraph (a) to read as follows:

**§242.1001 Obligations related to policies and procedures of SCI entities.**

(a) *Capacity, integrity, resiliency, availability, and security*. (1) Each SCI entity shall 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.

(2) Policies and procedures required by paragraph (a)(1) of this section shall include, at a minimum:

(i) The establishment of reasonable current and future technological 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; and that are reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity without which there would be a material impact on any of its critical SCI systems;

(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;

(vii) Monitoring of such systems to identify potential SCI events;

(viii) The maintenance of a written inventory and classification of all SCI systems, critical SCI systems, and indirect SCI systems as such, and a program with respect to the lifecycle management of such systems, including the acquisition, integration, support, refresh, and disposal of such systems, as applicable;

(ix) A program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for any such systems, including: initial and periodic review of contracts with such third-party providers for consistency with the SCI entity's obligations under Regulation SCI; and a risk-based assessment of each third-party provider's criticality to the SCI entity, including analyses of third-party

provider concentration, of key dependencies if the third-party provider's functionality, support, or service were to become unavailable or materially impaired, and of any potential security, including cybersecurity, risks posed;

(x) A program to prevent the unauthorized access to such systems and information residing therein; and

(xi) An identification of the current SCI industry standard(s) with which each such policy and procedure is consistent, if any.

(3) Each SCI entity shall periodically review the effectiveness of the policies and procedures required by this paragraph (a), and take prompt action to remedy deficiencies in such policies and procedures.

(4) For purposes of this paragraph (a), such policies and procedures shall be deemed to be reasonably designed if they are consistent with current SCI industry standards, which shall be composed 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. Compliance with such current SCI industry standards as a safe harbor, however, shall not be the exclusive means to comply with the requirements of paragraph (a) of this section.

* * * * *

4. Amend § 242.1002 by:

a. In paragraph (b)(4)(ii)(B), removing the words "or participants" and adding in their place "participants, or, in the case of an SCI broker-dealer, customers";

b. Revising paragraph (b)(5) and (c)(3);

c. In paragraph (c)(4)(i), removing the “or” after the semicolon;

d. In paragraph (c)(4)(ii), removing the period and adding in its place “; or”; and

e. Adding paragraph (c)(4)(iii).

The revision and additions read as follows:

**§ 242.1002 Obligations related to SCI events.**

* * * * *

(b) * * *

(5) The requirements of paragraphs (b)(1) through (4) of this section shall not apply to any systems disruption or systems compliance issue that has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants. For such events, each SCI entity shall:

(i) Make, keep, and preserve records relating to all such systems disruptions or systems compliance issues; and

(ii) Submit to the Commission a report, within 30 calendar days after the end of each calendar quarter, containing a summary description of such systems disruptions, including the SCI systems affected by such systems disruptions during the applicable calendar quarter.

(c) * * *

(3) The information required to be disseminated under paragraphs (c)(1) and (2) of this section promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event has occurred, shall be promptly disseminated by the SCI entity to those members, participants, or, in the case of an SCI broker-dealer, customers of the SCI entity that any responsible SCI personnel has reasonably estimated may have

been affected by the SCI event, and promptly disseminated to any additional members, participants, or, in the case of an SCI broker-dealer, customers that any responsible SCI personnel subsequently reasonably estimates may have been affected by the SCI event; *provided, however,* that for major SCI events, the information required to be disseminated under paragraphs (c)(1) and (2) of this section shall be promptly disseminated by the SCI entity to all of its members, participants, or, in the case of an SCI broker-dealer, customers.

(4) * * *

(iii) A systems intrusion that is a significant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity.

5. Amend §242.1003 by revising paragraph (b) to read as follows:

**§242.1003 Obligations related to systems changes; SCI review.**

* * * * *

(b) *SCI review.* Each SCI entity shall:

(1) Conduct an SCI review of the SCI entity's compliance with Regulation SCI not less than once each calendar year for each calendar year during which it was an SCI entity for any part of such calendar year;

(2) Submit a report of the SCI review required by paragraph (b)(1) of this section to senior management of the SCI entity for review no more than 30 calendar days after completion of such SCI review. Such report of the SCI review shall include:

(i) The dates the SCI review was conducted and the date of completion;

(ii) The entity or business unit of the SCI entity performing the review;

(iii) A list of the controls reviewed and a description of each such control;

(iv) The findings of the SCI review with respect to each SCI system and indirect SCI system, which shall include assessments of: the risks related to the capacity, integrity, resiliency, availability, and security; internal control design and operating effectiveness; and an assessment of third-party provider management risks and controls;

(v) A summary, including the scope of testing and resulting action plan, of each penetration test review conducted as part of the SCI review; and

(vi) A description of each deficiency and weakness identified by the SCI review; and

(3) Submit to the Commission, and to the board of directors of the SCI entity or the equivalent of such board, the report of the SCI review required by paragraph (b)(2) of this section, together with the date the report was submitted to senior management and the response of senior management to such report, within 60 calendar days after its submission to senior management of the SCI entity.

**§ 242.1004 [Amended]**

6. Amend §242.1004 by:

a. In the section heading, adding “, and third-party providers” to the end of the heading;

b. In paragraph (a), after the word “participants”, adding “, and third-party providers”; and

c. In paragraph (b), after both instances of the word “participants” adding “, and third-party providers”.

**§ 242.1005 [Amended]**

7. Amend §242.1005 in paragraph (c) by:

a. Between “business” and “ceasing,” removing the “or” and adding a comma in its place; and

b. Immediately before “an SCI entity” adding “or otherwise ceasing to be an SCI entity,”.

**PART 249 – FORMS, SECURITIES EXCHANGE ACT OF 1934**

8. The general authority citation for part 249 continues to read as follows:

**Authority**: 15 U.S.C. 78a *et seq.* and 7201 *et seq.*; 12 U.S.C. 5461 *et seq.*; 18 U.S.C. 1350; Sec. 953(b) Pub. L. 111-203, 124 Stat. 1904; Sec. 102(a)(3) Pub. L. 112-106, 126 Stat. 309 (2012), Sec. 107 Pub. L. 112-106, 126 Stat. 313 (2012), Sec. 72001 Pub. L. 114-94, 129 Stat. 1312 (2015), and secs. 2 and 3 Pub. L. 116-222, 134 Stat. 1063 (2020), unless otherwise noted.

* * * * *

9. Revise Form SCI (referenced in § 249.1900).

**Note:** Form SCI is attached as Appendix A to this document. Form SCI will not appear in the Code of Federal Regulations.

By the Commission.

Dated: March 15, 2023.

**J. Matthew DeLesDernier,**

*Deputy Secretary.*

## Appendix A—Form SCI

**Securities and Exchange Commission**
**Washington, DC 20549**
**Form SCI**

---

Page 1 of _____ File No. SCI-{name}-YYYY-###

**SCI Notification and Reporting by:** {SCI entity name}

Pursuant to Rules 1002 and 1003 of Regulation SCI under the Securities Exchange Act of 1934

- ❑ Initial
- ❑ Withdrawal

---

**SECTION I: Rule 1002 - Commission Notification of SCI Event**

**A. Submission Type (select one only)**

- ❑ Rule 1002(b)(1) Initial Notification of SCI event
- ❑ Rule 1002(b)(2) Notification of SCI event
- ❑ Rule 1002(b)(3) Update of SCI event: ####
- ❑ Rule 1002(b)(4) Final Report of SCI event
- ❑ Rule 1002(b)(4) Interim Status Report of SCI event

If filing a Rule 1002(b)(1) or Rule 1002(b)(3) submission, please provide a brief description:

_____

_____

_____

**B. SCI Event Type(s) (select all that apply)**

- ❑ Systems compliance issue
- ❑ Systems disruption
- ❑ Systems intrusion

**C. General Information Required for (b)(2) filings.**

1) Has the Commission previously been notified of the SCI event pursuant to 1002(b)(1)? *yes/no*

2) Date/time SCI event occurred: *mm/dd/yyyy hh:mm am/pm*

3) Duration of SCI event: *hh:mm*, or *days*

4) Please provide the date and time when a responsible SCI personnel had reasonable basis to conclude the SCI event occurred:

*mm/dd/yyyy* *hh:mm am/pm*

5) Has the SCI event been resolved? *yes/no*

   a) If yes, provide date and time of resolution: *mm/dd/yyyy* *hh:mm am/pm*

6) Is the investigation of the SCI event closed? *yes/no*

   a) If yes, provide date of closure**:** *mm/dd/yyyy*

7) Estimated number of market participants potentially affected by the SCI event: ####

8) Is the SCI event a major SCI event (as defined in Rule 1000)? *yes/no*

**D. Information about impacted systems:**

**Name(s) of system(s):**

_____

_____

_____

**Type(s) of system(s) impacted by the SCI event (check all that apply):**

- ❑ Trading
- ☐ Clearance and settlement
- ☐ Order routing
- ❑ Market data
- ☐ Market regulation
- ☐ Market surveillance
- ❑ Indirect SCI systems (please describe):

_____

_____

_____

**Are any critical SCI systems impacted by the SCI event (check all that apply)? Yes/No**

1) Systems that directly support functionality relating to:
   - ❑ Clearance and settlement systems of clearing agencies
   - ❑ Openings, reopenings, and closings on the primary listing market
   - ❑ Trading halts
   - ☐ Initial public offerings
   - ❑ The provision of consolidated market data
   - ☐ Exclusively-listed securities

2) ☐ Systems that provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets (please describe):

_____

_____

_____

**SECTION II: Periodic Reporting (select one only)**

**A. Quarterly Reports:** For the quarter ended: mm/dd/yyyy

- ❑ Rule 1002(b)(5)(ii): Quarterly report of systems disruptions with no or a de minimis impact.
- ❑ Rule 1003(a)(1): Quarterly report of material systems changes
- ❑ Rule 1003(a)(2): Supplemental report of material systems changes

**B. SCI Review Reports**

- ❑ Rule 1003(b)(3): Report of SCI review, together with the response of senior management

  Date of completion of SCI review: *mm/dd/yyyy*

  Date of submission of SCI review to senior management: *mm/dd/yyyy*

**SECTION III: Contact Information**

Provide the following information of the person at the {SCI entity name} prepared to respond to questions for this submission:

First Name: Last Name:

Title:

E-Mail:

Telephone: Fax:

**Additional Contacts (Optional)**

First Name: Last Name:

Title:

E-Mail:

Telephone: Fax:

First Name: Last Name:

Title:

E-Mail:

Telephone: Fax:

**SECTION IV: Signature**

Confidential treatment is requested pursuant to Rule 24b-2(g). Additionally, pursuant to the requirements of the Securities Exchange Act of 1934, {SCI Entity name} has duly caused this {notification}{report} to be signed on its behalf by the undersigned duly authorized officer:

Date:

By (Name) Title (

_____)

"Digitally Sign and Lock Form"

---

| | |
|---|---|
| **Exhibit 1:**<br>**Rule 1002(b)(2)**<br>**Notification of SCI Event**<br>Add/Remove/View | Within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that the SCI event has occurred, the SCI entity shall submit a written notification pertaining to such SCI event to the Commission, which shall be made on a good faith, best efforts basis and include:<br>(a) a description of the SCI event, including the system(s) affected; and<br>(b) to the extent available as of the time of the notification: the SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; the potential impact of the SCI event on the market; a description of the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved or timeframe within which the SCI event is expected to be resolved; and any other pertinent information known by the SCI entity about the SCI event. |
| **Exhibit 2:**<br>**Rule 1002(b)(4)**<br>**Final or Interim Report of SCI Event**<br>Add/Remove/View | When submitting a final report pursuant to either Rule 1002(b)(4)(i)(A) or Rule 1002(b)(4)(i)(B)(2), the SCI entity shall include:<br>(a) a detailed description of: the SCI entity's assessment of the types and number of market participants affected by the SCI event; the SCI entity's assessment of the impact of the SCI event on the market; the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved; the SCI entity's rule(s) and/or governing document(s), as applicable, that relate to the SCI event; and any other pertinent information known by the SCI entity about the SCI event;<br>(b) a copy of any information disseminated pursuant to Rule 1002(c) by the SCI entity to date regarding the SCI event to any of its members, participants, or, in the case of an SCI broker-dealer, customers; and<br>(c) an analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI event, the number of such parties, and an estimate of the aggregate amount of such loss.<br>When submitting an interim report pursuant to Rule 1002(b)(4)(i)(B)(1), the SCI entity shall include such information to the extent known at the time. |
| **Exhibit 3:**<br>**Rule 1002(b)(5)(ii)**<br>**Quarterly Report of De Minimis SCI Events**<br>Add/Remove/View | The SCI entity shall submit a report, within 30 calendar days after the end of each calendar quarter, containing a summary description of systems disruptions that have had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants, including the SCI systems affected by such systems disruptions during the applicable calendar quarter. |

| | |
|---|---|
| **Exhibit 4:**<br>**Rule 1003 (a)**<br>**Quarterly Report of Systems Changes**<br>Add/Remove/View | When submitting a report pursuant to Rule 1003(a)(1), the SCI entity shall provide a report, within 30 calendar days after the end of each calendar quarter, describing completed, ongoing, and planned material changes to its SCI systems and the security of indirect SCI systems, during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion. An SCI entity shall establish reasonable written criteria for identifying a change to its SCI systems and the security of indirect SCI systems as material and report such changes in accordance with such criteria.<br><br>When submitting a report pursuant to Rule 1003(a)(2), the SCI entity shall provide a supplemental report of a material error in or material omission from a report previously submitted under Rule 1003(a)(1). |
| **Exhibit 5:**<br>**Rule 1003(b)(3)**<br>**Report of SCI review**<br>Add/Remove/View | The SCI entity shall provide the report of the SCI review, together with the date the report was submitted to senior management and the response of senior management to such report, within 60 calendar days after its submission to senior management of the SCI entity. |
| **Exhibit 6:**<br>**Optional Attachments**<br>Add/Remove/View | This exhibit may be used in order to attach other documents that the SCI entity may wish to submit as part of a Rule 1002(b)(1) initial notification submission or Rule 1002(b)(3) update submission. |

## GENERAL INSTRUCTIONS FOR FORM SCI

### A. Use of the Form

Except with respect to notifications to the Commission made pursuant to Rule 1002(b)(1) or updates to the Commission made pursuant to Rule 1002(b)(3), any notification, review, description, analysis, or report required to be submitted pursuant to Regulation SCI under the Securities Exchange Act of 1934 ("Act") shall be filed in an electronic format through an electronic form filing system ("EFFS"), a secure website operated by the Securities and Exchange Commission ("Commission"). Documents attached as exhibits filed through the EFFS system must be in a text-searchable format without the use of optical character recognition. If, however, a portion of a Form SCI submission (e.g., an image or diagram) cannot be made available in a text-searchable format, such portion may be submitted in a non-text searchable format.

### B. Need for Careful Preparation of the Completed Form, Including Exhibits

This form, including the exhibits, is intended to elicit information necessary for

Commission staff to work with SCI entities to ensure the capacity, integrity, resiliency, availability, security, and compliance of their automated systems. An SCI entity must provide all the information required by the form, including the exhibits, and must present the information in a clear and comprehensible manner. A filing that is incomplete or similarly deficient may be returned to the SCI entity. Any filing so returned shall for all purposes be deemed not to have been filed with the Commission. See also Rule 0-3 under the Act (17 CFR 240.0-3).

**C. When to Use the Form**

Form SCI is comprised of six types of required submissions to the Commission pursuant to Rules 1002 and 1003. In addition, Form SCI permits SCI entities to submit to the Commission two additional types of submissions pursuant to Rules 1002(b)(1) and 1002(b)(3); however, SCI entities are not required to use Form SCI for these two types of submissions to the Commission. In filling out Form SCI, an SCI entity shall select the type of filing and provide all information required by Regulation SCI specific to that type of filing.

The first two types of required submissions relate to Commission notification of certain SCI events:

(1) "Rule 1002(b)(2) Notification of SCI Event" submissions for notifications regarding systems disruptions, systems compliance issues, or systems intrusions (collectively, "SCI events"), other than any systems disruption or systems compliance issue that has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants; and

(2) "Rule 1002(b)(4) Final or Interim Report of SCI Event" submissions, of

which there are two kinds (a final report under Rule 1002(b)(4)(i)(A) or Rule 1002(b)(4)(i)(B)(2); or an interim status report under Rule 1002(b)(4)(i)(B)(1)).

The other four types of required submissions are periodic reports, and include:

(1) "Rule 1002(b)(5)(ii)" submissions for quarterly reports of systems disruptions which have had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants;

(2) "Rule 1003(a)(1)" submissions for quarterly reports of material systems changes;

(3) "Rule 1003(a)(2)" submissions for supplemental reports of material systems changes; and

(4) "Rule 1003(b)(3)" submissions for reports of SCI reviews.

Required Submissions for SCI Events

For 1002(b)(2) submissions, an SCI entity must notify the Commission using Form SCI by selecting the appropriate box in Section I and filling out all information required by the form, including Exhibit 1. 1002(b)(2) submissions must be submitted within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred.

For 1002(b)(4) submissions, if an SCI event is resolved and the SCI entity's investigation of the SCI event is closed within 30 calendar days of the occurrence of the SCI event, an SCI entity must file a final report under Rule 1002(b)(4)(i)(A) within five business days after the resolution of the SCI event and closure of the investigation regarding the SCI event. However, if an SCI event is not resolved or the SCI entity's investigation of the SCI event is not closed within 30 calendar days of the occurrence

of the SCI event, an SCI entity must file an interim status report under Rule 1002(b)(4)(i)(B)(1) within 30 calendar days after the occurrence of the SCI event. For SCI events in which an interim status report is required to be filed, an SCI entity must file a final report under Rule 1002(b)(4)(i)(B)(2) within five business days after the resolution of the SCI event and closure of the investigation regarding the SCI event. For 1002(b)(4) submissions, an SCI entity must notify the Commission using Form SCI by selecting the appropriate box in Section I and filling out all information required by the form, including Exhibit 2.

Required Submissions for Periodic Reporting

For 1002(b)(5)(ii) submissions, an SCI entity must submit quarterly reports of systems disruptions which have had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants. The SCI entity must select the appropriate box in Section II and fill out all information required by the form, including Exhibit 3.

For 1003(a)(1) submissions, an SCI entity must submit its quarterly report of material systems changes to the Commission using Form SCI. The SCI entity must select the appropriate box in Section II and fill out all information required by the form, including Exhibit 4.

Filings made pursuant to Rule 1002(b)(5)(ii) and Rule 1003(a)(1) must be submitted to the Commission within 30 calendar days after the end of each calendar quarter (i.e., March 31st, June 30th, September 30th and December 31st) of each year.

For 1003(a)(2) submissions, an SCI entity must submit a supplemental report notifying the Commission of a material error in or material omission from a report

previously submitted under Rule 1003(a). The SCI entity must select the appropriate box in Section II and fill out all information required by the form, including Exhibit 4.

For 1003(b)(3) submissions, an SCI entity must submit its report of its SCI review, together with the date the report was submitted to senior management and the response of senior management to such report, to the Commission using Form SCI. A 1003(b)(3) submission is required within 60 calendar days after the report of the SCI review has been submitted to senior management of the SCI entity. The SCI entity must select the appropriate box in Section II and fill out all information required by the form, including Exhibit 5.

Optional Submissions

An SCI entity may, but is not required to, use Form SCI to submit a notification pursuant to Rule 1002(b)(1). If the SCI entity uses Form SCI to submit a notification pursuant to Rule 1002(b)(1), it must select the appropriate box in Section I and provide a short description of the SCI event. Documents may also be attached as Exhibit 6 if the SCI entity chooses to do so. An SCI entity may, but is not required to, use Form SCI to submit an update pursuant to Rule 1002(b)(3). Rule 1002(b)(3) requires an SCI entity to, until such time as the SCI event is resolved and the SCI entity's investigation of the SCI event is closed, provide updates pertaining to such SCI event to the Commission on a regular basis, or at such frequency as reasonably requested by a representative of the Commission, to correct any materially incorrect information previously provided, or when new material information is discovered, including but not limited to, any of the information listed in Rule 1002(b)(2)(ii). If the SCI entity uses Form SCI to submit an update pursuant to Rule 1002(b)(3), it must

select the appropriate box in Section I and provide a short description of the SCI event. Documents may also be attached as Exhibit 6 if the SCI entity chooses to do so.

**D. Documents Comprising the Completed Form**

The completed form filed with the Commission shall consist of Form SCI, responses to all applicable items, and any exhibits required in connection with the filing. Each filing shall be marked on Form SCI with the initials of the SCI entity, the four-digit year, and the number of the filing for the year (e.g., SCI Name-YYYY-XXX).

**E. Contact Information; Signature; and Filing of the Completed Form**

Each time an SCI entity submits a filing to the Commission on Form SCI, the SCI entity must provide the contact information required by Section III of Form SCI. Space for additional contact information, if appropriate, is also provided.

All notifications and reports required to be submitted through Form SCI shall be filed through the EFFS. In order to file Form SCI through the EFFS, SCI entities must request access to the Commission's External Application Server by completing a request for an external account user ID and password. Initial requests will be received by contacting (202) 551-5777. An e-mail will be sent to the requestor that will provide a link to a secure website where basic profile information will be requested. A duly authorized individual of the SCI entity shall electronically sign the completed Form SCI as indicated in Section IV of the form. In addition, a duly authorized individual of the SCI entity shall manually sign one copy of the completed Form SCI, and the manually signed signature page shall be preserved pursuant to the requirements of Rule 1005.

**F. Withdrawals of Commission Notifications and Periodic Reports**

If an SCI entity determines to withdraw a Form SCI, it must complete Page 1 of the Form SCI and indicate by selecting the appropriate check box to withdraw the submission.

**G. Paperwork Reduction Act Disclosure**

This collection of information will be reviewed by the Office of Management and Budget in accordance with the clearance requirements of 44 U.S.C. 3507. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number. The Commission estimates that the average burden to respond to Form SCI will be between one and 125 hours, depending upon the purpose for which the form is being filed. Any member of the public may direct to the Commission any comments concerning the accuracy of this burden estimate and any suggestions for reducing this burden.

Except with respect to notifications to the Commission made pursuant to Rule 1002(b)(1) or updates to the Commission made pursuant to Rule 1002(b)(3), it is mandatory that an SCI entity file all notifications, reviews, descriptions, analyses, and reports required by Regulation SCI using Form SCI. The Commission will keep the information collected pursuant to Form SCI confidential to the extent permitted by law. Subject to the provisions of the Freedom of Information Act, 5 U.S.C. 522 ("FOIA"), and the Commission's rules thereunder (17 CFR 200.80(b)(4)(iii)), the Commission does not generally publish or make available information contained in any reports, summaries, analyses, letters, or memoranda arising out of, in anticipation of, or in connection with an examination or inspection of the books and records of any person or any other investigation.

## H. Exhibits

List of exhibits to be filed, as applicable:

Exhibit 1: Rule 1002(b)(2) – Notification of SCI Event. Within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that the SCI event has occurred, the SCI entity shall submit a written notification pertaining to such SCI event to the Commission, which shall be made on a good faith, best efforts basis and include: (a) a description of the SCI event, including the system(s) affected; and (b) to the extent available as of the time of the notification: the SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; the potential impact of the SCI event on the market; a description of the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved or timeframe within which the SCI event is expected to be resolved; and any other pertinent information known by the SCI entity about the SCI event.

Exhibit 2: Rule 1002(b)(4) – Final or Interim Report of SCI Event. When submitting a final report pursuant to either Rule 1002(b)(4)(i)(A) or Rule 1002(b)(4)(i)(B)(2), the SCI entity shall include: (a) a detailed description of: the SCI entity's assessment of the types and number of market participants affected by the SCI event; the SCI entity's assessment of the impact of the SCI event on the market; the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved; the SCI entity's rule(s) and/or governing document(s), as applicable, that relate to the SCI event; and any other pertinent information known by the SCI entity about the SCI event; (b) a copy of any information disseminated pursuant

to Rule 1002(c) by the SCI entity to date regarding the SCI event to any of its members, participants, or, in the case of an SCI broker-dealer, customers; and (c) an analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI event, the number of such parties, and an estimate of the aggregate amount of such loss. When submitting an interim report pursuant to Rule 1002(b)(4)(i)(B)(1), the SCI entity shall include such information to the extent known at the time.

Exhibit 3: Rule 1002(b)(5)(ii) – Quarterly Report of De Minimis SCI Events. The SCI entity shall submit a report, within 30 calendar days after the end of each calendar quarter, containing a summary description of systems disruptions that have had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants, including the SCI systems affected by such SCI events during the applicable calendar quarter.

Exhibit 4: Rule 1003(a) – Quarterly Report of Systems Changes. When submitting a report pursuant to Rule 1003(a)(1), the SCI entity shall provide a report, within 30 calendar days after the end of each calendar quarter, describing completed, ongoing, and planned material changes to its SCI systems and the security of indirect SCI systems, during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion. An SCI entity shall establish reasonable written criteria for identifying a change to its SCI systems and the security of indirect SCI systems as material and report such changes in accordance with such criteria. When submitting a report pursuant to Rule 1003(a)(2), the SCI entity shall provide a supplemental report of a material error in or material omission

from a report previously submitted under Rule 1003(a); provided, however, that a supplemental report is not required if information regarding a material systems change is or will be provided as part of a notification made pursuant to Rule 1002(b).

Exhibit 5: Rule 1003(b)(3) – Report of SCI Review. The SCI entity shall provide the report of the SCI review, together with the date the report was submitted to senior management and the response of senior management to such report, within 60 calendar days after its submission to senior management of the SCI entity.

Exhibit 6: Optional Attachments. This exhibit may be used in order to attach other documents that the SCI entity may wish to submit as part of a Rule 1002(b)(1) initial notification submission or Rule 1002(b)(3) update submission.

## I. Explanation of Terms

**Critical SCI systems** means any SCI systems of, or operated by or on behalf of, an SCI entity that: (1) directly support functionality relating to: (i) clearance and settlement systems of clearing agencies; (ii) openings, reopenings, and closings on the primary listing market; (iii) trading halts; (iv) initial public offerings; (v) the provision of market data by a plan processor; or (vi) exclusively-listed securities; or (2) provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.

**Indirect SCI systems** means any systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems.

**Major SCI event** means an SCI event that has had, or the SCI entity reasonably estimates would have: (1) any impact on a critical SCI system; or (2) a significant

impact on the SCI entity's operations or on market participants.

**Responsible SCI personnel** means, for a particular SCI system or indirect SCI system impacted by an SCI event, such senior manager(s) of the SCI entity having responsibility for such system, and their designee(s).

**SCI entity** means an SCI self-regulatory organization, SCI alternative trading system, plan processor, exempt clearing agency, SCI competing consolidator, SCI broker-dealer, or registered security-based swap data repository.

**SCI event** means an event at an SCI entity that constitutes: (1) a systems disruption; (2) a systems compliance issue; or (3) a systems intrusion.

**SCI review** means a review, following established and documented procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems, and which review, using appropriate risk management methodology, contains: (1) with respect to each SCI system and indirect SCI system of the SCI entity, assessments performed by objective personnel of: (A) the risks related to capacity, integrity, resiliency, availability, and security; (B) internal control design and operating effectiveness, to include logical and physical security controls, development processes, systems capacity and availability, information technology service continuity, and information technology governance, consistent with industry standards; and (C) third party provider management risks and controls; and (2) penetration test reviews performed by objective personnel of the network, firewalls, and production systems, including of any vulnerabilities of its SCI systems and indirect SCI systems identified pursuant to paragraph § 242.1001(a)(2)(iv); (3) *provided, however,* that assessments of SCI systems directly supporting market regulation or market

surveillance shall be conducted at a frequency based upon the risk assessment conducted as part of the SCI review, but in no case less than once every three years**.**

**SCI systems** means all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance; *provided, however,* that with respect to an SCI broker-dealer that satisfies only the requirements of paragraph (2) of the definition of "SCI broker-dealer," such systems shall include only those systems with respect to the type of securities for which an SCI broker-dealer satisfies the requirements of paragraph (2) of the definition.

**Systems Compliance Issue** means an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable.

**Systems Disruption** means an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system.

**Systems Intrusion** means any: (1) unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity; (2) cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system; or (3) significant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria.

[FR Doc. 2023-05775 Filed: 4/13/2023 8:45 am; Publication Date: 4/14/2023]