**June 13, 2023**

**VIA ELECTRONIC SUBMISSION (rule-comments@sec.gov)**

**Vanessa Countryman, Secretary,**

**Securities and Exchange Commission,**

**100 F Street NE, Washington,**

**DC 20549-1090.**

**Re:**

**File No. S7-07-23; Release No. 34-97143; Regulation Systems Compliance and Integrity**

Dear Ms. Countryman,

The Global Association of Central Counterparties ("CCP12") appreciates the opportunity to comment on the SEC's Proposed Regulation SCI ("Reg SCI Proposal" or "Proposal"). CCP12 represents 42 members from around the world, who operate over 60 individual central counterparties ("CCPs"), representing over 95% of the centrally cleared risk management in initial margin terms.

CCP12 members recognize the importance of evolving their cybersecurity programs as cyber incidents continue to grow in number, frequency, and sophistication in order to continue delivering the benefits of central clearing and their risk management role to the world's markets. CCPs and their stakeholders strive to meet the highest standards for continuity of operations and integrity given the essential role they serve for their participants and markets. In recent years, the attention and efforts devoted to prudent and resilient management of cybersecurity have grown alongside an evolving threat environment. Although CCP12 recognizes that updates and specificity can often bring clarity to requirements, we note that it can also introduce regulatory uncertainty and unintended consequences. As a result, we urge the SEC to consider global efforts to align industry standards and best practices to promote strong cybersecurity within the U.S. securities market.

CCP12 highlighted several areas of the Proposal where refinement and clarification would be helpful, including with respect to the overlap of the Reg SCI Proposal with the SEC's Proposed Rule 10 ("Rule 10 Proposal"),[1] the expanded third-party risk management requirements, and the updated definitions of systems intrusion and systems disruption.

[1] Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents (File Number S7-06-23).

**Discussion of Specific Comments**

1. **Reg SCI and the Rule 10 Proposal achieve the same intended cyber resilience outcome objectives.**

CCP12 notes considerable overlap between Reg SCI (i.e., current and proposed) and the Rule 10 Proposal and appreciates the SEC's acknowledging that such an overlap exists. CCP12 believes the purpose of the Rule 10 Proposal is ultimately aimed at ensuring a safe and efficient securities market, which is consistent with the purpose of Reg SCI. The SEC also notes that while the policies and procedures requirements under Reg SCI differ in scope and purpose from the Rule 10 Proposal, these requirements as they relate to cybersecurity (currently and as would be amended) are generally consistent with the Rule 10 Proposal.

The SEC notes this overlap but explains there is a practical difference in scope – namely that Reg SCI focuses on Reg SCI and indirect Reg SCI information systems, whereas the Rule 10 Proposal would have a broader scope, which also covers information systems that are not SCI systems or indirect SCI systems. CCP12 recognizes that there is such a gap between the two, however, we also believe Reg SCI would already ensure the same cyber resilience outcomes at SCI entities that the Rule 10 Proposal intends to achieve for its covered entities. These specific concerns are detailed in CCP12's companion comment letter that focuses primarily on the Rule 10 Proposal ("CCP12 Rule 10 Letter"[2]). The following points are noted as examples of redundancy between Reg SCI, current and proposed, and the Rule 10 Proposal:

- Information systems that are not Reg SCI or indirect SCI systems would not be able to affect the SCI entity's ability to conduct critical business functions (e.g., ensure prompt and accurate clearing and settlement of securities transactions). For information systems that are not scoped in as an indirect SCI system, these systems would have to be logically or physically separate from SCI systems.
- Reg SCI's reporting requirements cover not only what would be considered a "significant cybersecurity incident" under proposed §§ 242.10(a)(10), (c), and (d), but generally all "systems disruptions," "systems intrusions," and "systems compliance issues" unless they are determined to have de minimis impact.
- Form SCI already requires an SCI entity to identify the type of "SCI event" it is experiencing (or has experienced), including whether it is a "systems intrusion," which seems consistent with Rule 10 Proposal's concepts of cybersecurity incidents, as well as details regarding the incident. Form SCI, even if the terminology used in the form differs from proposed Form SCIR, would effectively provide the SEC with the same information that would be provided through Form SCIR.
- Regarding public disclosures, current practice by covered entities, which include covered clearing agencies, the outcome for publicly disclosing information is already being achieved through existing requirements for which they and any subsidiaries are subject to. This includes Reg SCI's responsible disclosure requirements to its participants/members and the

[2] https://ccp12.org/wp-content/uploads/2023/06/05062023_CCP12_response_to_the_SEC_Rule_10_Proposal.pdf

requirements for covered clearing agencies to disclose how they are managing the risks addressed under the SEC's covered clearing agency standards.

CCP12 requests that the SEC remove the regulatory uncertainty resulting from what appears to be a set of proposed requirements that would be overlapping or duplicative with Reg SCI (without an accompanying clear roadmap for such entities to navigate the varying terms and processes of the two rules), either by scoping covered clearing agencies out from the Rule 10 Proposal or by providing assurances to covered clearing agencies that compliance with Reg SCI would be considered compliance with the Rule 10 Proposal.

2. **CCP12 recommends that the SEC consider a more flexible and risk-based approach to third-party requirements.**

**Third parties that "indirectly" provide services for SCI systems and indirect SCI systems**

The Proposal reads that each SCI entity will need 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, indirect SCI systems" (emphasis added).[3] The placement of the word 'indirectly' appears to imply that 4th and nth party providers are a type of third-party when used throughout the Proposal. Therefore, the SEC is significantly increasing the number of entities that would be subject to oversight under the Proposal. The inclusion of service providers to service providers, means that SCI entities will need to "manage and oversee" 4th and nth parties when using a third-party provider. By way of example, an SCI system may be provided by a third-party, which in turn may use a cloud service provider ("CSP") and a full suite of third-party providers for its own security and resilience needs. These nth parties may include a broad range of third parties under the current definition, such as third-party development services, off-the-shelf software licensors or maintenance, and support services. Each of these nth party providers would be subject to oversight under the Proposal, regardless of how critical the nth party is to the applicable systems.

CCP12 therefore requests that the SEC clarify expectations around managing and overseeing 4th and nth party risks, including clarification regarding the scope third parties that will be subject to oversight. Absent a contractual right, it is difficult for an SCI entity to manage and oversee an nth party. Typically, managing 4th and nth party risk is conducted through contracts, whereby firms include a clause that requires a third-party provider to notify the financial institution if 4th parties are used or otherwise restrict or remove the ability to use 4th parties entirely. The firm typically determines which approach to use based on internal risk assessments and pertinent third-party risk management tools. Additionally, firms typically require third-party providers to have their own third-party provider programs, which includes requirements that meet or exceed a firm's own third-party provider program.

CCP12 recommends that the term "indirectly" be removed if the SEC did not intend to directly scope in the risk management of nth parties. However, if the Proposal did intend to require SCI entities to manage and oversee 4th and nth parties, CCP12 requests that the SEC modify the requirement to promote more

[3] Proposal 113

flexibility, such as by indicating SCI entities need to manage the risks of third parties, rather than "manage and oversee."

**Third-party concentration risk considerations**

The SEC states that "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 mitigating overreliance on a given third-party provider by the SCI entity or by the industry."[4] Understanding industry-wide concentration risks, however, will require that regulators aggregate and share information with SCI entities so that these SCI entities could fully understand where potential concentration risks may exist. Individual SCI entities do not have knowledge of those third-party providers used by other market participants. Without this information, SCI entities lack the visibility into potential industry-wide concentrations or the expected actions that should be taken in light of a perceived concentration.

Additionally, CCP12 appreciates the work of the U.S. Treasury to understand potential concentration risks related to the use of CSPs throughout the financial services sector as highlighted in their recent white paper, *The Financial Services Sector's Adoption of Cloud Services.*[5] CCP12 encourages the SEC to collaborate with the U.S. Treasury, through the Financial and Banking Information Infrastructure Committee ("FBIIC") or other means, to further understand potential CSP concentration risk and partner with private sector, where necessary. CCP12 emphasizes that the goal of identifying concentration risk should be to manage these risks and not just to identify or eliminate the concentration itself.

Lastly, CCP12 supports reviewing and monitoring third-party concentration risks from an individual entity perspective. However, SCI entities should not be required to avoid using a certain third-party provider solely due to risk of concentration. SCI entities need to have the ability to weigh the risk of third-party provider concentration against expected gains in resiliency, efficiency and effectiveness.

**Managing the potential risk of unavailability for certain third-party providers through business continuity/disaster recovery plans ("BC/DR")**

The Proposal includes a requirement under proposed § 242.1001(a)(2)(v) for SCI entities to have BC/DR plans 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." Further, the SEC explicitly mentions considering extended outage scenarios such as if a third-party provider "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."[6] This type of scenario is outside the typical scope of BC/DR plans. Firms typically manage relationships with third parties through contracts and relationships. CCP12 appreciates the SEC's concerns over the ability to maintain operations when using third-party providers; however, the example of an extended outage may be construed to mean that the way to solve certain risks is through the use of multiple third-

[4] Proposal 117
[5] U.S. Treasury, The Financial Services Sector's Adoption of Cloud Services - https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf
[6] Proposal 119

party providers. The challenge with this approach is that each third-party provider may have proprietary implementations making it highly complicated to switch third-party providers with reasonable assurance that the application or system would operate in the new technology environment without incident. For example, given the complexities involved in enabling a transfer of operations across inconsistent features in different CSP environments, CCP12 recommends that the SEC make clear that using multiple CSPs for resilience is not the preferred solution to addressing the unavailability of a critical third-party provider in a BC/DR context. Instead, the SCI entity should have the ability to design their BC/DR in the manner that is most appropriate for its offering.

CCP12 supports the need to consider a wide array of extreme but plausible scenarios for BC/DR and believes most of the scenarios discussed in the Proposal are typical BC/DR scenarios. CCP12 notes that the proposed amendment to § 242.1001(a)(2)(v) appears only to make more explicit the existing requirement to address disruptions that originate at a third-party provider given that Reg SCI already applies to systems that are operated "on behalf of" the SCI entity (i.e., by third-party providers).

**Industry and sector-wide BC/DR testing for security-based swap data repositories ("SBSDRs")**

CCP12 believes it is appropriate for SBSDRs to include relevant clients and third-party providers in its testing of BC/DR plans, as would be required under §§ 242.1004(a) and (b). However, existing industry-wide testing focuses on recovery of market operations that would come before the activity would be reported to an SBSDR. Although industry-wide exercises would provide insights into those operational incidents that may have significant market impacts to the financial services sector, the time commitment to participate in these exercises is outsized by this benefit for purposes of SBSDRs. We would therefore ask that the SEC allow SBSDRs to participate as observers to the existing industry-wide exercises as a means of complying with § 242.1004(c), or exempt entirely SBSDRs from coordinating industry- or sector-wide BC/DR testing.

3. **The definition of systems intrusion should be limited to actual cybersecurity incidents that caused harm**

The expanded definition of "systems intrusions" presents challenges for SCI entities, as it includes *attempted* intrusions, as well as intrusions that caused actual harm. We believe that attempted and actual intrusions should receive different regulatory treatment, given the difference in level of risk. The SEC's proposed definition encompasses the following:

> a. "Second 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."
>
> b. "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."

CCP12 understands the expanded definition is meant to cover a cybersecurity event that causes disruptions or significant degradation to SCI systems and indirect SCI systems, should the event have

occurred outside of an SCI or indirect SCI system and did not result in an entry into or access to these systems.

Additionally, the proposed third prong of the systems intrusion definition would require SCI entities to provide the SEC with information on significant attempted unauthorized entries that could ultimately be unsuccessful. The SEC notes that the objective of requiring this information is to provide its staff with, important information regarding threats and 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 as other SCI entities and market participants.[7] We appreciate the SEC recognizing that it would be undesirable to require that all attempted intrusions be considered significant. However, the definition of systems intrusions should be limited to events that cause actual harm, particularly due to the strong threat intelligence sharing mechanisms that are established throughout the financial services sector. The proposed definition would lead to unnecessary and time-consuming reporting without a discernible marginal benefit to the SEC or the market. CCP12 would also therefore recommend that any final rule not include attempted intrusions in the definition of systems intrusion. Instead, we recommend that the SEC should seek appropriate threat intelligence reports, whether through government reporting (e.g., U.S. Cybersecurity and Infrastructure Security Agency's Cyber Incident Reporting for Critical Infrastructure Act) or third-party threat intelligence reporting (e.g., Crowdstrike).

CCP12 would also reiterate its suggestion, provided in full in its Rule 10 Letter,[8] to harmonize cyber incident reporting requirements as outlined by the Financial Stability Board[9] and other US governmental agencies. Specifically, the SEC should adopt a flexible approach to cybersecurity policies and procedures that relies on existing frameworks like the National Institute of Standards and Technology's Cybersecurity Framework. The SEC should also leverage the statutory and upcoming regulatory framework outlined in CIRCIA by providing a safe harbor from additional reporting requirements for critical infrastructure covered entities and working with CISA and the U.S. Department of the Treasury to gather the information it seeks.

**4. The terms third-party provider and service providers should be harmonized**

CCP12 proposes a harmonization of terminology across the Reg SCI Proposal and Rule 10 Proposal, so as to ensure clarity across what currently appears to be varied use of terms between regulations. By way of example, Reg SCI uses the term "third-party provider," whereas the Rule 10 Proposal uses the term "service providers". Similarly, the recent SEC proposal on Covered Clearing Agency Resilience and Recovery and Wind-Down Plans includes a discussion of the multiple definitions of "service provider". The divergence in definitions across different SEC rulemaking efforts may lead to confusion, needless complexity and gaps in application. Harmonizing these terms will enhance clarity and coherence in the overall regulatory framework. This is of particular importance to CCPs given the SEC has proposed

[7] Proposal 132.
[8] https://ccp12.org/wp-content/uploads/2023/06/05062023_CCP12_response_to_the_SEC_Rule_10_Proposal.pdf
[9] FSB Recommendations to Achieve Greater Convergence in Cyber Incident Reporting - https://www.fsb.org/wp-content/uploads/P130423-1.pdf

several rules in the last year that contain similar, but not identical, definitions, creating at a minimum a significant administrative burdens for impacted entities to parse the distinctions in those definitions.[10]

5. **The SEC should consider an appropriate implementation timeline**

CCP12 encourages the SEC to carefully consider the implementation timeline for newly scoped-in SCI entities to comply with Reg SCI. An adequate timeline will enable newly scoped-in SCI entities to make any necessary changes in processes or technology and limit the risk of harming operations. CCP12 would highlight that to the degree possible, compliance should make use of existing diligence mechanisms, such as surveys, reviews of third-party materials, and certifications such as SOC 2.

CCP12 also encourages the SEC to consider the overlapping requirements between Reg SCI and Rule 10 in determining an implementation timeline for both rules. While covered CCP12 members have been compliant with Regulation SCI for almost a decade, they will need to review their existing operational (including cybersecurity) risk management policies and procedures against the requirements imposed by any final version of the proposed amendments to Reg SCI; consult the relevant SEC supervisory and policy teams to further understand the amended Reg SCI; determine the changes that are necessary to comply with Reg SCI; ensure that such changes would not conflict with other U.S. or non-U.S. regulatory requirements to which the CCP are also subject; and execute on such changes. Each step of this change management process is subject to diligent governance and reviews, including pursuant to SEC and CFTC mandates and guidance. To the degree that contracts with service providers must be repapered, CCP12 would like to indicate that this is a laborious and costly process. As a result, CCP12 requests that the SEC carefully consider these factors when setting a compliance date for meeting the new requirements.

Additionally, CCP12 requests that the SEC provide clarification on proposed[11] section 242.1003(b)(1), which would require an SCI review to be conducted "not less than once each calendar year for each calendar year during which [the SCI entity] was an SCI entity for any part of such calendar year." The SEC clarifies 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 SEC. 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." This may not be sufficient time for the new SCI entity to conduct an SCI review given the large number of relevant policies and procedures for the objective personnel to review and test, which cannot be completed without having a full year to conduct such a review.

[10] We note that the SEC itself appears to recognize the potential for confusion and administrative burden arising from a profusion of definitions for similar terms and concepts. *See* RIN 3235-AN19 Covered Clearing Agency Resilience and Recovery and Wind-Down Plans, Release No. 34-97516 (May 17, 2023), at fn. 82 (discussing SEC's views on overlap of definitions relating to third-party service providers in not only Reg SCI and Rule 10 proposals, but also a recent proposal relating to clearing agency governance), *available at* https://www.sec.gov/rules/proposed/2023/34-97516.pdf.

[11] Proposal 196

CCP12 appreciates the opportunity to provide its feedback to the Reg SCI Proposal and for the SEC's consideration of the points outlined in this letter. CCP12 welcomes any opportunity to provide further clarity to its views as may be requested by the SEC.

## About CCP12

CCP12 is the global association for CCPs, representing 42 members who operate over 60 individual central counterparties (CCPs) across the Americas, EMEA, and the Asia-Pacific region.

CCP12 promotes effective, practical, and appropriate risk management and operational standards for CCPs to ensure the safety and efficiency of the financial markets it represents. CCP12 leads and assesses global regulatory and industry initiatives that concern CCPs to form consensus views, while also actively engaging with regulatory agencies and industry constituents through consultation responses, forum discussions, and position papers.

For more information, please contact the office by e-mail at office@ccp12.org or through our website by visiting www.ccp12.org.

## CCP12 Members