June 5, 2023

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

Secretary

Securities and Exchange Commission

100 F Street NE, Washington

DC 20549-1090

Re: SEC Proposes New Rule on 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

The Global Association of Central Counterparties ("CCP12") appreciates the opportunity to comment on the SEC's Proposed Rule 10 ("Rule 10 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 expect 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. As such, we appreciate the efforts led by authorities, such as the SEC, to focus on cybersecurity and broadly support the intention of the Rule 10 Proposal, as it applies to covered clearing agencies. We would note that in addition to previous comments to international standard setting bodies' and jurisdictional authorities' consultations on cyber matters, CCP12 is also responding to the SEC's Regulation Systems, Compliance and Integrity ("Reg SCI") proposal separately.

CCP12 highlights several areas of the Proposal where we consider refinement and clarification would be helpful, including the requirements to publicly disclose significant cybersecurity incidents and the significant redundancy that Proposed Rule 10 would create for entities that are

already (or will be) subject to multiple overlapping rules, including Reg SCI, currently and as it is proposed to be amended. CCP12 does acknowledge a difference between the Rule 10 Proposal, which encompasses all systems, and Reg SCI, which is restricted to Reg SCI and indirect Reg SCI systems. Our view, however, is that Reg SCI already ensures the same level of cyber resilience at SCI entities as the Rule 10 Proposal seeks to establish for its covered entities, both of which include clearing agencies. The substantial overlap in these rules leads to significant redundancy for SCI entities. It is also incumbent upon the SEC to balance the need for enhanced cybersecurity practices while also acknowledging that premature incident disclosure may harm investors. Our comments below are intended to bring additional clarity and consistency to the proposed requirements for covered entities, particularly covered clearing agencies, and identify areas where regulatory uncertainty could be mitigated, strengthening the rule text and avoid confusion for covered entities during implementation.

Discussion of Specific Comments

1. **Proposed Rule 10 introduces regulatory uncertainty given it appears to be substantially redundant in scope and outcome for the entities that are or will be subject to Reg SCI**

CCP12 notes considerable overlap between Reg SCI (i.e., current and proposed) and the Rule 10 Proposal. The SEC notes this overlap but explain 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 that 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. 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 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 redundant 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. Finally, to the extent the SEC believes there remains a need to apply the Rule 10 Proposal to SCI entities to cover the risk management of those information systems that are not SCI systems or indirect SCI systems, CCP12 believes the SEC's proposed general requirement for covered entities to "establish, maintain, and enforce written policies and procedures that are reasonably designed to address the covered entity's cybersecurity risks" under § 242.10(b)(1), and not the subsequent prescriptive requirements, would be and allow the covered entity flexibility to adopt a risk-based approach to managing the cybersecurity risks from these non-critical systems.

2. The Proposal does not align with Congressional, Executive, and Other Governmental efforts to harmonize cyber incident reporting requirements.

CCP12 proposes a harmonization of terminology across the Rule 10 Proposal and those of Reg SCI, 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.

CCP12 notes that many covered entities regulated by the SEC are also global organizations and therefore, the SEC should consider global efforts to harmonize cyber incident reporting requirements. For example, the Financial Stability Board, which includes the SEC as a member,

recently published its final report on Recommendations to Achieve Greater Convergence in Cyber Incident Reporting ("Report").[1] The Report contains recommendations that aim to promote convergence among cyber incident reporting frameworks, while recognizing that a one-size-fits-all approach is not feasible. The Report includes a specific recommendation for financial authorities to continue to explore ways to align cyber incident reporting regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimize potential fragmentation and improve interoperability.[2]

Additionally, as many CCP12 members play a critical role in the financial services sector, many will be subject to the U.S. Cybersecurity and Infrastructure Security Agency's ("CISA") Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"). One of the goals of CIRCIA is to harmonize U.S. federal incident reporting requirements and establish interagency information sharing requirements.[3] There will be significant overlap to those firms that will be required to comply with CIRCIA and the Rule 10 Proposal incident reporting requirements which leads to complex implementation challenges if these rules are not aligned.

We thus recommend that the SEC further harmonize the Rule 10 Proposal with existing cybersecurity requirements and cyber incident reporting requirements. 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 ("NIST") 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.

3. Public disclosure requirements could have financial stability implications and may cause substantial harm to the covered entity.

As noted above, CCP12 and its membership recognize the importance of timely incident reporting and support promoting transparency as an essential component to maintaining fit-for-purpose risk management, but CCP12 does not believe public disclosure of significant cybersecurity incidents as proposed is appropriate for CCPs. Due to the sensitive nature of the information, public cybersecurity incident reporting, especially in a contemporaneous manner before the incident is resolved, could cause substantial harm to the U.S. securities market. In particular, such public reporting may provide potential cyber adversaries with a "playbook", thus, exposing covered entities to additional attacks, which is especially concerning given the critical role covered clearing agencies play in U.S. securities markets. The SEC's perceived benefits of

[1] FSB Recommendations to Achieve Greater Convergence in Cyber Incident Reporting - https://www.fsb.org/wp-content/uploads/P130423-1.pdf
[2] FSB Report, Recommendation 2
[3] Public Law 117–103, Div. Y (2022) (to be codified at 6 U.S.C. 681–681g)

public disclosure need to be carefully balanced with the need to protect the stability of the U.S. securities market.

In addition, the SEC's stated benefit of providing information to customers, counterparties, members, registrants, or users such that the information could be used to "avoid certain Covered Entities with less well-developed cybersecurity procedures,"[4] or choose not to do business with a covered entity with a history of significant cybersecurity incidents, does not readily apply to clearing agencies that already have robust cybersecurity programs under current SEC regulations. The type of principal-agent problem articulated by the SEC does not arise for clearing agencies given existing regulatory compliance obligations and rigorous examinations schedules.[5]

Additionally, the requirement for immediate notification of a significant cybersecurity event to the SEC and followed by subsequent reporting under Part I within 48 hours, may mean that an entity has not had sufficient time to gather and verify the information required to complete Part I of Form SCIR, which could result in incomplete or inaccurate information, require multiple amended reports, and potentially draw resources away from mitigation. Further, SCI entities (i.e., including covered clearing agencies) are already subject to a separate incident reporting program, where SCI events (unless they are determined to be de minimis) are subject to immediate notifications, 24-hour subsequent reporting, and updates as material information arises. The SEC also explains in the Proposal that entities that fall under both requirements, which includes covered clearing agencies, must follow both processes for those incidents that trigger both reporting thresholds (which have different reporting frequencies and different deliver methods to the SEC), rather than one harmonized single process, but does not appear to provide supporting rationale for the necessity of dual regimes and how the resulting burden is offset. CCP12 recommends aligning and harmonizing with Reg SCI by either scoping covered clearing agencies out from the Rule 10 Proposal, (as noted in Section 1 above) or by allowing covered clearing agencies' reporting under the Reg SCI process to serve as compliance with the Rule 10 Proposal process. Thus, CCP12 proposes the SEC's policy goals with respect to covered clearing agencies would be met by confidential disclosure directly to the SEC by inclusion of the disclosure summary of cybersecurity risks under the Covered Clearing Agencies Standards disclosure framework.

As noted above, CCP12 does not believe public disclosure of significant cybersecurity incidents is appropriate for CCPs. Should the SEC nevertheless favor such disclosure, CCP12 would stress the crucial question as to the timing of disclosures, as they may interfere with the

[4] Proposal 377

[5] Proposal 377; Insofar as principals (customers) prefer a higher level of cybersecurity focus by agents (Covered Entities), public disclosure would act as an incentive for Covered Entities to increase their focus in this area and signal their commitment to protecting customers' funds and data.

management of the incident. The Rule 10 Proposal states "[t]herefore, the Covered Entity would need to file a Part I and an updated Pat II of proposed Form SCIR with the SEC relatively contemporaneously."[6] This required timing would impose significant burden on a covered entity at a time when its efforts and resources should be focused on investigating and remediating the incident. Covered entities may not have completed a full assessment of the incident and its impacts at such an early stage. In order to avoid confusion and ensure resources are directed appropriately, if any public disclosure is required, it should be required only after the incident has been fully investigated and remediated, when the covered entity has a more accurate understanding of the significance and impact of an incident. It may also be advisable that authorities, not least of which the SEC, have the ability to convene and review when certain elements of an attack on key infrastructure is disclosed.

4. **The proposed definitions of "Cybersecurity Incident" and "Significant Cybersecurity Incident" should be modified**

CCP12 recommends removing "jeopardizes" from the definition of "Cybersecurity Incident" and limit the scope of incidents that cause actual harm. Removing "jeopardizes" would be in line with the latest FSB Cyber Lexicon[7] definition of cyber incident. Limiting incidents to those that impose an actual harm would avoid the reporting of harmless incidents at the expense of time and resources and ultimately, the reporting of these incidents provides no clear risk management benefit.

CCP12 also advises that the definition of "Significant Cybersecurity Incident" should require a higher threshold. Specifically, the second prong of the definition, "a cybersecurity incident, or a group of related cybersecurity incidents, that 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 (1) substantial harm to the Market Entity; or (2) substantial harm to a customer, counterparty, member, registrant, or user of the Market Entity, or to any other person that interacts with the Market Entity." The inclusion of (2) within the second prong of the definition would capture incidents that may only impact a single market entity, single customer, or single person that interacts with the covered clearing agency that was impacted, which may not amount to significant or demonstrable harm to the operations or stability of the U.S. securities markets. Furthermore, the use of the phrases "leads to" and "reasonably likely to result in" in the second prong of the definition of Significant Cybersecurity Event are subjective and may interfere with the SEC's goal of comprehensively aggregating information about cybersecurity incidents in order to inform future policy decisions. We encourage the SEC to provide guidance on the

[6] Proposal 167
[7] FSB Cyber Lexicon - https://www.fsb.org/wp-content/uploads/P130423-3.pdf

manner in which those terms might apply to the various different types of covered entities. Absent such guidance, the data collected by the SEC may lack comparability and consistency.

5. **The public disclosure requirement may disrupt other government agencies from performing their investigatory duties.**

CCP12 recommends a revision to Part II of proposed Form SCIR to allow the covered entity to delay publicly disclosing a significant security incident or an update where the Attorney General requests such a delay. CCP12 noted that the Rule 10 Proposal proposes a "national security" exception to the public disclosure requirements however, allowing delay only on the Attorney General's determination conflates national security with law enforcement. As discussed by President Biden in his Executive Order on Improving the Nation's Cybersecurity, cybersecurity requires more than government action. It requires a collaboration between the public and private sectors to successfully function. Even within such collaboration, the SEC must leave room for the covered entity to make its own determination that disclosure of a cybersecurity incident on Part II of proposed Form SCIR may serve as a roadmap for malicious actors.

Reg SCI, for example, authorizes entities to make such determinations. In that rule, the SEC allows for delayed public disclosures if the SCI Entity "determines that dissemination of such information would likely compromise the security of the SCI Entity . . . and documents the reason for such determination." National security risk determinations must expand further than the Attorney General to lessen the risk of malicious actors preying on any infrastructure vulnerabilities. The SEC should allow agencies such as CISA to make determinations of national security risks. Premature reporting to the SEC could disrupt the ability of other government agencies to perform their investigatory duties.

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