MSRB
Municipal Securities Rulemaking Board

June 5, 2023

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: **File No. S7-06-23 - 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**

Dear Ms. Countryman,

The Municipal Securities Rulemaking Board (the "MSRB") appreciates the opportunity to provide comments to the Securities and Exchange Commission (the "Commission") in response to the Commission's proposal to adopt a new Rule 10 ("proposed Rule 10") to address cybersecurity risks to the U.S. securities markets and market participants (the "Proposal").[1]

The MSRB is a self-regulatory organization established by Congress with the statutory mandate under Section 15B of the Securities Exchange Act of 1934 to promulgate rules for the municipal securities market that protect investors, state and local governments and other municipal entities, obligated persons and the public interest. The MSRB fulfills its mission to safeguard the nearly $4 trillion municipal securities market by, among other activities, establishing rules for brokers, dealers, municipal securities dealers and municipal advisors that engage in municipal securities and advisory activities. MSRB rules are designed to prevent fraud and manipulation and promote fair dealing and a fair and efficient market.

As the Commission noted in the Proposal, the MSRB relies on information systems, including the Electronic Municipal Market Access (EMMA®) website, to carry out its mission. The MSRB operates the EMMA website to further promote a fair and efficient market. The EMMA website increases the transparency of the municipal securities market by providing free public access to municipal securities disclosures and data. It also provides investors, state and local governments and other market participants with key information and tools to effectively use that information.

---

[1] Cybersecurity Risk Management, Exchange Act Release No. 97142 (Mar. 15, 2023), 88 FR 20212 (Apr. 5, 2023) ("Proposed Rule 10 Release").

The MSRB is subject to the Commission's Regulation Systems Compliance and Integrity ("Regulation SCI")[2], which imposes strict requirements, including in the area of cybersecurity, on the EMMA website and other MSRB systems that are critical to the functioning of the U.S. securities markets. The MSRB maintains a comprehensive control environment designed to address the security of its systems, including cybersecurity risks affecting those systems.

The MSRB supports the Commission's goals to protect investors in the U.S. securities markets and the markets themselves from cybersecurity risks. As the Commission noted in the Proposal, entities in the U.S. securities markets rely on technology systems to perform key functions and these systems are a target for threat actors. The MSRB is concerned about certain aspects of proposed Rule 10, however, and believes that certain modifications are necessary to ensure that the rule has its intended effect.

The MSRB's comments and suggestions are described below and relate to:

- the broad scope of key definitions,
- the prescriptive requirements regarding the contents of written contracts between covered entities and their service providers,
- the requirement that covered entities publicly disclose cybersecurity risks,
- the lack of an exception to delay public disclosure of a significant cybersecurity incident for legitimate security concerns, and
- the need to harmonize proposed Rule 10 with Regulation SCI to limit overlap and complexity for entities that are already subject to Regulation SCI.

I. Scope of Proposed Rule 10

The MSRB believes that the scope of proposed Rule 10 is overly broad, which could diminish the effectiveness of the rule by diverting a disproportionate amount of covered entities' efforts to information and systems that have little or no relevance to the U.S. securities markets. Proposed Rule 10 includes two key definitions that establish the scope of the rule's requirements – "information" and "information systems." Information is defined in Section (a)(6) of proposed Rule 10 as "any records or data related to the market entity's business residing on the market entity's information systems, including, for example, personal information received, maintained, created, or processed by the market entity."[3] Information systems are defined in Section (a)(7) of proposed Rule 10 as "the information resources owned or used by the market entity, including, for example, physical or virtual infrastructure controlled by the information resources, or components thereof, organized for the collection, processing,

---

[2] 17 CFR 242.1000-1007.

[3] Proposed Rule 10 Release, 88 FR at 20343.

maintenance, use, sharing, dissemination, or disposition of the covered entity's information to maintain or support the covered entity's operations."[4]

The MSRB believes that these definitions would subject more information and systems of covered entities to proposed Rule 10's requirements than is necessary to accomplish the Proposal's goals. The definitions do not appear to contain any meaningful limitations and seemingly capture nearly all systems of a covered entity. For example, the defined term "information systems" could be understood to cover as information resources the third-party software-as-a-service (SaaS) solutions that the MSRB uses for employee rewards/recognition and employee expense reimbursement, although those SaaS solutions have no apparent relevance to the U.S. securities markets or the MSRB's ability to fulfill its role as a self-regulatory organization. In addition, the defined term "information," while using "personal information" as an example of the records and data that it covers, seemingly includes information that the MSRB maintains that is unrelated to the U.S. securities markets (*e.g.*, anonymized data from internal employee surveys) and information that the MSRB publicly discloses.

As a result of their breadth, the definitions of information and information systems fail to appropriately reflect the prioritization of a covered entity's critical systems and most sensitive information. The Proposal frequently cites to publications by the National Institute of Standards and Technology ("NIST"), and the Commission indicates that in designing proposed Rule 10's requirements, it considered several sources, including NIST's Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Framework").[5] The NIST Framework provides that its first core element is to "identify," among other things, assets "that enable the organization to achieve business purposes . . . consistent with their relative importance to organizational objectives and the organization's risk strategy."[6] The NIST Framework further provides that "resources (*e.g.*, hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value."[7]

Proposed Rule 10 deviates from these aspects of this recognized industry standard. The definitions of information and information systems would apply a one-size-fits-all approach – imposing the rule's rigorous requirements on nearly all information and systems of a covered entity regardless of their criticality or importance to the covered entity or the fair, orderly and

---

4 Id. at 20343 – 44.

5 Id. at 20226 n.117.

6 NIST Framework, at 24, Table 2: Framework Core (ID, AM) (Apr. 2018), *available at,* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

7 Id. at Table 2: Framework Core (ID, AM-5).

efficient functioning of the U.S. securities markets. The NIST Framework itself recognizes that "[t]he Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure." [8] The broad scope of proposed Rule 10 would not reflect the appropriate prioritization and classification of a covered entity's information and systems.

The overly broad definitions also would render much of proposed Rule 10 difficult for a covered entity to implement.[9] For example, if nearly all of a covered entity's systems are covered by the rule, then nearly all of a covered entity's service providers would be subject to the rule's rigorous service provider oversight requirements in Section (b)(1)(iii)(B) (including, as described above, service providers that pose little to no risk of impacting the covered entity's operations) and nearly all of a covered entity's information would be subject to the information protection requirements in Section (b)(1)(iii)(A).[10]

Without any meaningful limitations in these definitions, covered entities would be required to spend a disproportionate amount of time and resources on complying with proposed Rule 10's requirements in regard to information and systems that have little or no relevance to the U.S. securities markets. The NIST Framework indicates that "[o]rganizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent,"[11] but proposed Rule 10 would not provide entities with this flexibility and instead would impose strict requirements on seemingly all information and systems of a covered entity.

The MSRB suggests that the Commission revise the definitions of information and information systems in proposed Rule 10 to reflect a risk-based approach that tailors the scope of the rule to cover only those systems that are critical to the entity's operations and which, if breached, would be likely to cause some harm to investors or the fair, orderly and efficient functioning of the U.S. securities markets.

---

8 Id. at vi, Executive Summary.

9 The Commission indicated in the Proposal that it did not expect the MSRB would incur significant costs as a result of complying with the policies and procedures requirements of proposed Rule 10 because the MSRB is already subject to Regulation SCI and has strong incentives to invest in a comprehensive cybersecurity program. Proposed Rule 10 Release, 88 FR at 20303. While the MSRB already invests significant resources towards its cybersecurity program, proposed Rule 10 would be much broader than Regulation SCI and would result in significant additional costs to the MSRB.

10 Id. at 20344.

11 NIST Framework, at vi, Executive Summary.

II. Third-Party Contractual Provisions

The MSRB supports the Commission's efforts to require oversight of service providers by covered entities. It is important for covered entities to effectively oversee service providers because, while their use may allow covered entities to leverage secure technologies and platforms to enhance their cybersecurity, service providers also may present cybersecurity risks to a covered entity. The MSRB's policies and procedures relating to vendor management are designed to mitigate these risks.

The MSRB believes that proposed Rule 10's prescriptive requirements regarding the contents of covered entities' written contracts with service providers are unlikely to achieve the Proposal's goals and may result in unintended consequences. The MSRB suggests that the Commission instead take a more principles-based approach that requires covered entities to conduct a level of oversight of service providers that is proportionate to the cybersecurity risks they pose to the covered entity, investors, or the U.S. securities markets.

Section (b)(1)(iii)(B) of proposed Rule 10 requires oversight by covered entities "of service providers that receive, maintain, or process the covered entity's information, or are otherwise permitted to access the covered entity's information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider, through which the service providers are required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of [proposed Rule 10], that are designed to protect the covered entity's information systems and information residing on those systems."[12]

Depending on its size, a covered entity may have hundreds of service providers that support its systems in different ways, calling for different levels of contractual protection for the covered entity. A covered entity, through its knowledge of its own cybersecurity risks and by conducting due diligence on potential service providers, is in the best position to determine which contract provisions are needed with a particular service provider in order to protect the entity's information and systems and facilitate sufficient oversight.

Proposed Rule 10's requirements regarding the contents of the contract between a covered entity and its service provider also could lead to outcomes that negatively impact cybersecurity risk management and, accordingly, are inconsistent with the Proposal's goals. For example, the rule may force a covered entity to use a less secure or less reliable service provider because that provider will agree to the rule-required contract provisions (while a more secure or more reliable vendor will not) or a covered entity may be unable to leverage a third-party technology or platform that is more secure than it could develop in-house because that third-party will not agree to them.

---

12 Proposed Rule 10 Release, 88 FR at 20344.

Further, the contract provisions that a particular service provider is willing to accept may not be an effective indicator of the provider's controls. Highly secure service providers with large customer bases may be unwilling to agree to contract provisions that deviate from their standard language, but these providers may offer more secure systems to a covered entity than others that will agree.

III. Public Disclosure of Cybersecurity Risks

The MSRB is concerned that the requirement to publicly disclose cybersecurity risks and covered entities' responses to these risks could have a negative effect on cybersecurity in the U.S. securities markets. Section (d)(1)(i) of proposed Rule 10 requires a covered entity to provide "a summary description of the cybersecurity risks that could materially affect the covered entity's business and operations and how the covered entity assesses, prioritizes, and addresses those cybersecurity risks."[13]

In complying with proposed Rule 10's requirement to disclose cybersecurity risks that could materially affect it, a covered entity may be forced to publicly highlight valuable information that resides on its systems. Threat actors may not have been aware of such information and could use the disclosures to evaluate potential targets. In disclosing how it assesses, prioritizes and addresses cybersecurity risks, a covered entity also could be forced to disclose information relating to specific security practices or cybersecurity vulnerabilities, which could encourage a breach or provide a roadmap for threat actors to execute a cyber-attack.

While the Commission acknowledges certain of these risks in the Proposal, it is not clear how a covered entity could provide meaningful disclosure under proposed Rule 10 without disclosing information that may increase its cybersecurity risk. If a covered entity provided a disclosure that was so high-level that it did not disclose such information, it is unlikely to provide meaningful information to market participants, thus eroding the Commission's rationale for the disclosure. The MSRB recommends that the Commission not adopt a requirement in proposed Rule 10 for public disclosure of cybersecurity risks.

IV. Lack of an Exception to Delay Public Disclosure of Significant Cybersecurity Events

The MSRB is concerned that proposed Rule 10's requirement to promptly disclose significant cybersecurity incidents to the public would not allow a covered entity to delay such disclosure if legitimate security concerns warrant such a delay. Section (d)(1)(ii) of proposed Rule 10 requires a covered entity to "provide a summary description of each significant cybersecurity incident that has occurred during the current or previous calendar year,"[14] and Section (d)(4)

---

13 Id. at 20345.

14 Id.

requires a covered entity to "promptly provide an updated disclosure . . . after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes."[15]

The MSRB agrees that prompt disclosure of significant cybersecurity incidents may be beneficial so that affected market participants can take proactive or remedial measures in response. However, there may be instances where prompt disclosure could further harm market participants and the covered entity. If a covered entity is forced to publicly disclose a significant cybersecurity incident before it is able to effectively remediate it, that disclosure could result in further harm once the threat actor becomes aware that its efforts have been discovered. Premature public disclosure also may increase the likelihood of additional attacks by other threat actors once they are alerted that the covered entity may have a vulnerability.

In adopting Regulation SCI, the Commission acknowledged commenters' concerns that prompt disclosure of security-related events could be sensitive and raise security concerns, and permitted a delay in dissemination of security-related events if an entity determined that dissemination would compromise the security of its systems or an investigation of the event and documented the reason for such determination.[16] The MSRB recommends that the Commission include a similar provision in proposed Rule 10 through which a covered entity can delay public disclosure of a significant cybersecurity incident if such a delay is needed for legitimate security concerns.

V. Harmonization with Regulation SCI

As the Commission noted in the Proposal, the MSRB and certain other covered entities that would be subject to proposed Rule 10 are also "SCI entities" subject to Regulation SCI. [17] Regulation SCI imposes requirements on certain systems, called "SCI systems," which are any "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."[18] Regulation SCI's requirements relating to security also apply to indirect SCI systems, which are

---

15 Id.

16 Regulation Systems Compliance and Integrity, Exchange Act Release No. 73639 (Nov. 19, 2014), 79 FR 72252, 72334 (Dec. 5, 2014) ("Regulation SCI 2014 Adopting Release").

17 17 CFR 242.1000.

18 Id.

any systems that "if breached, would be reasonably likely to pose a security threat to SCI systems."[19]

Accordingly, systems of the MSRB and other SCI entities that the SEC considers "central to the functioning of the U.S. securities markets"[20] are already subject to rigorous requirements in Regulation SCI. Those requirements include security-related requirements such as: (i) maintaining and enforcing policies and procedures reasonably designed to ensure that SCI systems and indirect SCI systems have levels of security adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets,[21] (ii) reporting to the Commission of security-related events, referred to as systems intrusions,[22] and (iii) dissemination of information to impacted market participants regarding systems intrusions.[23]

The Commission also has separately proposed amendments to Regulation SCI to enhance requirements relating to, among other things, third party/vendor management and cybersecurity.[24] The MSRB is supportive of the Commission's efforts with respect to Regulation SCI and believes the Commission's adoption of Regulation SCI strengthened the technology infrastructure of the U.S. securities markets. While it would require a significant effort to comply with certain of the enhanced requirements in the proposed amendments to Regulation SCI, the MSRB believes the amendments generally are appropriately tailored to SCI systems and indirect SCI systems.

Proposed Rule 10 would overlap significantly with Regulation SCI's existing and proposed requirements. One example, among others, of the overlap between Regulation SCI and proposed Rule 10 relates to incident reporting to the Commission and market participants.

---

19 Id.

20 Regulation SCI 2014 Adopting Release, 79 FR at 72273.

21 17 CFR 242.1001 (a)(1).

22 Id. at 242.1002(b). Systems intrusions are defined in Regulation SCI as "any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity." Id. at 242.1000. The Commission's proposed amendments to Regulation SCI would increase the scope of the definition of systems intrusions to incorporate additional incidents. Regulation Systems Compliance and Integrity, Exchange Act Release No. 97143 (Mar. 15, 2023), 88 FR 23146, 23269 (Apr. 14, 2023) ("Regulation SCI 2023 Proposing Release").

23 17 CFR 242.1002(c).

24 Regulation SCI 2023 Proposing Release, 88 FR at 23146.

Under Regulation SCI, SCI entities are required to report systems intrusions to the Commission. The reporting obligations for a systems intrusion include an immediate notification, a written notification within twenty-four hours, regular updates, and interim and/or final written notifications.[25] Where the reporting is required electronically under Regulation SCI (as is the case for written notifications), such reporting must be done through Form SCI which is filed on the SEC's electronic form filing system (EFFS).[26] SCI entities also must promptly disseminate certain information about a systems intrusion to its members or participants that may have been affected by it, unless the SCI entity determines that dissemination of such information would likely compromise the security of its SCI systems or indirect SCI systems, or an investigation of the systems intrusion.[27]

Under proposed Rule 10, covered entities would be required to report significant cybersecurity incidents to the Commission. The reporting obligations would include an immediate written electronic notice, a prompt report made no later than forty-eight hours, and prompt updates to that report made no later than forty-eight hours following circumstances identified in the rule.[28] Aside from the immediate written electronic notice, the other reporting under proposed Rule 10 would be done through the Commission's Electronic Data Gathering, Analysis, and Retrieval System ("EDGAR system").[29] Under proposed Rule 10, covered entities would also be required to promptly publicly disclose certain information about significant cybersecurity events through the EDGAR system and on their websites.[30]

In some instances, an incident that constitutes a significant cybersecurity incident under proposed Rule 10 also would constitute a systems intrusion under Regulation SCI. In such cases,

---

25 17 CFR 242.1002(b)(1)-(4). These reporting requirements do not apply to systems intrusions that the SCI entity reasonably estimates would have no or a de minimis impact on its operations or on market participants; instead, such systems intrusions are reported to the Commission on a quarterly basis. Id. at (b)(5). However, the SEC's proposed amendments to Regulation SCI would eliminate this "de minimis" exception for systems intrusions. Regulation SCI 2023 Proposing Release, 88 FR at 23269.

26 17 CFR 242.1006.

27 Id. at 242.1002 (c)(2), (3). The market dissemination requirements do not apply to systems intrusions that the SCI entity reasonably estimates would have no or a de minimis impact on its operations or on market participants. Id. at (c)(4).

28 Proposed Rule 10 Release, 88 FR at 20344-45.

29 Id. at 20345.

30 Id.

a covered entity would spend a significant amount of time, effort and resources complying with the different reporting requirements in proposed Rule 10 and Regulation SCI. Each rule would require different information to be reported to the Commission at different time intervals using different Commission systems.

While navigating these Commission reporting requirements, an entity also would need to disclose certain information publicly under proposed Rule 10 through an EDGAR filing and on the entity's website, and disseminate different information to affected market participants under Regulation SCI. Because Rule 10 does not include an exception to delay public disclosure of significant cybersecurity incidents for legitimate security concerns, if an entity determines to delay dissemination of information to market participants under Regulation SCI because such dissemination would likely compromise the security of its SCI systems or indirect SCI systems, or an investigation of the systems intrusion, the SCI entity would nonetheless be required to disclose that information publicly under proposed Rule 10. This result would effectively nullify an exception that the Commission provided in Regulation SCI.

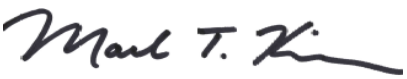
The efforts to comply with these differing requirements for incident reporting to the Commission and incident disclosure to the public and market participants could divert time and attention of personnel and, accordingly, detract from incident response and remediation during a critical time for an entity. As seen in this example, two distinct rules covering similar subject matter are likely to introduce a significant compliance burden on covered entities.

If the Commission decides that applying proposed Rule 10 to SCI entities is necessary, the MSRB recommends that the Commission consider ways to harmonize proposed Rule 10 with Regulation SCI to avoid unnecessary overlap and complexity for entities that are subject to both Regulation SCI and proposed Rule 10. At a minimum, for example, the MSRB suggests that the Commission exempt SCI entities from the reporting requirements of proposed Rule 10 with respect to SCI systems and indirect SCI systems.

VI. Conclusion

The MSRB appreciates the opportunity to provide comments to the Commission on the Proposal. Please contact Jacob Lesser, General Counsel, at 202-838-1395 if you would like to discuss the MSRB's comments or have any questions.

Sincerely,



Mark T. Kim
Chief Executive Officer

cc: David Sanchez, Director, Office of Municipal Securities