DTCC
ADVANCING FINANCIAL MARKETS. TOGETHER.™

Nashira W. Spencer
Managing Director &
Chief Security Officer

DTCC Jersey City
570 Washington Blvd
Jersey City, NJ 07310

Tel: +1 212 855 1613
nspencer@dtcc.com

June 5, 2023

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

VIA EMAIL: rule-comments@sec.gov

RE:

File No. S7-06-23; Release No. 34-97142; 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 No. S7-07-23; Release No. 34-97143; Regulation Systems Compliance and Integrity

Dear Ms. Countryman:

The Depository Trust & Clearing Corporation ("DTCC"), on behalf of its registered clearing agency subsidiaries, The Depository Trust Company ("DTC"), Fixed Income Clearing Corporation ("FICC"), and National Securities Clearing Corporation ("NSCC"); its exempt clearing agency subsidiary, DTCC ITP Matching (US) LLC ("DTCC ITP Matching"); and its registered securities-based swap data repository ("SBSDR") subsidiary, DTCC Data Repository (U.S.) LLC ("DDR"), appreciates the opportunity to comment on the proposed cybersecurity risk management rule ("Proposed Rule 10" or "Proposal") issued by the Securities and Exchange Commission ("SEC" or "Commission") on March 15, 2023.[1]

Background

DTCC is the parent company of DTC, FICC, NSCC, DTCC ITP Matching, and DDR. DTC is a registered clearing agency and the U.S. central securities depository, providing settlement services for virtually all equity, corporate and municipal debt trades, and money market instruments in the United States. FICC and NSCC are registered clearing agencies and central counterparties ("CCPs") providing clearing, settlement, risk management, and CCP services for trades in the U.S. cash securities markets. Each registered clearing agency has been designated as a systemically important financial market utility ("SIFMU") by the Financial Stability Oversight Council pursuant to Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank Act").[2]

[1] See Proposed Rule 10 Release No. 34-97142; File No. S7-06-23 (March 15, 2023), available at https://www.sec.gov/rules/proposed/2023/34-97142.pdf.

[2] Additionally, DTC, FICC, and NSCC are registered clearing agencies under the Securities Exchange Act of 1934, as amended, and, as such, are supervised by the Commission. In addition, DTC also licensed as a New York Limited Purpose Trust Company and state member bank of the Federal Reserve System and, as such, is subject to supervision and examination by the Federal Reserve Bank of New York under delegated authority from the Board of Governors of the Federal Reserve System and the New York State Department of Financial Services.

DTCC ITP Matching is a wholly-owned subsidiary of DTCC ITP LLC, a Delaware limited liability company controlled by its sole member, DTCC. DTCC ITP Matching has received a Commission exemption from registration as a clearing agency to operate as a central matching service provider ("CMSP").

DDR, as part of DTCC's Global Trade Repository service, provides transaction reporting services for derivatives in the United States and Canada. DDR is registered as an SBSDR with the SEC, is provisionally registered as a swap data repository ("SDR") with the Commodity Futures Trading Commission ("CFTC"), and is recognized or designated by Canadian regulators to provide derivatives reporting services in all Canadian provinces and territories.

Executive summary

DTCC, through its subsidiaries, is the largest post-trade market infrastructure for the global financial services industry and supports its mission to protect clients and the broader financial markets. Given DTCC's critical role in the industry, we maintain a robust cybersecurity program and invest in innovative cyber solutions to protect our services against malicious actors and cyberattacks. DTCC has a comprehensive cyber resilience program, which includes internal cybersecurity policies and procedures as well as thorough system safeguards and testing programs that apply across its business areas. Further, DTCC's cybersecurity services (e.g., vulnerability management, risk assessments, identity, and access management) apply to and are conducted across its business areas in a manner that is proportionate to the risks inherent to its business information and applications. The delivery of security services at the enterprise-level promotes consistency of cyber risk controls across business areas, enables efficient deployment of cyber expertise and resources, and decreases fragmentation of the cyber risk management frameworks utilized by financial institutions. This enterprise-level framework is intended to strengthen our cyber defenses, mitigate risk, maintain cyber resilience, including rapidly but safely recovering from a cyberattack (among other types of disruptive events) and adapting to the everchanging cyber threat landscape.

An ever-changing risk landscape magnifies the importance of operational resilience – the ability of registrants to anticipate and continue to provide its critical services regardless of the nature or origin of a disruptive event, including cybersecurity events. DTCC recognizes the need for financial institutions' cybersecurity programs to evolve as new and increasing threats emerge and appreciates the Commission's continued efforts to strengthen the cyber resiliency of the U.S. securities market in light of the changing environment. Although we recognize that specificity can often bring clarity to requirements, we note that it can also introduce regulatory uncertainty and unintended consequences. Moreover, such regulatory uncertainty and unintended consequences are compounded when affected entities must respond to multiple proposed rulemakings that have considerable overlap in scope, purpose, and applicability among themselves and with existing requirements. For example, Proposed Rule 10 and the Commission's Regulation Systems Compliance and Integrity ("Reg SCI"), current and as proposed to be amended ("Proposed Reg SCI"), are sufficiently similar in some ways and different in others to create a substantial amount of complexity and confusion in implementation for the entities that would be subject to both rules, including all of the aforementioned DTCC subsidiaries.[3] Accordingly, DTCC emphasizes the importance of global coordination and alignment to industry standards and best practices to promote a solid foundation for cybersecurity practices within the securities markets. To this end, as discussed in detail below, we believe there are a few aspects of Proposed Rule 10 that the Commission should reconsider or provide further refinement and flexibility, in order to strengthen the rule text and avoid confusion for covered entities during implementation.

Discussion of specific comments

1. *After comparing the two proposals, DTCC believes that Proposed Rule 10 is redundant in scope and outcome for the entities that are or will be subject to Reg SCI (if the proposed amendments are adopted) and therefore the costs and burdens Proposed Rule 10 would impose on such entities, including the affected DTCC entities, are not fully*

[3] DTCC provides comments on Proposed Reg SCI in this letter to the extent they relate to any comments on Proposed Rule 10. DTCC expects to submit a separate comment letter focusing on Proposed Reg SCI by its comment deadline of June 13, 2023. See Proposed SCI Release No. 34-97143; File No. S7-07-23 (March 15, 2023), available at https://www.sec.gov/rules/proposed/2023/34-97143.pdf. For simplicity, any references in this letter broadly to "Reg SCI" will mean both the current rule and as it is proposed to be amended.

explained or justified. To the extent the Commission believes Proposed Rule 10 is still appropriate for SCI entities, the Commission must explain more clearly, using practical examples as opposed to high-level and conclusory statements, how affected entities should navigate the varying terminology and processes of the two proposals in a manner that avoids unnecessary regulatory uncertainty and associated burden and costs (generally responsive to questions 91, 92, 94, and 95 of the Proposal).

Proposed Rule 10 and Reg SCI both address cybersecurity risk management to achieve intended outcomes of safe and efficient markets at entities like DTCC's subsidiaries, but from slightly different perspectives. Reg SCI addresses operational risk management generally, which includes cybersecurity risk management, for the SCI systems that have been identified as directly supporting any core market functions (and, for purposes of security standards, for indirect SCI systems). In contrast, Rule 10 proposes to only focus on cybersecurity risk, albeit across a broader set of information systems (and the information that would reside on such systems) than Reg SCI. The Commission explains that there is a practical difference in scope, where Reg SCI is focused on entities' "operational capability and the maintenance of fair and orderly markets" but Rule 10 "would have a broader scope than Regulation SCI…because it would require Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks" and that unlike Reg SCI, "these requirements would therefore cover SCI systems, indirect SCI systems, and information systems that are not SCI systems or indirect SCI systems."[4] As noted above, operational risk management includes cybersecurity risk management and therefore, from a risk perspective, Reg SCI is broader in scope. To this end, the Commission appears to believe that Proposed Rule 10 covers a "gap" in Reg SCI only with respect to those information systems that are not SCI systems or indirect SCI systems.

DTCC agrees there is technically such a gap between the two rules. For reasons detailed below, DTCC believes, however, that Reg SCI would already ensure the same cyber resilience outcomes at SCI entities that Proposed Rule 10 intends to achieve for its covered entities, rendering Rule 10 redundant for SCI entities. As also detailed below, to the extent the Commission disagrees with DTCC's view (and supporting rationale) that Proposed Rule 10 is redundant for SCI entities and continues to believe Rule 10 should also be applied to SCI entities, DTCC believes Rule 10, as proposed, would create an enormous amount of regulatory uncertainty and associated costs and burden for SCI entities to implement, given that the SEC has not clearly explained where it believes gaps in the cyber resilience outcomes exist between Reg SCI and Rule 10. As such, DTCC recommends that the SEC remove unnecessary redundancy either by scoping SCI entities out from Rule 10 or by providing assurances to SCI entities that compliance with Reg SCI would be considered compliance with Rule 10. To the extent the SEC continues to believe separate application of Rule 10 to SCI entities is warranted, DTCC recommends that the SEC avoid creating regulatory uncertainty and unnecessary implementation burdens by clearly explaining where it believes gaps exist in the cyber resilience outcomes between Reg SCI and Rule 10 and provide the industry with a clear roadmap for entities to navigate the varying terminology and processes of the two rules.

A. Unclear benefits to separate, yet duplicative cybersecurity requirements

As a general matter, after comparing the two proposals, DTCC does not believe Rule 10 would strengthen an SCI entity's cyber resilience beyond what is required under Reg SCI. SCI entities like DTCC's subsidiaries are already required to identify SCI systems that directly support any core market functions and identify indirect SCI systems that, if breached, could pose a security threat to SCI systems. Further, SCI entities are required to establish policies and procedures reasonably designed to ensure that such systems have capacity, integrity, resiliency, availability, and security adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets (which would necessarily include policies and procedures addressing cybersecurity risks, as would be required under Proposed Rule 10). This requirement sets a comprehensive principles-based standard and is coupled with a number of specific and stringent requirements on key aspects of operational risk management. Importantly, Reg SCI applies to indirect SCI systems. To not be scoped in as an indirect SCI system, such system would have to be logically or

[4] Proposed Rule 10 Release, pages 212-213.

physically separate from SCI systems.[5] As such, by definition, information systems that are logically or physically separate from an SCI entity's SCI systems and indirect SCI systems would not be able to affect the SCI entity's ability to, for example, ensure prompt and accurate clearing and settlement of securities transactions or safeguard relevant securities and funds (in the case of a registered clearing agency). Further, in practice, when an SCI entity is determining whether its systems are SCI systems, indirect SCI systems, or neither, it is effectively conducting the risk assessment required by proposed § 242.10(b)(i), and appropriately managing cybersecurity risks by logically or physically separating the relevant systems.[6] It is therefore unclear how Rule 10 would strengthen an SCI entity's cybersecurity risk management given the stringent and effectively broad requirements of Reg SCI.

Relatedly, DTCC firmly believes that the existing Reg SCI requirements for immediate notification, 24-hour subsequent reporting, regular updates on new or incorrect information, and prompt responsible disclosure to the SCI entity's participants/members are more than sufficient to meet the relevant aspects of the Commission's stated objectives for establishing a separate but overlapping reporting program under Proposed Rule 10. The Commission's objective with respect to notification and reporting under Rule 10 "is to improve the Commission's ability to monitor and evaluate the effects of a significant cybersecurity incident on Covered Entities and their customers, counterparties, members, registrants, or users, as well as assess the potential risks affecting financial markets more broadly."[7] The Commission's objective with respect to the public disclosure requirement is to "provide greater transparency to customers, counterparties, registrants, or members of the Covered Entity, or to users of its services, about the Covered Entity's exposure to material harm as a result of a cybersecurity incident, which, in turn, could cause harm to customers, counterparties, members, registrants, or users."[8]

For SCI entities, both objectives are already met under Reg SCI. 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 for "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 Proposed Rule 10's concepts of cybersecurity incidents, as well as details regarding the incident. Form SCI, even if the terminology used in the information request differs from proposed Form SCIR, would effectively provide the Commission with the same information that would be provided through Form SCIR. For example, 24 hours following initial notification, SCI entities would be required to submit information on "(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."[9] Although Form SCIR would focus on specific cybersecurity information, such as a description of the threat actor (if known and applicable), DTCC believes an SCI entity would provide such information under Reg SCI when reporting under sections (a) and (b) of Form SCI.

---

[5] Proposed Reg SCI Release, page 125.

[6] Reg SCI establishes operational risk management requirements for an SCI entity's "SCI systems" as defined under 17 CFR 242.1000, as well as "indirect SCI systems" (and for certain heightened requirements, "critical SCI systems"), the definitions of which leverage the definition of SCI systems. Currently under 17 CFR 242.1000, "*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." As the Commission states in Proposed Reg SCI, "[r]ecognizing that SCI systems may be vulnerable if other types of systems are not physically or logically separated, 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. 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." See Proposed Reg SCI release, page 125.

[7] Proposed Rule 10 Release, page 131.

[8] Proposed Rule 10 Release, page 160.

[9] Proposed Reg SCI Release, page 402.

DTCC recognizes that the Commission has indicated there could be "significant cybersecurity incidents" under Rule 10 that would not meet the current or proposed definition of "SCI event" under Reg SCI, because the reporting requirements under Reg SCI would not be triggered by events impacting information systems that are not SCI systems or indirect SCI systems (and thus indicating that there could be incidents affecting only those systems that are not SCI systems or indirect SCI systems that could meet the definition of a significant cybersecurity incident). However, given that the Commission did not provide specific examples, it is unclear to DTCC how this situation could materialize in practice, given that those information systems that have been preemptively logically or physically separated from SCI systems and indirect SCI systems, by definition, would not be able to disrupt or degrade the SCI entity's core operations (thereby not being able to cause significant harm). For example, any web interface or communication system of an SCI entity that could cause a disruption or degradation to core operations would, by definition, already fall under Reg SCI. We request that the Commission provide specific examples of incidents it would expect to trigger a Rule 10 notification but not a Regulation SCI notification (particularly if the Commission adopts its expanded definition of "systems intrusion" under Proposed Reg SCI). Additionally, to the extent the Commission believes such examples exist, DTCC encourages the Commission to consider whether this would mean that the threshold for a "significant cybersecurity incident" is too low. (DTCC provides specific feedback on the appropriateness of Proposed Rule 10's triggers for notification, reporting, and disclosure from a standalone perspective in Section 4.)

The Commission has also noted specifically that the information from the public disclosures under Proposed Rule 10 "could be used by these persons to manage their own cybersecurity risk and, to the extent they have choice, select a Covered Entity with which to transact or otherwise conduct business."[10] DTCC notes that for market utilities like its subsidiaries, this intended use of publicly disclosed information is already being met by the existing requirements that its subsidiaries are subject to – including 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 Commission's covered clearing agency standards (including operational risk broadly).[11] Further, given that DTCC is not publicly traded (and therefore has no retail investors) and does not have direct client relationships with retail investors, it is unclear how the general public (outside of potential threat actors, as discussed further in Section 3) could readily use such information with respect to DTCC for the purposes identified by the Commission in the proposal.

B. Substantial uncertainty, complexity, and costs of the Proposal

To the extent the Commission disagrees with DTCC's interpretation and related rationale for the two proposals with respect to SCI entities and adopts Proposed Rule 10 as proposed, it would introduce an enormous amount of regulatory uncertainty, implementation complexity, and associated costs to SCI entities. Although the Commission acknowledged that there is duplication or overlap between the two proposals and identified certain areas of overlap at a high level, it did not provide a clear roadmap for entities to navigate the varying terminology and processes of the proposals, such as specific though non-exhaustive examples.[12] Without such clarity, it is difficult for potential covered entities to determine what changes to (or new) policies and procedures would be necessary to comply with the two sets of overlapping requirements.

For example, the Commission stated that a "Covered Entity that implements reasonably designed policies and procedures in compliance with the requirements of Proposed Rule 10 described above that cover its SCI systems and indirect SCI systems should generally satisfy the existing general policies and procedures requirements of Regulation SCI that pertain to cybersecurity" (emphasis added).[13] The Commission, however, has not clearly identified the specific requirements under Reg SCI it considers would "pertain to cybersecurity." Given that Reg SCI only expressly references cybersecurity in two proposed provisions under the Commission's current Proposed Reg SCI (and nowhere in the current rule text), it creates regulatory uncertainty for SCI entities who would need to correctly interpret the Commission unstated views regarding which Reg SCI provisions it meant to cover in its statement. Further, in addition to identifying

---

[10] Proposed Rule 10 Release, page 161.
[11] 17 CFR § 240.17Ad-22(e)23.
[12] For example, what is the practical difference between the "service providers" under Proposed Rule 10 and "third-party providers" under Reg SCI and between the "annual review" under Proposed Rule 10 and the "SCI review" under Reg SCI?
[13] Proposed Rule 10 Release, page 216; a similar statement was made in Proposed Reg SCI Release, page 166.

specific provisions in the final rule, it would important for the Commission to provide sufficient clarity around how entities should attempt to comply with the two sets of requirements in a manner that is not redundant or overly burdensome, such as providing more concrete assurances of substituted compliance.

The Commission also suggested that a "Market Entity could use one comprehensive set of policies and procedures to satisfy the requirements of proposed Rule 10 and the existing and proposed cybersecurity-related requirements of Regulation SCI…, so long as: (1) the cybersecurity-related policies and procedures required under… Regulation SCI fit within and are consistent with the scope of the policies and procedures required under proposed Rule 10; and (2) and the policies and procedures requirements of proposed Rule 10 also address the more narrowly-focused existing and proposed cybersecurity-related policies and procedures requirements under Regulation SCI…" (emphasis added).[14] DTCC notes that this seems to be an acknowledgement that there is inherent redundancy between the two proposals. Further, consistent with DTCC's observation above, SCI entities would need to understand and rely on the Commission's expressed identification of the provisions under Reg SCI that it believes to be consistent with that of Rule 10, in order to determine the changes it may need to make to its existing policies and procedures. For example, DTCC already has an existing cybersecurity program that is aligned with the requirements of Reg SCI (which it would consider to be comprehensive). Without more explicit direction and mapping between the two proposals from the Commission, particularly given the different uses of terminology and framing, we reiterate that it is unclear what changes to (or new) policies and procedures DTCC would need to introduce into existing and longstanding risk management policies and procedures to satisfy Proposed Rule 10. Consistent with the Commission's rationale for suggesting that SCI entities "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," DTCC encourages the Commission to adopt the same terminology and provisions for what it believes to be consistent requirements across its related rulemakings to avoid introducing such confusion to SCI entities.[15]

Moreover, the Commission expressly states that it believes its approach of establishing two separate notification and reporting programs – one under Proposed Rule 10 and the other under Reg SCI – would be appropriate including because the public disclosures or notifications required by Proposed Rule 10 would require "different types of information to be disclosed, largely to different audiences at different times."[16] However, as noted above, it is unclear whether the requested information would be effectively different between "significant cybersecurity incidents" under Form SCIR and "systems intrusions" under Form SCI. Further, as also noted above, the Commission's stated objective of disclosure to provide investors the ability to manage their own cybersecurity risks and select covered entities with which to transact or otherwise conduct business is not applicable to market utilities. Under Reg SCI, entities already provide information to the Commission and their members/participants. It is also unclear how the complexities and associated costs and burden introduced by different reporting timing under the two regimes is reasonable.

Finally, to the extent the Commission continues to believe there are true differences between the two reporting programs, it also does not appear to explain why it believes these differences are necessary to achieve the stated purpose of the rulemaking, particularly given the concerted global and domestic efforts to harmonize cybersecurity incident reporting in recognition of the significant burden placed on entities to report to sometimes multiple regulators in various

[14] Proposed Rule 10 Release, page 213.
[15] Proposed Reg SCI Release, page 116.
[16] Proposed Rule 10 Release, page 209.

forms and at varying time intervals.[17, 18] For the Commission to require entities to submit additional and separate notice, reporting, and disclosure of incidents, the vast majority – if not all – of which, would have already been covered under existing SEC requirements would especially seem inconsistent with such harmonization efforts. It would be more efficient if the Commission harmonizes the two programs into a single notification and reporting program that would be able to serve both purposes. An entity should be required to prioritize its resources around incident response and remediation, rather than redundant compliance reporting exercises.[19] (DTCC provides specific feedback on the appropriateness of Proposed Rule 10's disclosure requirements from a broader perspective in Section 3.)

C. DTCC recommendation to remove regulatory uncertainty created by Proposed Rule 10 for SCI entities

To this end, DTCC strongly encourages the SEC to provide regulatory certainty to entities that would be subject to multiple overlapping rules and consider scoping "SCI entities" out from Rule 10, or provide certainty that compliance with Reg SCI constitutes compliance with Rule 10.

To the extent the SEC continues to believe that there is a need to apply Rule 10 to SCI entities, it would be helpful to understand where specifically the SEC believes there to be a gap in the expected outcome between the two sets of requirements. From DTCC's review of the two proposals, it appears that the Commission believes a "gap" exists between the two rules with respect to addressing the cybersecurity risks of information systems that are not SCI systems or indirect SCI systems (i.e., systems that are logically or physically separated from critical services and core operations).[20] If so, DTCC believes the proposed general requirement for a covered entity 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 sufficient to address this gap and allow the covered entity flexibility to adopt a risk-based approach to managing the cybersecurity risks from these non-critical systems.[21] To the extent the Commission believes there are other gaps between the outcome expected from Regulation SCI (existing and as proposed) and Proposed Rule 10 that must be filled by prescriptive requirements, DTCC requests that the SEC clarify where specifically it believes such gaps exist and provide a clear roadmap for entities to navigate the varying terminology and processes of the proposals.[22]

---

[17] For example, when the Federal banking agencies finalized computer-security incident notification requirements for banking organizations and bank service providers in November 2021 ("Banking Notification Rule"), the banking agencies deliberately scoped out financial market utilities that were designated as systemically important ("SIFMUs") by the Financial Stability Oversight Council ("FSOC"). The banking agencies accepted DTCC's public comment (among others) raising concerns of overlap between the proposed banking agency rule and existing regulatory notification requirements. The proposed banking agency rule would have scoped DTC in as a "banking organization," which would have subjected DTC to notification requirements that overlapped with Regulation SCI. The banking agencies determined that excluding SEC- and CFTC-supervised SIFMUs from the final banking agency rule "is appropriate because these [SIFMUs] are already subject to incident notification requirements in other federal regulations," and that this change (in addition to others) is "intended to address comments and reduce over- and unnecessary notification by both banking organizations and bank service providers." See 86 FR 66424, at 66426 and 66427.

[18] In addition to recent efforts around harmonizing cybersecurity reporting, Title VIII of the 2010 Dodd-Frank Act also contains a relatively analogous recognition of and attempt to limit burden on reporting entities. Under Section 809, FSOC and the Federal Reserve Board must coordinate requests for information, reports, or records from SIFMUs, first with the SIFMUs' Title VIII Supervisory Agency ("SA") to determine if such information is already available from the SA, before requests can be made directly to the SIFMU.

[19] See Recommendation 4 of the Financial Stability Board's (FSB's) *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting*: Financial authorities should implement incremental reporting requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of bringing the incident under control.

[20] In the Proposed Reg SCI release (page 162), the Commission's states that "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," but that these policies and procedures "do not and would not apply to other systems maintained by an SCI entity."

[21] This would be not unlike how the current general operational risk management standard under 17 CFR 240.17Ad-22(e)(17) for "covered clearing agencies" can work in tandem with the more specific requirements under Reg SCI (currently and as proposed to be amended) for SCI entities which include covered clearing agencies.

[22] For example, what is the practical difference between the "service providers" under Proposed Rule 10 and "third-party providers" under Reg SCI.

2. *DTCC recommends that the Commission align the timing of and requirements in the Proposal with global and domestic efforts to harmonize and enhance cybersecurity reporting requirements.*

DTCC recommends that the Commission further collaborate with other agencies that are active in cyber resilience and reconcile and harmonize what the SEC is proposing with existing and upcoming cybersecurity requirements. While the Commission is focused on U.S. Market Entities, many Market Entities regulated by the Commission are global organizations and therefore, the Commission should consider global efforts to harmonize cyber incident reporting requirements.

For example, as referenced earlier, in April 2023, the Financial Stability Board ("FSB"), which includes the SEC as a member, published its final report on *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting* ("FSB Report").[23] The FSB Report contains 16 recommendations that aim to promote convergence among cyber incident reporting frameworks, while recognizing that a one-size-fits-all approach is not feasible. It expressly 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.[24] Where relevant in the sections below, DTCC identifies the specific FSB Report Recommendations with which the Proposal seems to conflict. In March 2022, Congress also enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), which, among other goals, aims to harmonize federal incident reporting requirements and establish interagency information sharing requirements.[25] In particular, CIRCIA requires the Cybersecurity and Infrastructure Security Agency ("CISA") to develop and implement regulations requiring covered entities to report certain cyber incidents to CISA and requires the Department of Homeland Security ("DHS") to establish and chair an intergovernmental Cyber Incident Reporting Council to coordinate, deconflict, and harmonize federal incident reporting requirements. CISA is currently reviewing the hundreds of comments it has received since the start of its rulemaking process and expects to publish a draft notice of proposed rulemaking by the end of March 2024.[26]

DTCC recognizes that, while the scope of CIRCIA is more limited than Proposed Rule 10, there would be significant overlap for those firms that would be subject to both incident reporting requirements and significant implementation challenges if these requirements are not aligned. Such firms would also incur unnecessary costs and burden, should they be required to implement changes to their operational (including cybersecurity) risk management policies and procedures to comply with Rule 10 when it is adopted, and then potentially immediately be required to do so again when CISA finalizes its rulemaking. Implementing changes to a firm's policies and procedures may sound simple, but involves a complex, iterative, costly, and resource intensive process. For example, DTCC and other similarly situated SCI entities must review their existing operational (including cybersecurity) risk management policies and procedures against final Rule 10; consult the relevant SEC supervisory and policy teams to understand Rule 10, if it is adopted without the changes or additional clarity that DTCC seeks; determine the changes that are necessary to comply with Rule 10; ensure that such changes would not put themselves in conflict with other U.S. – including any amendments to Reg SCI – or global regulatory requirements to which they are also subject; and execute on such changes. Changes may be needed with respect to additional or revisions to documentation; new or changes to systems, processes, procedures, and controls; changes to organizational and staffing responsibilities; and training to global staff on such changes. Each step of this change management process is subject to rigorous governance and due diligence review. These steps are necessary and important to ensure that any changes made to systems, processes, procedures, and controls are implemented as planned, particularly given that any changes to an SCI entity's systems that support critical market operations or services present a source of operational risk in and of itself.

---

[23] DTCC has participated in several public/private working groups focused on Cyber Incident Reporting and more specifically with the FSB Cyber Incident Reporting working group on the development of this 2023 FSB Report and the 2020 FSB Effective Practices for Cyber Incident Response and Recovery. https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/

[24] FSB Report, Recommendation 2.

[25] Public Law 117–103, Div. Y (2022) (to be codified at 6 U.S.C. 681–681g).

[26] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

We thus encourage the Commission avoid imposing unnecessary costs, burden, and operational risks to affected entities and refrain from establishing a new and separate cybersecurity notification regime at least while the industry awaits the implementation of CIRCIA.

3. *Requiring covered entities to provide public disclosure of significant cybersecurity incidents increases the risk of substantial harm to the covered entity experiencing the incident and the U.S. securities markets more broadly, without offsetting benefits; such risks significantly increase should incidents need to be disclosed before they have been resolved.*

As noted earlier, the Proposal would establish a requirement for immediate notification, 48-hour subsequent reporting, updates to the SEC when new material is discovered, and public disclosure of "significant cybersecurity incidents" likely before the incidents have been fully remediated. DTCC recognizes the importance of timely notification to the SEC with respect to significant incidents; its four current SCI entities (DTC, FICC, NSCC, and ITP Matching) have had processes and procedures to immediately notify the SEC of a broader set of incidents (i.e., "SCI events") since Reg SCI's adoption in 2014. These entities are also already subject to 24-hour subsequent reporting of SCI events, updates to the SEC where new material is discovered, and prompt disclosure of such incidents to its affected participants/members (or in the case of "major SCI events," to all its participants/members). As noted above, DTCC primarily believes that the incident notification, reporting, and disclosure requirements under Reg SCI already achieve the outcomes of Proposed Rule 10's stated objectives and encourages the Commission to consider compliance with Regulation SCI's requirements to be sufficiently compliant with the Rule 10 incident notification, reporting, or disclosure requirements. There should only be one streamlined process to achieve essentially the same expected outcomes of both rules.

Additionally, as a general matter, DTCC does not support public disclosure of significant cybersecurity incidents, even as "a summary description" under the Proposal. As described further below, DTCC believes the costs and risks would far outweigh any perceived benefits of such disclosure, especially should these disclosures be required before the incident has been fully remediated. As such, DTCC does not believe the Commission should adopt a public disclosure requirement for significant cybersecurity incidents. However, to the extent the Commission disagrees with DTCC's views and rationale (detailed below), DTCC firmly believes the Commission should allow entities the flexibility to delay public disclosure until the incident has been fully investigated, remediated, and resolved. To not do so would risk substantial harm to the securities markets, investors, and the affected covered entity.

A. Material risks of public disclosure of significant cybersecurity incidents, including market stability implications

There are material risks of harm to market stability, investors, and the reporting entity, from public disclosure of significant cybersecurity incidents, even in summary form and especially if the disclosure is required while the incident is still being investigated, remediated, and resolved.

Public disclosures (and the detailed non-public disclosures to the Commission, if not adequately protected from intrusion) could serve as a roadmap for cybersecurity threat actors to gain a foothold into critical infrastructure. Nation-state threat actors actively look for vulnerabilities in critical infrastructure to exploit and leverage against countries that operate against their own interests. Use of a well-known, expected, and centralized location to maintain both confidentially reported information and public disclosures of ongoing incidents, such as the SEC's EDGAR database, would create single point of access to such useful information on vulnerabilities in the U.S. financial sector and serve as an appealing target for threat actors.[27] With respect to the confidential detailed responses to Part I of Form SCIR that would be reported to EDGAR, DTCC is concerned with the risk that such information could be a clear target for

[27] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

malicious attacks.[28, 29] Further, from a general market stability perspective, DTCC observes that a requirement to rush public reporting of incidents, regardless of whether a company has successfully managed and recovered from an incident, could seriously mislead investors and the public about the degree of actual risk and lead to unintended consequences.

From an individual entity perspective, while the incident is still happening, the entity faces the critical decision of either erring on the side of caution against potential future enforcement actions and reporting incidents prematurely only to meet the Rule 10 deadlines (which can raise the material risks of market panic noted above) versus delaying reporting until more accurate information is acquired (which lowers the risk of unnecessary market panic but raises the risk of being subject to enforcement actions after the fact). From a market stability and investor protection perspective, DTCC believes that entities should be subject to *responsible* disclosure requirements and be able to prioritize market stability concerns and remediation efforts over compliance against potentially harmful public disclosure deadlines. Covered entities must be afforded the time to determine the full impact of the incident and its potential impact to the market, market participants, and individual investors before disclosure of incidents should be considered. DTCC notes that the proposed public disclosure requirement is also duplicative with state data breach notifications and the proposed timeline for reporting is not harmonized with these existing requirements. Every U.S. state and four territories already have data breach notification requirements for consumers. These state requirements also outline what amounts to the equivalent of "significant cybersecurity incidents" that would trigger consumer notification; and in many cases notifications are also required to state agencies, law enforcement, and consumer reporting agencies furthering the stated goal of Proposed Rule 10 notification to consumers and other interested parties without the need for additional regulation.

Finally, we note that our concerns regarding public disclosure are in alignment with comments that the SEC has received in response to previous consultations regarding proposals for public disclosure of cyber incidents, specifically *Cybersecurity, Risk Management, Strategy, Governance and Incident Disclosure (File Number S7-09-22)*, including comments from Microsoft, NYSE, and Nasdaq. The concerns raised in those comment letters are applicable to the Rule 10 proposal and could manifest for Reg SCI entities. We urge the SEC to consider this matter holistically and harmonize where possible.

B. Unclear benefits of public disclosure of significant cybersecurity incidents and hypothetical scenario and response to Form SCIR

Although DTCC agrees that there is value in sharing incident information and threat intelligence, we believe the material risks that would arise in broad public disclosure (particularly before a significant cybersecurity incident has been resolved) far outweigh any perceived benefit that "a summary description" of a significant cybersecurity incident under proposed § 242.10(d)(1)(ii) could yield on top of the notifications, reporting, and information sharing that is already occurring through existing requirements and arrangements (including those that SCI entities are subject to under Reg SCI). As noted above, DTCC believes that the information the SEC already receives on SCI events achieves the SEC's objectives of better understanding the nature and extent of a particular significant cybersecurity incident and the efficacy of an entity's response, assessing the potential cybersecurity risks affecting the U.S. securities markets, and identifying trends across covered entities, particularly if the proposed expansion of "SCI entity" and "SCI intrusion" is adopted.[30] Further, there currently exists a number of threat intelligence reports (e.g., Crowdstrike, IC3) that the

---

[28] On September 20, 2017, the then Chairman of the SEC publicly disclosed that an incident—specifically, a software vulnerability in a component of the agency's EDGAR system—previously detected in 2016 resulted in unauthorized access to non-public information – https://www.sec.gov/files/Eval-of-the-EDGAR-Systems-Governance-and-Incident-Handling-Processes.pdf. See also the SEC's latest OIG report – https://www.sec.gov/files/fy-2022-independent-evaluation-sec-implementation-fisma-2014-report-no-574.pdf.

[29] FSB Recommendation 16: Financial authorities should implement secure forms of incident information handling to ensure protection of sensitive information at all times.

[30] Under Proposed Reg SCI, SEC proposes to expand the definition of "SCI entity" to include all exempt clearing agencies, certain broker/dealers, and SBSDRs (see Proposed Reg SCI Release at page 391). It also proposes to expand the definition of "systems intrusion" under Reg SCI to include cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system; and 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 (see Proposed Reg SCI Release at page 392).

Commission can access to derive industry-wide patterns and information such as nation-state threat actors. Moreover, DTCC believes the Commission has overestimated the potential value of "public" disclosure of summary descriptions of incidents that the Commission foresees for "persons to manage their own cybersecurity risk and, to the extent they have choice, select a Covered Entity with which to transact or otherwise conduct business." DTCC believes the expected value is not only inapplicable to market utilities with no retail investors (as was noted above), but also would generally provide little value with respect to other types of covered entities.

As a concrete example, DTCC leverages and builds on the Commission's hypothetical scenario of a ransomware attack on a registered clearing agency's margin calculation system, which DTCC anticipates would trigger both reporting regimes under Reg SCI and under Proposed Rule 10.[31] If this ransomware attack resulted in the clearing agency's inability to calculate margin obligations for its members until monetary demands are met, there is a risk that the clearing agency's clearing fund becomes under (or over) funded, while the incident is being resolved, even if clearing and settlement operations can continue to function. Should this attack be undertaken by a sophisticated threat actor backed by the resources of a nation-state actor, it would be extremely challenging for the clearing agency to obtain an accurate understanding of, for example, whether any data was stolen, altered, or accessed or used for any other authorized purposes, within 48-hours after initial discovery of the incident and initial notification to the SEC.[32] In order to limit sharing publicly information that may turn out to be erroneous following further investigation, the public disclosure of such an incident will necessarily have to be high-level. With respect to Rule 10's public disclosure a potential summary description regarding this hypothetical scenario could be provided on proposed Question 3 on Part II of Form SCIR:

> *On [Current Date minus 48 hours], a cyber incident occurred on an application responsible for a key clearing and / or settlement process. The incident has not yet been resolved and remediated, and it is not yet determined whether any data were stolen, altered, or accessed or used for any other unauthorized purpose. Certain [ABC Clearing Agency] participants may be affected by the incident until it is resolved, though clearing and settlement continue to operate.*

This type of generic summary could describe the hypothetical scenario above or it could describe an entirely different incident that, through further investigation by the affected entity, is determined to not actually be a significant cybersecurity incident. DTCC anticipates that the latter scenario may occur for those affected entities concerned with potential regulatory enforcement actions (after the fact) that feel pressured to prematurely report incidents out of an abundance of caution. To this end, DTCC does not believe this summary description would enable the public (i.e., those other than the Commission or affected participants/members of an SCI entity, who would already receive notification and reporting) to better assess ABC Clearing Agency's cyber resilience. It would not serve any purpose other than elevating the risks described in the previous section, including alerting other potential threat actors to an ongoing issue that it may not otherwise be aware of (given the hypothetical example that clearance and settlement would continue to operate), creating panic and unease for securities market participants, and dividing the affected entity's resources and focus between remediating the incident and ensuring enforcement actions will not materialize after the fact. Although summary descriptions of incidents that have been fully remediated have less risk of leading to these harmful outcomes, there is still little to be gained by disclosing such information. As emphasized further below, however, to require covered entities to publicly disclose even summary information on incidents while they are still being investigated and remediated would particularly be harmful to the markets and industry.

C. Timing of public disclosures matters greatly

To the extent the Commission insists on requiring public disclosures of significant cybersecurity incidents, the Commission should consider adopting a more flexible approach to such disclosure. The Rule 10 Proposal states "the covered entity would need to file a Part I and an updated Part II of proposed Form SCIR with the Commission relatively

---

[31] Proposed Rule 10 Release at page 73.

[32] DTCC notes that it was in October 2017 that the SEC disclosed that an EDGAR test filing accessed by third parties as a result of the 2016 intrusion of the SEC's EDGAR system contained certain sensitive personal identifiable information of individuals. See https://www.sec.gov/news/press-release/2017-186.

contemporaneously."[33] Covered entities should only be required to publicly disclose information after the incident has been fully investigated and remediated, when the covered entity would have a more accurate understanding of the significance and impact of an incident and would have remediated to prevent further damage. Requiring an entity to publicly disclose a significant incident before it has been fully investigated and remediated can alert threat actors that a firm is in distress and is possibly vulnerable, increasing the immediate likelihood of further attacks; undermine confidence in the financial system and its institutions; and create unwarranted litigation and enforcement risks.

Importantly, Reg SCI grants the SCI entity the ability to delay disclosing information on a "systems intrusion" – which seems consistent with Proposed Rule 10's concepts of cybersecurity incidents – if it determines that such disclosure "would likely compromise the security of the SCI entity's SCI systems or indirect SCI systems or an investigation of the systems intrusion."[34] This critical flexibility does not appear to be provided in Proposed Rule 10 and should be included in the final requirement should the SEC adopt a public disclosure requirement for significant cybersecurity incidents, and would be consistent with Recommendation 4 of the FSB Report.[35]

4. *Proposed definitions of "cybersecurity incident" and "significant cybersecurity incident" should be narrowed to those that cause actual or demonstrable harm to the market entity's critical operations or to the stability of the U.S. securities markets.*

Cybersecurity Incident. DTCC recommends removing "jeopardizes" from cybersecurity incident and limit the scope to those events that cause actual harm (which would carry through to the definition of significant cybersecurity incidents, limiting reportable incidents to those that cause actual harm). Removing "jeopardizes" would be in line with the latest FSB Cyber Lexicon definition of cyber incident with Recommendations 5 and 8 from the FSB Report.[36] Limiting the incident definition to those that impose an actual harm would also limit uncertainty (and associated time and resources) for entities that must determine whether an incident truly should be reported given an actual impact versus whether it is just an event that could provide interesting information to recipients but no required action.

Significant Cybersecurity Incident. The threshold of a "significant cybersecurity incident" should be raised as it currently would cover incidents that could cause significant harm to one individual or counterparty. Specifically, in addition to the first prong of its proposed definition, which requires disclosure of those cybersecurity incidents that significantly disrupt or degrade the ability of the market entity to maintain its critical operations, the second proposed prong of the definition would require the disclosure of 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 two types of impact: (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."

We note that the first type of impact, substantial harm to the market entity, seems to be duplicative of the first prong of the definition; we would consider substantial harm to a market entity to mean a disruption or degradation of its ability to maintain its critical operations. Further, the second type of impact, substantial harm to a customer, counterparty, member, registrant, or user of the market entity, would capture incidents that may only impact a single market entity, single customer, or single person that interacts with the market entity that was impacted, which may not amount to a significant or demonstrable harm to the market entity's operations or to the stability of the U.S. securities markets, which is the stated purpose of the Proposal. For example, in the event of an email outage, many firms could use

---

[33] Proposed Rule 10 Release at page 167.
[34] See Reg SCI, § 242.1002(c)(2).
[35] FSB Recommendation 4: Financial authorities should implement incremental reporting requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of bringing the incident under control.
[36] FSB Recommendation 5: Select appropriate incident reporting triggers. Financial authorities should explore the benefits and implications of a range of reporting trigger options as part of the design of their cyber incident reporting regime.
FSB Recommendation 8: Financial authorities that use materiality thresholds should consider finetuning threshold language, or explore other suitable approaches, to encourage prompt reporting by FIs for material incidents

text messaging, voice calls, or other communications channels to maintain internal communications, and in those cases where this disruption does not inhibit the provision of market services, that incident, by itself, should not rise to the level of a reportable incident under Proposed Rule 10. Only those significant incidents that would prohibit or significantly delay the entity's services would meet the substantial "harm" threshold. For clarity and to be consistent with the objectives of Proposed Rule 10, DTCC requests that the Commission consider tying the second prong more clearly to those cybersecurity incidents that would cause significant harm to the market entity's critical operations or pose a threat to the stability of the U.S. securities markets.

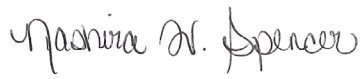
5. *DTCC believes it is imperative that the Commission establish an appropriate implementation timeline that would allow covered entities, and in particular, those that would be subject to multiple overlapping rulemakings, ample time to review the new requirements, determine the changes that would be required, and implement such changes.*

The Commission did not appear to propose a compliance date for Proposed Rule 10 (though it sought comment on the appropriate compliance date specifically for the proposed disclosure requirement under question 71). If the Commission adopts the Proposal in a manner that continues to overlap or be duplicative of other requirements for certain entities, that will create significant implementation challenges for the relevant entities. It will take covered entities substantial time to review multiple new rules against existing systems, processes, policies, procedures, and controls (collectively, cybersecurity measures) to determine what changes to (or new) cybersecurity measures would be necessary, execute on such changes, and conduct testing to ensure compliance – consistent with the change management and due diligence processes DTCC described above in Section 2. The Commission should allow for sufficient time for covered entities to implement the requirements, especially if multiple rules are finalized concurrently and are not sufficiently harmonized or aligned. Based on our preliminary analysis, DTCC believes covered entities will need at least 18 months to implement any final rule.

Conclusion

DTCC appreciates the opportunity to provide comments on the Proposal and your consideration of the views expressed in this letter. DTCC welcomes the opportunity for further discussions and engagement on the topics we raised. If possible, DTCC would also appreciate opportunities to share potential additional comments, given the tight timing for reviewing multiple concurrent rulemakings. If you have any questions or need further information, please contact me at nspencer@dtcc.com.

Sincerely,



Nashira Spencer
Managing Director and Chief Security Officer
The Depository Trust & Clearing Corporation