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 9, 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. S7-07-23; Release No. 34-97143; Regulation Systems Compliance and Integrity

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

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 amendments to Regulation Systems Compliance and Integrity ("Proposed Reg SCI" 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 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.

[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 ("Federal Reserve Board") 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. DTCC's registered and exempt clearing agencies have been subject to the Commission's Regulation SCI since its adoption in 2014. If the proposed expanded definition of "SCI entity" is adopted as proposed, DDR would become subject to Regulation SCI.

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. DTCC recognizes the need for risk-management regulations, particularly for entities that directly support the core functions of the U.S. securities market, to evolve as new and increasing sources of risk emerge and appreciates the Commission's continued efforts to strengthen the operational resilience of these entities in light of the changing environment. Although we recognize that updates and 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, Reg SCI (currently and as proposed to be amended)[3] and the Commission's Proposed Cybersecurity Risk Management Rule ("Proposed Rule 10") 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.[4] Additionally, DTCC's SBSDR subsidiary, DDR, is currently subject to similar operational risk management requirements under the SEC's Rule 13n-6 and under the SDR System Safeguards rule established by the Commodity Futures Trading Commission ("CFTC").[5] 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.

As discussed in detail below, we believe there are a few aspects of Proposed Reg SCI 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. In a few instances, we note unique considerations for DDR, should it be subject to Reg SCI.

Discussion of specific comments

1. *After comparing relevant proposed and current rules, DTCC believes Reg SCI already achieves the same cyber resilience outcomes under Proposed Rule 10 for the entities that are or will be subject to Reg SCI, and that existing requirements that SBSDRs are subject to already achieve the same broader operational resilience outcomes under Reg SCI. The Commission should remove redundant requirements for its entities or provide clarity on where it believes "gaps" exist and explain more clearly, using practical examples as opposed to high-level and conclusory statements, how affected entities should navigate the varying*

[3] 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.
[4] On June 5, 2023, DTCC submitted a companion comment letter, which primarily focuses on Proposed Rule 10, but also makes relevant references to Proposed Reg SCI, available at https://www.sec.gov/comments/s7-06-23/s70623-199519-399522.pdf. 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.
[5] *See* 17 CFR 240.13n-6 and 17 CFR 49.24, respectively.

terminology and processes of overlapping rules in a manner that avoids unnecessary regulatory certainty and associated burden and costs (generally response to questions 87, 88, and 89 of the Proposal).

DTCC appreciates the SEC's acknowledgement that there is duplication or overlap between Proposed Reg SCI and other proposals or existing regulations and that it provided preliminary and high-level statements regarding where the duplication or overlap exist. However, the Proposal did not appear to specify whether and where the SEC has determined the overlap (including varying terminology) to be consistent or provide a clear roadmap for potentially affected entities to navigate the varying terminology and processes of these overlapping proposed and existing requirements. Based on the questions for comment, it seems that the Commission anticipates relying on public commenters to help identify such consistency or inconsistency issues.[6] DTCC endeavors to support this effort by providing feedback in the sections below. However, we recognize that much of our response relies heavily on our analysis and interpretation of the high-level statements in the Proposal.

A. Reg SCI already achieves the cyber resilience outcomes intended to be achieve by Proposed Rule 10

Based on review of the two proposals, DTCC believes Reg SCI already achieves the cyber resilience outcomes for SCI entities that Proposed Rule 10 intends to achieve for its covered entities, albeit from a slightly different perspective. Reg SCI is broader in scope and 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 Proposed Rule 10 "would relate to certain of the requirements of Regulation SCI (currently and as it would be amended). The Commission believes this result would be appropriate because the policies and procedures requirements of Regulation SCI (currently and as it would be amended) differ in scope and purpose from [Proposed Rule 10]…, and because the policies and procedures required under Regulation SCI that relate to cybersecurity (currently and as it would be amended) are generally consistent with the proposed requirements of [Proposed Rule 10]" (emphasis added). Further, the Commission states that Reg SCI requirements "do not and would not apply to other systems maintained by an SCI entity."[7] Although the Commission offers a generic explanation regarding the difference in "scope" of information systems that are covered under either Proposal, it does not appear to provide an explanation regarding the differences in "purpose." However, from DTCC's review of the two proposals, it seems Rule 10 intends to strengthen the cyber resilience of proposed covered entities, though ultimately for purposes of ensuring a safe and efficient securities market, which DTCC understands to be consistent with the purpose of Reg SCI. Given that Reg SCI is broader in scope from a risk perspective, 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 and certainly supports and has comprehensive cybersecurity risk management that takes a proportionate risk-based approach with respect to information systems that are not SCI systems or indirect SCI systems. For specific reasons detailed in DTCC's companion comment letter that primarily focuses on Proposed Rule 10 ("DTCC Rule 10 Letter"), even if such a gaps exists, however, DTCC does not

---

[6] In addition to questions 87-89 of the Proposal, on page 160 of the Proposed Reg SCI Release, "the Commission encourages commenters: (1) to identify any areas where they believe the relation between requirements of the existing or proposed requirements of Regulation SCI and the proposed requirements of the Exchange Act Cybersecurity Proposal … would be particularly costly or create practical implementation difficulties; (2) to provide details on why these instances would be particularly costly or create practical implementation difficulties; and (3) to make recommendations on how to minimize these potential impacts, while also achieving the goal of this proposal to address, among other things, the cybersecurity risks faced by SCI entities."

[7] See Proposed Reg SCI Release, page 162. The Commission also makes similar statements in Proposed Rule 10. 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" (Proposed Rule 10 Release, pages 212-213).

believe Proposed Rule 10 would strengthen an SCI entity's cyber resilience beyond what is required under Reg SCI.[8]

To this end, DTCC is not recommending scope changes to Proposed Reg SCI, given that DTCC has had almost a decade of experience complying with the existing rule and believe that Reg SCI establishes more appropriate requirements than the Rule 10 Proposal with respect to the purposes of each rulemaking (even for a potential new SCI entity like DDR). Instead, DTCC recommends here and in the DTCC Rule 10 Letter that the SEC remove unnecessary redundancy either by scoping SCI entities out from Rule 10 or 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 created by Proposed Rule 10 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. To the extent the "gap" that Proposed Rule 10 aims to fill for Reg SCI is limited to the cybersecurity risk management of information systems that are neither SCI systems nor indirect SCI systems, DTCC believes the Commission's 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 covered entities flexibility to adopt a risk-based approach to managing the cybersecurity risks from these non-critical systems.[9]

B. Redundancy between Proposed Reg SCI and existing requirements applicable to SBSDRs (generally responsive to questions 97 and 100).

DDR has established systems, policies, procedures, and processes (collectively, "operational risk measures") to comply with existing relevant requirements established by its U.S. and non-U.S. regulators.[10] In the Proposal, the Commission acknowledged that SBSDRs like DDR are already subject to other similar requirements, and specifically highlighted SEC Rule 13n-6 and the CFTC's SDR System Safeguards rule as the "regulatory baseline" – the current market practices as well as applicable regulations in the absence of these proposed rules – for its analysis of benefits and costs of the proposal to expand Regulation SCI to SBSDRs. The Commission proposes to retain Rule 13n-6 even if the expanded definition of "SCI entity" is finalized to include SBSDRs. The Commission explains its rationale "that Rule 13n-6 should be preserved, with the requirements of [Proposed Reg SCI], if adopted, working to complement Rule 13n-6" and that compliance with the "requirements in the SBSDR rules, including Rule 13n-6, is, thus, an important building block for better ensuring the integrity of an SBSDR's data quality upon which the Commission and the securities markets rely."[11] However, following DTCC's review of Rule 13n-6, it is nearly identical to Reg SCI's § 242.1001(a)(1), both in language and expected regulatory outcome.[12] Should the expanded definition of "SCI entity" be finalized to include SBSDRs, DTCC recommends

---

[8] As explained in more detail in Section 1 of the DTCC Rule 10 Letter, with the inclusion of requirements for SCI entities to identify "indirect SCI systems" along with "SCI systems," an SCI entity is already effectively required to manage its cybersecurity risks with respect to all its information systems, by ensuring that any information systems that would not be subject to the requirements of Reg SCI must be logically or physically separate from SCI systems (i.e., systems that support core securities market functions); issues arising in these essentially non-critical systems, by definition, should not cause harm to SCI systems. From the perspective of Proposed Rule 10's requirement to publicly disclose summary descriptions of "significant cybersecurity incidents," although Reg SCI's responsible disclosure requirement to members/participants is not fully public, its requirements fulfill Proposed Rule 10's objectives of enabling relevant parties "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" without incurring material risks of public disclosure (Proposed Rule 10 Release, page 161).

[9] 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 for SCI entities, which include covered clearing agencies.

[10] In addition to the SEC and CFTC, DDR is subject to regulation by 13 Canadian market regulators led by the Ontario Securities Commission.

[11] See Proposed Reg SCI Release, page 37.

[12] Rule 13n-6 states that "[e]very security-based swap data repository, with respect to those systems that support or are integrally related to the performance of its activities, shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its systems provide adequate levels of capacity, integrity, resiliency, availability, and security." Reg SCI § 242.1001(a)(1) states that "[e]ach SCI

that the SEC make a conforming change to Rule 13n-6 by removing the provision or at least by amending it to explicitly state that, for any SBSDR that is also an SCI entity, compliance with Reg SCI would constitute compliance with Rule 13n-6. Rule 13n-6's slightly inconsistent language would otherwise create regulatory uncertainty between it and Reg SCI for SBSDRs.

The Commission is also seeking feedback (under questions 97 and 100) on the activities that new SCI entities currently perform that are already consistent with the requirements under Proposed SCI and commenters' views on prospective costs of applying Regulation SCI to SBSDRs. Unfortunately, DTCC finds it difficult to respond to these questions, as it would depend on the Commission's views regarding Proposed Reg SCI's consistency with the existing CFTC System Safeguards rule, which is a comprehensive set of requirements for the management of operational risk (which includes cybersecurity risk) for SDRs. Whereas DTCC preliminarily believes that the two sets of requirements seem generally consistent (and therefore DDR's existing operational risk measures would already be generally consistent with Proposed Reg SCI), DTCC is concerned that the Commission may consider the differences in terminology and structure between Proposed Reg SCI and the CFTC rule to be substantial enough to yield materially different outcomes. DTCC notes that the Commission indicated that it believes the requirements to be consistent, because it anticipates compliance costs for some new SCI entities could be lower, given that they are already subject to existing regulatory requirements that are similar to the Reg SCI provisions.[13] It also did not appear to identify as a potential cost to SBSDRs (or other new SCI entities), any challenges associated with new SCI entities having to reconcile between overlapping or inconsistent requirements. Additionally, DTCC believes that past experience also serves as indication of the SEC's intention to ensure consistency between the two sets of rules; DTCC notes that the SEC and CFTC's past coordination and harmonization efforts with respect to entities that are jointly registered with both agencies (including DDR) were well-received and instrumental to creating a cost-efficient data reporting regime for the U.S. derivatives markets. As we discuss below, we believe that formal coordination between the two agencies is also advisable in this instance.

DTCC seeks the Commission's clarification that Reg SCI is consistent with the CFTC System Safeguards rule, and to the extent it does, to clarify that the CFTC's rules would meet the definition of a "current SCI industry standard" under the safe harbor provision in § 242.1001(a)(4), which considers such standards to be "information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body" that includes "a U.S. governmental entity or agency." To the extent the Commission believes there to be inconsistencies, DTCC respectfully requests that the Commission clarify why it would not consider the CFTC's System Safeguards standards to meet the definition of a current SCI industry standard, work with SBSDRs to identify areas of inconsistency, explain why such inconsistency is important to retain, and address the resulting overlapping requirements in any cost-benefit analysis of a final rule. Importantly, harmonization between the SEC and CFTC for jointly registered entities would affect not only the burden and costs associated with DDRs' implementation of Reg SCI, if it is scoped in under the final rule, but also future rulemakings by the two agencies. CFTC Chairman Rostin Behnam recently discussed a regulatory agenda, which includes thematically enhancing risk management and resilience across intermediaries, exchanges, and derivatives clearing organizations and fostering sound and responsive practices regarding cybersecurity and the use of third-party vendors across all registrants.[14] The scope of this agenda would seem to overlap with the requirements of the SEC's Proposed Reg SCI as well as Proposed Rule 10. DTCC believes continued efforts between the SEC and CFTC to harmonize and coordinate on their respective related rulemakings for jointly registered entities is essential to avoiding imposing unnecessary burden and costs on such entities.

---

entity shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, indirect SCI systems, have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets."

[13] See Proposed Reg SCI Release, pages 324 and 358 as examples.

[14] The CFTC Chairman's remarks are available at https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam32.

2. DTCC strongly encourages the Commission to adopt a more flexible, risk-based approach to its requirements around use of third-party providers

The Commission has proposed a set of amendments to Regulation SCI that expressly address third-party providers in specific areas. Although the proposed requirements would be applicable to third-party providers generally, the discussion in the Proposed Reg SCI Release focuses primarily on cloud service providers ("CSPs"). DTCC offers specific feedback and recommendations below with respect to certain proposed third-party provider requirements from the perspectives of general implications and implications for new technologies such as cloud services.

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

Under proposed § 242.1001(a)(2)(ix), the Commission would require each SCI entity to have "a program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for [its SCI systems and, for purposes of security standards, indirect SCI systems], including: initial and periodic review of contracts with such third-party providers for consistency with the SCI entity's obligations under Regulation SCI…." The inclusion and placement of the term "indirectly" seems to imply that the Commission would consider service providers of third parties (i.e., "4th party" or "nth party") to be a type of "third-party provider" wherever the term is used in Proposed Reg SCI. This could mean, among other requirements, that SCI entities will need to "manage and oversee" nth parties along with its direct service providers. Absent a contractual relationship with an nth party, it would be challenging for SCI entities to formally manage or oversee the security practices of the nth party, as it would be nearly impossible to directly effect a change in practice or behavior of the nth party. However, SCI entities could manage their *risks* to these providers, generally through a combination of conducting due diligence of its third-party's supplier risk program or other contractual requirements (e.g., SLAs, incident reporting). The inclusion of such clauses is typically determined by the SCI entity based on service type and inherent risk that the third-party provider presents to the SCI entity. Additionally, SCI entities could also choose to require a third-party provider to include in any agreements the third party has with any additional party to include terms incorporating the agreement between the original entity and its third-party provider. DTCC, however, would not consider these measures to be means of "managing or overseeing" any indirect relationships, but rather the risks arising from such relationships.

DTCC observes that the Commission may not have intended to include nth parties in scope of "third party providers" given that proposed § 242.1001(a)(2)(ix) includes a provision for SCI entities to conduct "initial and periodic review of contracts with such third-party providers…" suggesting that the Commission would expect an SCI entity's "third-party providers" to have a contractual relationship with the SCI entity. Further, the Commission also explains that [the service provider oversight requirements of Proposed Rule 10] with respect to its SCI systems and indirect SCI systems should generally satisfy the proposed requirements of Regulation SCI that the SCI entity's policies and procedures include a program to manage and oversee third-party providers that provide functionality, support, or service, directly or indirectly, for SCI systems and indirect SCI systems. Proposed Rule 10's provisions around oversight of "service providers" seem limited to those relationships that are bound by "a written contract between the covered entity and the service provider."[15] As noted above, entities would have contractual relationships with direct third-party providers but not indirect providers.

Nevertheless, DTCC requests that the Commission clarify the use of "indirectly" in this proposed requirement and would propose the Commission remove this term if it did not intend to directly scope in the risk management of nth parties to the requirement. To the extent, however, the Proposal does mean to cover nth parties in some capacity, DTCC strongly recommends that the SEC provide clarification in the final rule that, rather than a requirement to manage and oversee nth parties directly, the SCI entity has the flexibility to employ a risk-based approach to identifying, assessing, and managing, as appropriate, risks arising from potential nth parties, including by considering the following revision to proposed § 242.1001(a)(2)(ix): "A program that adequately manages the risks of ~~to manage and oversee~~ third-party providers that provide…."

[15] See Proposed Rule 10, § 242.10(b)(1)(iii)(B).

B. Considerations related to third-party provider concentration

The Commission states that, as part of meeting the requirement under proposed § 242.1001(a)(2)(ix) for an SCI entity to conduct a risk-based assessment of each third-party provider's criticality to the SCI entity, "SCI entities would be required to consider third-party provider concentration, which would help ensure that they properly account and prepare contingencies or alternatives for an overreliance on a given third-party provider by the SCI entity or by its industry."[16] As implied by the Commission's statement, third-party concentration risks can be defined from an individual entity's perspective as a high volume of spend with one third party or using one for multiple critical services. Concentration risks may also occur when an industry relies too heavily on one supplier to perform critical services for their operations.[17]

From the individual entity perspective, an SCI entity would generally take into consideration the potential impact of its use of a third party across multiple services and review concentration risks as part of ongoing monitoring of service providers. SCI entities, however, also need to take a balanced approach and weigh any risk of service provider concentration against any gains in resiliency, efficiency, or effectiveness of using a third-party to deliver services to its members or clients. To this end, requirements around third-party risk management should enable the SCI entity to take such a balanced, risk-based approach; a regulatory outcome in which SCI entities are obligated to choose a lesser provider (including by maintaining services in-house) only due to potential concentration risks would be less than ideal.

From the industry-wide concentration perspective, DTCC notes that it will take public/private collaboration to understand where these risks may exist, and therefore addressing such risks cannot be the sole responsibility of each SCI entity. Although an individual entity can contribute information to authorities on its own third-party use, they are not in a position to determine or manage industry-wide concentration. Such an entity does not have visibility into whether another financial (or other type of) institution is using a particular third party nor would it know the capacity or purpose of any other entity's use of a third party. Thus, the public sector is better positioned to collect such information from the relevant entities and third-party providers to identify third party usage and general concentration. (We note that, even so, the more-challenging questions lie in how to determine appropriate thresholds for what is considered an unfavorable level of concentration and develop effective strategies for addressing such concentration risk.) We applaud efforts by the U.S. Treasury to identify and understand potential concentration risks related to the use of CSPs throughout the financial services sector through their white paper, *The Financial Services Sector's Adoption of Cloud Services* ("Treasury Cloud Paper").[18] With regards to how the Commission should proceed with its own current proposals around SCI entities managing concentration risk, before moving to any final requirements we recommend collaboration with U.S. Treasury efforts, through the Financial and Banking Information Infrastructure Committee ("FBIIC") or other means, to further understand potential CSP concentration risk issues and partner with the private sector to identify ways to manage concentration risk, where necessary. Given the inability of the financial services sector to create additional third-party competitors, DTCC emphasizes that the goal of identifying concentration risks is to manage risks resulting from concentration of providers and not necessarily the concentration of providers itself (which, again, we believe is a question that only the public sector may consider).

C. Business continuity/disaster recovery ("BC/DR") planning to address the unavailability of certain third-party providers

The Proposal includes an express requirement under proposed § 242.1001(a)(2)(v) for SCI entities to have BC/DR plans that "are reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity without which there would be a material impact on any of its critical SCI systems." The Commission explicitly mentions considering not only typical BC/DR scenarios such as a momentary outage that causes a feed to be interrupted or an extended cybersecurity event on the third-

[16] Proposed Reg SCI Release, page 117.
[17] Concentration can also refer to geographic concentration of third parties, where multiple third parties are located in the same geographic region. Concentration risk can also be defined as the probability of loss arising from a lack of diversification.
[18] U.S. Treasury, The Financial Services Sector's Adoption of Cloud Services - https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

party provider, but also instances that seem more consistent with general business risk scenarios such as if a third-party provider goes into bankruptcy or even "breaches its contract and decides to suddenly, unilaterally, and/or permanently cease to provide the SCI entity's critical SCI systems with functionality, support, or service." In the latter case, the SEC recognizes that while "it may appear to be improbable, given the criticality of the critical SCI systems to the SCI entity and U.S. securities markets, SCI entities should have plans in place to account for such scenarios, however remote." Further, in providing examples of ways to address such scenarios, the SEC suggested that "an SCI entity could consider if use of a CSP for its critical SCI systems also warrants maintaining an "on-premises" backup data center or other contingency plan which could be employed in the event of the above scenarios noted above."[19]

In general, DTCC supports *considering* a full spectrum of extreme scenarios when planning for BC/DR, coupled with *appropriately planning* for them in a manner that is risk-based and in consideration of the tradeoffs between risks and benefits against all of the applicable risks (e.g., although certain risks may increase in using a third party to support an operation, it may be worthwhile to gain significantly more operational resilience) and will continue to do so under its current BC/DR planning. Further, with respect to the typical BC/DR scenarios identified by the Commission, DTCC believes that these are already covered under the current Reg SCI requirements, given that Reg SCI already applies to systems that are operated "on behalf of" the SCI entity (i.e., by third-party providers).[20] This is because an SCI entity is accountable to meeting the standards in Reg SCI (including the relevant recovery and resumption requirements) whether its SCI, indirect SCI, or critical SCI systems are operated by the SCI entity itself or by a third-party provider. In this regard, the Commission's proposed amendment to § 242.1001(a)(2)(v) would seem to only make more explicit the existing requirement to address disruptions that originate at a third-party provider.

With respect to the other types of scenarios that the Commission suggested would fall under BC/DR planning, DTCC respectfully offers a different perspective for the Commission's consideration. DTCC believes that a third-party provider's bankruptcy or sudden decision to breach its contract would fall outside the typical scope of BC/DR plans. In our experience, this is a type of scenario that firms would typically manage through contracts and relationships, such as under the Commission's proposed general requirement to manage and oversee third-party provider risks under § 242.1001(a)(2)(ix), rather than through disaster recovery processes. DTCC appreciates and shares the Commission's concerns over an SCI entity's ability to maintain or achieve timely recovery of operations when relying on third-party providers. However, the SEC's statements above can be construed to mean that its preferred way for SCI entities to solve for this remote risk of using third parties for purposes of achieving the recovery time objectives under Reg SCI is through the use of multiple and redundant third-party relationships. We believe our perspective is supported by the Proposed Reg SCI Release's discussion of how to approach third-party BC/DR arrangements with CSPs, where the Commission appears to be stating guidance that if SCI entities use CSPs, the SCI entities should maintain multiple CSP relationships or an on-premise backup as the appropriate BC/DR arrangements. DTCC notes, however, that a requirement to use either a different CSP or an on-premises data center as an additional backup to a (primary) CSP's own resiliency infrastructure constitutes substantially raising the longstanding domestic and international standards for clearing agencies to have a secondary site for purposes of BC/DR recovery and resumption (i.e., backup capabilities that are geographically diverse under current Reg SCI).[21] To require additional forms of backup infrastructure would be

---

[19] Proposed Reg SCI Release, page 119.

[20] Under Reg SCI: "*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"; "*Indirect SCI systems* means any systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems"; and "*Critical SCI systems* means any SCI systems of, or operated by or on behalf of, an SCI entity that [directly support certain core market functions]."

[21] The 2003 *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, which was issued jointly by the SEC, the Federal Reserve Board, and the Office of the Comptroller of the Currency, established the expectation for core clearing and settlement organizations to have "back-up facilities a significant distance away from their primary sites" in order to "avoid being subject to the same set of risks as the primary location" (available at https://www.sec.gov/news/studies/34-47638.htm). In 2012, the CPMI-IOSCO published the *Principles for Financial Market Infrastructures* ("PFMI"), which also contained a similar and clearer expectation for FMIs under Principle 17 to incorporate in BC/DR plans "the use of a secondary site" with a distinct risk profile from the primary site, to achieve timely recover and resumption of operations should there be a disruption at the primary site (available at https://www.bis.org/cpmi/publ/d101a.pdf). The PFMI further notes that FMIs can *consider* the need and possibilities for a third site.

establishing a requirement similar to having backup(s) to the backup, which is inconsistent with longstanding standards.[22] However, the intent of the Proposal is unclear in this regard, and we believe the SEC should clarify whether or not it is proposing to impose such a new standard.

Moreover, DTCC notes that the Commission's proposed amendment is not limited to CSPs and would cover longstanding third-party provider arrangements. For example, as indicated above, even on-premises data centers would have manufacturers of the hardware infrastructure and software used to operate them that can theoretically also decide to breach contract and exit the business suddenly or cease providing support. Typical third-party risk mitigation practices (including the planning of exit strategies) include establishing contractual obligations for third parties to provide, for example, one-year notice to its client if it wishes to wind down its business or service to the client. If the Commission does not consider such longstanding practices to be sufficient, SCI entities would necessarily have to reconsider all of its third-party relationships and be concerned that, in order to comply with Proposed Reg SCI, it would need to bring all operations in-house, even if there are third-party providers with better expertise in a particular field. Given that the examples provided in the Proposal focuses on CSPs, however, it seems that CSPs constitute the underlying concern that the SEC is addressing with proposed amendments to § 242.1001(a)(2)(v). In this regard, DTCC does not believe the use of CSPs would present risks beyond the types of risks that an SCI entity would need to manage with respect to other types of technology or infrastructure third-party providers such that it would warrant a different and more burdensome (and, as described further below, operationally complex) BC/DR backup arrangement requirement.

To sum up our comments on these particular aspects of proposed amendments in BC/DR planning and accompanying discussion, in any final adoption of the relevant requirements, DTCC recommends that the Commission (1) confirm that the proposed amendments under § 242.1001(a)(2)(v) to address the unavailability of certain third-party providers is limited to typical BC/DR scenarios and that the suggested general business risk scenarios are more appropriately considered and managed as part of the program to manage and oversee third-party provider risks under § 242.1001(a)(2)(v) (i.e., through the use of appropriate contract provisions), in order to avoid upending longstanding third-party risk management practices;[23] and (2) clarify, in particular, whether or not it intends to establish BC/DR backup arrangement requirements that are inconsistent with longstanding domestic and international standards, and if so, the attendant costs and burdens of such a standard.

D. The use of multiple CSPs or an on-premises backup to a CSP arrangement is more appropriate for longer-term exit strategies than for BC/DR processes

The challenge with these approaches for BC/DR planning is that, while conceptually sound, each third-party provider has proprietary implementations making it highly operationally complicated to design a system that would enable immediately switching third-party providers (thereby increasing operational risks) and costly to SCI entities (thereby lowering efficiency and effectiveness), as the Commission has generally acknowledged.[24] Specifically, these potential approaches have several drawbacks, which render them impractical to addressing BC/DR scenarios when applied to complex businesses and business solutions, but more appropriate in planned exit strategies with longer transfer timeframes.

First, a multi-vendor approach is defined as a financial institution that disperses its exposure to a single cloud service provider by using multiple CSP vendors. Although conceptually this appears to be an adequate solution to manage the risks associated with using one cloud service provider, there are challenges associated with this solution. Infrastructure as a Service (IaaS) offerings differ significantly between CSPs, which creates additional

---

[22] An SCI entity would, however, take steps to gain comfort that a CSP's offered backup infrastructure can meet the longstanding secondary site expectation before using its services (which is not unlike considerations for traditional arrangements, for which primary and backup infrastructures are provided by the same third-party provider).

[23] Additionally, DTCC would offer that should a critical third-party provider suddenly and unilaterally decide to breach an existing contract with an SCI entity, perhaps a more efficient and effective approach could be for a regulatory or government agency to intervene, in light of financial stability concerns, to help persuade such a critical third-party provider to reconsider what would be a market destabilizing decision.

[24] See Proposed Reg SCI Release, page 372. Further, under the SEC's covered clearing agency standards 17 CFR 240.17Ad-22(e)(17) and (e)(21), DTC, NSCC, and FICC must manage their operational risks and be efficient and effective in meeting the requirements of their participants and the markets they serve.

complexity when architecting business applications across two or more CSPs. Doing so would require complex application designs to ensure that both the information and application capabilities are the same across the two environments. Second, CSPs' intellectual property are based on the differences in service offerings, rendering the ability to close these gaps improbable. On-premise cloud solutions also lack the proprietary features employed by CSPs (e.g., AWS, Azure). Therefore, migrating business applications from these CSPs to on-premise solutions could require numerous months and at an enormous cost to rearchitect applications to operate in a new on-premise environment. Finally, there is a general shortage of staff with expertise in cloud services, and general IT and cyber skills may not translate fully to the cloud environment without additional training. Further, the skills required to deploy and secure applications in one CSP do not necessarily translate to the other CSPs, given the lack of interoperability between CSPs, which would require the limited staff with cloud expertise to develop additional skills for multi-cloud environments. This approach may exacerbate the shortage of the proprietary cloud security expertise currently in the marketplace.[25] Therefore, in addition to the unclear need for singling out CSPs (relative to other technology or infrastructure providers), the current approaches suggested by the Commission may negatively impact the planning and resiliency benefits necessary to improve efficiency in the financial markets.

Notwithstanding our concerns immediately above, DTCC recognizes that moving from an existing CSP relationship to another CSP or an on-premises replacement solution can be appropriate for third-party exit strategies with longer transfer timeframes. However, for the purposes of applying such a solution to the BC/DR context DTCC respectfully requests that the SEC reconsider this approach, given the complexities involved in performing within established BC/DR recovery and resumption timeframes. Consistent with our reasoning above, for example, in order to enable such transfer, an entity may be limited to only the standard services of either CSP (and not any proprietary enhanced resiliency features), thus lowering the operational resilience benefits of using CSPs and by extension, the resilience of the SCI entity. Further, as we have noted above, the types of risks presented by CSPs relative to other types of technology service providers (in this context, lack of interoperability among other technology service providers also exists as it does among CSPs) are not sufficiently different relative to other types of technology third-party service providers to warrant establishing a new third-party risk management framework. Therefore, we encourage the SEC to avoid applying a disparate standard to the use of CSPs versus other types of technology service providers, as it does not seem to be justified and would stifle technological innovation and the ability of SCI entities to achieve higher operational resiliency.

E. BC/DR industry and sector-wide testing for SBSDRs

Existing § 242.1004(c) requires that SCI entities coordinate the testing of its BC/DR plans on an industry- or sector-wide basis with other SCI entities. SIFMA facilitates an annual coordinated testing program for the securities industry (the exercise involves test transactions for commercial paper, equities, options, futures, fixed income, settlement, payments, Treasury auctions and market data). On the same day, the FIA leads the futures test component.[26]

As a general matter, DTCC believes it to be appropriate for SBSDRs to include relevant clients and third-party providers in its testing of BC/DR plans, as would be required under §§ 242.1004(a) and (b). However, we note that existing industry-wide testing focuses on recovery of market operations that would come before the activity would be reported to an SBSDR. Although industry-wide exercises would provide insights into those operational incidents that may have significant market impacts to the financial services sector, the time commitment to participate in these exercises is outsized by this benefit for purposes of SBSDRs. Currently, an SBSDR receives completed client transactions and responds with either an acknowledgement that the trade was

[25] These points are generally consistent with those expressed in the Treasury Cloud Paper, which explain that "While many financial institutions can increase resilience by operating in multiple regions of the same CSP, few experts believe that complex use cases can be developed to support seamless failover from one CSP environment to a different CSP environment. Reasons include the inherent differences among service offerings, the associated complexity of designing across multiple cloud environments, and the need to hire multiple staff familiar with various environments. While complete portability appears to be the idealized solution to solve dependencies, it is not currently, nor is it likely to become, technically practical for many complex services. One key impediment is a lack of interoperability in identity and access management services across the major cloud providers and third-party solutions. Even if it became more practical, instantaneous substitutability might come with challenges that may make it inadvisable for many financial institutions and use cases (e.g., due to greater risks and costs required to design and secure multiple environments)." See page 56 of Treasury Cloud Paper.

[26] https://www.sifma.org/resources/general/industry-wide-business-continuity-test/

received successfully, or a response that submission data needs to be corrected. These transactions are submitted unilaterally, and do not depend on a counterparty when submitted. DTCC believes that the only BC/DR testing that would be relevant to SBSDRs would be for clients, on an annual basis, to complete a connectivity test between each client and the SBSDR, and no industry-coordinated test would be needed or relevant. DTCC would therefore ask that the Commission allow SBSDRs to participate as observers to the existing industry-wide exercises as a means of complying with § 242.1004(c), or exempt entirely SBSDRs from coordinating industry- or sector-wide BC/DR testing.

3. *DTCC does not believe the expansion of the "systems intrusion" definition, particularly with respect to the inclusion of significant attempted unauthorized entry, is appropriate*

The Commission is proposing to expand the definition of "systems intrusion" to include two additional types of cybersecurity events, which would broaden the scope of immediately reportable SCI events. The first additional type of systems intrusion would include successful cybersecurity incidents that the Commission believes are not fully covered under the existing definition and the second additional type would capture unsuccessful, but significant, attempts to enter an SCI entity's SCI systems or indirect SCI systems. DTCC offers specific feedback and recommendations below with respect to these two requirements.

A. <u>Cybersecurity event that disrupts, or significantly degrades, the normal operations of an SCI system</u>

The Commission noted that there is a gap between the current definition of a "systems intrusion," which covers unauthorized entries "into" SCI systems and indirect SCI systems, and a "systems disruption," which covers an event "in" SCI systems that disrupts or significantly degrades the normal operations of an SCI system. Combined, these definitions would not technically cover a cybersecurity event that causes disruptions or significant degradation to SCI systems and indirect SCI systems, should the event have occurred outside of an SCI or indirect SCI system and did not result in an entry into or access to these systems. The Commission proposes to cover this gap by adding a second prong to the definition of systems intrusion, noting that the "[s]econd prong is intended to include cybersecurity events on the SCI entity's SCI systems or indirect SCI systems that cause disruption to such systems, regardless of whether the event resulted in an entry into or access to them."[27]

DTCC agrees that such types of incidents should be covered, but it believes there is a simpler and clearer way of addressing this technical gap in the definition of an SCI event. DTCC recommends that the Commission refrain from adding a second prong to the "systems intrusion" definition, which would blur the lines between it and a "systems disruption." We recommend instead that the Commission make a minor amendment to systems disruptions as follows: "*Systems disruption* means an event ~~in an SCI entity's SCI systems~~ that disrupts, or significantly degrades, the normal operation of an SCI system."

B. <u>Significant attempted unauthorized entry into SCI systems or indirect SCI systems.</u>

The Commission is proposing to add a third prong to the definition of a systems intrusion, which would include "any significant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria."[28] The Commission notes that, in proposing to expand the definition of a "systems intrusion" to significant attempted unauthorized entries that could ultimately be unsuccessful, its intention is to provide the Commission and its staff important information regarding threats that may be posed to other entities in the securities markets, including other SCI entities. It also notes that this would help provide the Commission and its staff more complete information to assess the security status of the SCI entity, and also assess the impact or potential impact that unauthorized activity could have on the security of the SCI entity's affected systems as well as other SCI entities and market participants.[29]

---

[27] Proposed Reg SCI Release, page 133.
[28] Proposed Reg SCI Release, page 134.
[29] Proposed Reg SCI Release, page 132.

We appreciate the Commission recognizing that it would be undesirable to require that all attempted entries be considered significant. However, the definition of systems intrusions, which trigger extensive notifications, reporting, and disclosure requirements, should be limited to events that cause actual harm, particularly due to the strong threat-intelligence sharing mechanisms that are already established throughout the financial services sector. For example, there are many threat-intelligence reports that currently could offer the insights that the Commission and its staff may be looking for (e.g., Crowdstrike and IC3), including threat sources, such as sophisticated threat actors or a targeted campaign. When responding to events and remediating incidents, financial institutions are less concerned with attribution than the attack (or other type of incident) itself and would focus on the rapid restoration of the information system. It could take significant time to attribute the threat to, for example, a nation-state actor, a threat actor supported by a nation-state, or a sophisticated group of hackers (e.g., Lazarus). Further, attribution is usually attained from external threat intelligence organizations or government intelligence partners. Lastly, for critical infrastructure operators, the Cybersecurity and Infrastructure Security Agency ("CISA") is looking to gather this information for the clearly stated purpose of national security and the protection of U.S. interests domestically and abroad, where the sharing of this information may allow for diplomatic solutions and other government actions. Therefore, we believe the reporting of this information is more aligned to such remits rather than specific regulatory agency remits. To this end, the third prong would lead to unnecessary and time-consuming reporting, particularly given the regulatory uncertainty this additional trigger would bring to SCI entities, who may be concerned about having a different perspective than the Commission regarding whether a particular attempted unauthorized entry meets the threshold of "significant."

For the reasons above, DTCC strongly recommends that the Commission refrain from adopting the proposed third prong to "systems intrusion" and requiring significant attempted unauthorized entries that are ultimately unsuccessful to the scope of SCI events that would trigger immediate notifications and 24-hour subsequent reporting and updates on material changes, which carry significant compliance burden for SCI entities. To the extent the Commission believes that existing resources and sources of information on threat intelligence are not sufficient to help the Commission achieve its goals of understanding the threat landscape for the securities market and would like to establish a separate intelligence sharing and collaboration arrangement with SCI entities, DTCC would recommend doing so by working with existing public/private arrangements, relevant government agencies, and the industry to establish one that would fill a current gap, offer information sharing benefits to stakeholders broadly, and fall outside of regulatory compliance and enforcement processes.

4. *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 new entrants to Regulation SCI or 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 Reg SCI. 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 implement changes to its policies and procedures to ensure compliance with multiple new rules. 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 Reg SCI; consult the relevant SEC supervisory and policy teams to understand Reg SCI, if it is adopted without the changes or additional clarity that DTCC seeks; determine the changes that are necessary to comply with Reg SCI; ensure that such changes would not put themselves in conflict with other U.S. – including a final Rule 10 – 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. 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.

A. Additional considerations for new SCI entities, such as DDR (responsive to question 100).

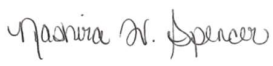
SEC should allow sufficient time for SCI entities (particularly new SCI entities) to implement the requirements, especially if these are all finalized at the same time (and are not sufficiently harmonized) as other related requirements. Additionally, DTCC is seeking clarification on proposed section 242.1003(b)(1), which would require an SCI review to be conducted "not less than once each calendar year for each calendar year during which [the SCI entity] was an SCI entity for any part of such calendar year." The SEC clarifies that "if an SCI entity is an SCI entity for any part of the calendar year, it must conduct the SCI review and submit the associated report of the SCI review to the SCI entity's senior management and board, as well as to the Commission. Thus, an SCI review would be required for a new SCI entity, even in its first year as an SCI entity and even if its starting date as an SCI entity were not until late in the year."[30]

DTCC notes that it may not be sufficient time to conduct an SCI review (either by including a new SCI entity into an ongoing SCI review process for other SCI entities in an organization or by starting an SCI review for a new SCI entity) if an entity becomes an SCI entity during the latter part of the calendar year. Given the SCI review lookback period of one year, there is an enormous amount of relevant policies and procedures for the objective personnel to review and test, which cannot be completed without having a full year to conduct such review. DTCC has an established ongoing annual SCI review period. If the SEC sets a compliance date closer to year end for new SCI entities, it would be difficult for DTCC to fold DDR into an SCI review process that has already been underway for its other SCI entities since the start of the review cycle. Even if DTCC starts an SCI review for DDR once the rule is final, challenges include (1) DDR would first need time to implement potential changes required by Proposed Reg SCI; (2) DDR would then be off-cycle from the rest of the DTCC entities in perpetuity; and (3) depending on the compliance date for completion of the SCI review for new entrants, there still may not be sufficient time to complete a full review for a new entrant during the initial year. DTCC recommends that the SEC establish a tiered compliance structure, where the SCI review for new SCI entities should be completed at least a full year after it has implemented policies and procedures to comply with the rest of the requirements in Reg SCI (and allowed to sync up with the SCI review cycle of any existing SCI entities in the organization).

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 raised in this letter. If possible, DTCC would also appreciate opportunities to share potentially 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

[30] Proposed Reg SCI Release, page148.