55 WATER STREET
NEW YORK, NY 10041-0099
TEL: 212-855-3240
lthompson@dtcc.com

July 8, 2013

VIA ELECTRONIC MAIL

Elizabeth M. Murphy, Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Re: Proposed Regulation Systems Compliance and Integrity
Securities and Exchange Commission ("SEC" or "Commission")
Release No. 34-6907; File Number S7-01-13 (March 7, 2013)

Dear Ms. Murphy:

The Depository Trust & Clearing Corporation ("DTCC") appreciates the opportunity to provide comments to the proposed Regulation Systems Compliance and Integrity ("Regulation SCI" or the "Regulation"), issued by the Commission in Release No. 34-6907; File No. S7-01-13, dated March 7, 2013 (the "Release"). DTCC, through its subsidiaries, is the largest post-trade market infrastructure for the global financial services industry, and supports its mission to protect its clients and the financial markets and systems as a whole through a sophisticated technology infrastructure. Given DTCC's critical role in the financial markets, and its reliance on its own technology infrastructure, DTCC is in full support of the goals of proposed Regulation SCI to ensure entities that are important to the functioning of the U.S. securities markets carefully design, develop, test, maintain, and surveil systems that are integral to their operations. DTCC acknowledges the Commission's effort and thought leadership in developing Regulation SCI. DTCC hopes that its comments contribute to a successful outcome of this important regulation and support the enhancement and protection of the securities markets.

Overview of DTCC

Technology plays a critical role in the operations of DTCC and its subsidiaries, and DTCC's systems, data centers, and businesses operate across multiple sites and environments. Several of DTCC's subsidiaries may be subject to the requirements of Regulation SCI.[1] DTCC has three wholly-owned subsidiaries which are registered clearing agencies under the Securities

[1] Omgeo LLC, a joint venture between DTCC and Thompson Reuters, provides its clients with post-trade pre-settlement trade management services. While Omgeo has received an exemption from full registration as a clearing agency under the Exchange Act by virtue of the fact that it operates a matching service, it will be subject to Regulation SCI and submits its comments in response to the Release separately.

Exchange Act of 1934, as amended (the "Exchange Act") – The Depository Trust Company ("DTC"), National Securities Clearing Corporation ("NSCC"), and Fixed Income Clearing Corporation ("FICC"). Further, the DTCC Data Repository (U.S.) LLC is a swap data repository registered with the Commodity Futures Trading Commission ("CFTC"), and plans to apply to become a security-based swap data repository ("SB SDR").

DTCC strives to streamline its core processes and information flows to create efficiencies, reduce risk, improve communications, and align its services with customer needs. To that end, DTCC regularly updates its technology systems to meet industry, regulatory, and compliance standards. Operationally, DTCC has implemented redundant systems at alternate locations that are frequently tested to ensure that its core systems are available in the event of an emergency. DTCC's technology infrastructure and IT platform enable it to effectively provide virtually uninterrupted support to the financial markets. This is achieved through a redundant and geographically dispersed operations infrastructure.

As the cross-market clearing agencies for the U.S. markets, DTC, NSCC, and FICC stand at the end of the securities processing chain and, therefore, are in a unique position to analyze opportunities to mitigate potential systemic risks in the markets, including those stemming from the rapid changes in market technology. DTCC staff participated in the Commission's October 2012 "Market Technology Roundtable", and DTCC plays an active role on major securities industry technology committees, sub-committees, and working groups addressing issues such as information security and industry-wide testing for business recovery. Furthermore, DTCC has been a voluntary participant in the Commission's current Automated Review Policy ("ARP") Inspection program.

I. General Comments

DTCC's comments below are preliminary in nature and DTCC may submit further views as it continues to consider the proposal. Given the complexity of the issues addressed in proposed Regulation SCI, and the diversity of entities that may be required to comply with the new Regulation, DTCC urges the Commission to consider convening an industry working group or a roundtable, similar to the "Market Technology Roundtable" conducted by the Commission in October 2012, to engage the industry in further discussion and development of the proposed requirements before they are finalized.

Scope and Applicability

In general, DTCC believes that the broad definitions of certain terms, which delineate the scope of proposed Regulation SCI, and the applicability of the proposed Regulation to a broad diversity of entities could trigger a number of notifications relating to events that could be considered, by certain SCI entities, as business as usual events without material impact on that entity's critical operations or core function, or on the market in which it operates. These less critical, and potentially very numerous, notifications will potentially mask the most critical events and divert valuable resources both at the SCI entity and at the Commission, reducing the efficiency of the Commission's oversight in this area. Particularly given the diversity of SCI entities to which the proposed Regulation applies, DTCC believes that the current structure of

these defined terms and the notice requirements that they trigger further create a risk of implementing unclear requirements, which would be difficult both to comply with and to enforce. This may create a risk that resources of both the SCI entities and the Commission would struggle to comply with requirements that focus on immaterial, ordinary course of business matters, not necessarily intended to be in the scope of the proposed Regulation, and may fail to give the proper attention to more critical systems maintenance, testing, and event resolution. This outcome would be counterproductive to the stated goals of the proposed Regulation.

As discussed in more detail below, DTCC recommends these defined terms be revised with more precision and defined with relevant materiality thresholds. A more risk-based approach to these concepts would permit the various SCI entities, each of which have very diverse infrastructures, platforms, and businesses of varying complexity, to apply the defined terms and associated requirements to their systems in a way that will adequately address the risks those entities face.

Timing and Complexity of Implementation

DTCC believes that, depending on the form in which the final rules are adopted, implementation of Regulation SCI by an SCI entity will take a substantial period of time. The time needed by SCI entities to meet the new requirements will vary by the type of SCI entity and the level of their current participation in the ARP Inspection Program. The steps necessary for all SCI entities to come into compliance with certain proposals within Regulation SCI, particularly with respect to proposed Rule 1000(b)(9) regarding industry-wide business continuity and disaster recovery plan testing, will necessarily be complex. Accordingly, DTCC believes the final Regulation SCI should provide that the time for an SCI entity to meet the new requirements have due regard for the complexity of required development and implementation.

II. Specific Comments on Proposed Regulation SCI

1. Scope of Regulation SCI: "SCI systems" and "SCI security systems"

Proposed Rule 1000(a) sets forth the fundamental definitions that delineate the scope of Regulation SCI, most importantly the definitions of "SCI systems" and "SCI security systems". In general, DTCC believes the definitions have been crafted too broadly, and should be refined to avoid an inconsistent application that could have the unintended consequence of pulling too much of the infrastructure of the U.S. securities markets into the scope of this Regulation. DTCC believes the Commission should consider permitting each SCI entity to perform an internal risk assessment of its systems, and from that assessment identify those systems it deems to fall within the definitions of *SCI systems* and *SCI security systems*. The Commission would have an opportunity review this assessment and the list of applicable systems, which may be delivered in connection with the other periodic reports contemplated by proposed Regulation SCI.

A. "SCI systems"

Proposed Rule 1000(a) defines "*SCI systems*" as "all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity, whether in production, development, or testing, that directly support trading, clearance and settlement, order routing, market data, regulation, or surveillance." In order to ensure that the scope of the definition is appropriate for each of the various SCI entities subject to Regulation SCI, DTCC recommends that this definition be revised to mean "all computer, network, electronic, technical, automated, or similar systems of an SCI entity that are in production and directly support *the SCI entity's core functions, such as* trading, clearance and settlement, order routing, market data, regulations, or surveillance, *which the SCI entity performs pursuant to applicable Commission regulations.*" DTCC believes this approach recognizes that each SCI entity has the best understanding of its own systems, and should, in consultation with its regulators, be responsible for identifying the systems that directly support its core regulatory functions.

DTCC believes that, for those SCI entities that have segregated their testing and production environments, it is important to exclude from this definition any systems that are in development and testing, and to ensure the defined term be limited to include only systems that are operating in production. Systems that are in development or in testing exist in controlled environments, insulated from production. By their very nature, test systems provide SCI entities with the opportunity to try proposed changes to SCI systems in an environment that does not impact the SCI system. Therefore, proposed functionality may not operate as anticipated and events may occur in these closed environments in the ordinary course of business. Such events are managed in a manner that does not have an impact on other systems within the SCI entity. DTCC asks the Commission to consider if these events, which do not impact the SCI entity's operations and have no risk of impacting its participants or the market in which it operates, are appropriate for inclusion within the scope of the requirements of Regulation SCI. Information regarding the status of systems that are in development or in testing would be captured in the notices regarding material systems changes under proposed Rule 1000(b)(6) and in the updates regarding those material systems changes in the periodic reports under proposed Rule 1000(b)(8). An alternative to capturing these events in the other requirements of Regulation SCI would be to require, within proposed Rule 1000(b)(1), that SCI entities establish, maintain, and enforce written policies and procedures that address implementation of systems changes such that any *testing* errors are corrected (and such corrections are retested) prior to implementation of those changes in production.

DTCC further believes, in response to the Commission's Request for Comment #22 on page 60 of the Release, that it is important to make clear that SCI entities should not be required to ensure compliance with Regulation SCI with respect to any systems *that are outside their control* and operated by third parties. DTCC believes it would be unduly burdensome and unrealistic for SCI entities to be accountable for compliance with respect to systems operated by other market participants that interface with the SCI systems, nor would SCI entities necessarily have access to information regarding such events sufficient to meet the reporting requirements in proposed Rules 1000(b)(4) and (5).

B. "SCI security systems"

Proposed Rule 1000(a) defines "*SCI security systems*" as "any system that shares a network with SCI systems that, if breached, would pose a security threat to SCI systems." As proposed, DTCC believes that the definition is too broad because systems in different, unrelated entities could very likely be considered interconnected through networks. DTCC believes that a risk-based definition would be more appropriate to meet the goals of proposed Regulation SCI, and network interconnectedness does not imply a source of risk from one system to another.

Preliminarily, DTCC believes the definition of "*SCI security systems*" would more properly be focused on the amount of isolation from one network to another. In particular, the definition should consider systems with physical interconnection where there is discreet access to, and control with respect to, an SCI system. It is critical in this context to focus on the trusted platforms that have access to an SCI system. "*SCI security systems*" could be identified by looking at the breadth of connectivity that creates a chain of trust between interconnected nodes, and where there may be access points to an SCI system.

As an example, a workstation whose access credentials allow it to gain access to an SCI system would be considered a critical SCI security system, but not necessarily the e-mail platform on that workstation. In the context of a system intrusion, if the e-mail platform on a workstation that does not have access to an SCI system is corrupted, the impact would be limited to that workstation alone, but if the corruption reached a workstation with access to an SCI system, the risk of harm could potentially be greater.

DTCC recognizes the obvious technical challenge in crafting a definition of SCI security systems, but believes that a more precise definition is crucial to the effectiveness of proposed Regulation SCI. DTCC believes it would be valuable for the Commission to work with representatives within the securities industry to collectively craft the most appropriate definition that will ensure that critical security systems are captured, while equally ensuring the proposed Regulation does not inadvertently capture systems that would not expose the SCI systems to a security threat.

2. Proposed Rule 1000(b)(4) and (5): Notification of SCI Events

A. Definitions of "SCI Events" and "dissemination SCI Events"

Proposed Rule 1000(a) defines an "*SCI event*", which would trigger various notice and other requirements within the proposed Regulation, by incorporating three separate defined events – a systems compliance issue, a systems disruption, and a systems intrusion. DTCC's comments on each of these three defined terms are set forth separately below.

In general, DTCC believes that the definitions should be risk-based in order to more appropriately align the proposed requirements with the overarching goals of Regulation SCI. Therefore, DTCC recommends that each of the defined terms comprising "*SCI events*" be limited by a materiality threshold and relate to only those events that cause a disruption to the SCI entity's ability to conduct its *core functions*, which it conducts pursuant to applicable

Commission regulations. Further, DTCC believes the Commission should consider whether it may be appropriate to differentiate between different types of SCI entities within the construction of these definitions. Certain events may have a more material impact on certain types of SCI entities than on others, and the current construction of the defined terms, without regard for the various types of SCI entities, could have the unintended consequence of triggering an inundation of notifications for minor events that may occur in the ordinary course of business for certain entities, diverting the Commission's resources and focus from critical and significant events.

- *"systems compliance issue"*

Proposed Rule 1000(a) defines a *"systems compliance issue"* as "an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the federal securities laws and rules and regulations thereunder or the entity's rules or governing documents, as applicable." DTCC recommends that this definition be limited to events that result in noncompliance with applicable the federal securities laws and rules and regulations thereunder or the SCI entity's rules or governing documents, as applicable, that has a materially negative impact on the SCI entity's ability to perform its core functions. DTCC further recommends that this definition be re-defined for each type of SCI entity, and be tied to the Commission regulations under which the SCI entity performs its core functions. For example, with respect to SCI entities that are clearing agencies registered under Section 17A of the Exchange Act, this definition would be interpreted as covering only those events that materially impact the SCI entity's ability to comply with the laws and rules under that Section.

- *"systems disruption"*

Proposed Rule 1000(a) defines a *"systems disruption"* as "an event in an SCI entity's SCI systems that results in: (1) a failure to maintain service level agreements or constraints; (2) a disruption of normal operations, including switchover to back-up equipment with near-term recovery of primary hardware unlikely; (3) a loss of use of any such system; (4) a loss of transaction or clearance and settlement data; (5) significant back-ups or delays in processing; (6) a significant diminution of ability to disseminate timely and accurate market data; or (7) a queuing of data between system components or queuing of messages to or from customers of such duration that normal service delivery is affected."

DTCC believes this definition should be limited by a materiality threshold, and should only cover *significant* events to the extent they have a materially adverse impact on the SCI entity's ability to perform its core functions and critical operations. To remain within the scope of proposed Regulation SCI's stated goals this event should be defined by the level of impact and potential risk posed to SCI systems and the wider securities market.

For example, with respect to subsection (1) in the proposed definition, very often service level agreements will experience minor, immaterial disruptions that are triggered outside of an SCI entity. Therefore, DTCC recommends that this subsection (1) of the definition be revised to capture only those most significant disruptions to a service level agreement that are caused by the SCI entity and that impede its ability to perform its core functions and critical operations; for

example, with respect to an SCI entity that performs clearing and settling functions, its ability to meet required clearing and settling deadlines. Additionally, DTCC recommends that subsection (4) in the proposed definition be revised to limit the loss of data that is considered a *systems disruption* to when a copy of the data is not *immediately* retrievable through back-up systems or record copies. Only when the data is not immediately recoverable through copies or other sources will there be a material impact on an SCI system, and should the event fall properly within the scope of Regulation SCI.

Further, DTCC believes that the Commission should not consider each instance in which a customer or systems user complains or inquires about a slowdown or disruption of operations as indicating that a systems disruption, as described in subsections (5) and (6), has taken place. DTCC believes that an SCI entity should have an opportunity to conduct an investigation into the cause of the inquiry or complaint before a determination is made that a reportable event has occurred. Finally, DTCC believes that subsection (7) in the proposed definition should be limited to instances when queuing impacts the ability of the SCI system to perform its intended function, and causes a material breach of a service level agreement. In certain circumstances queuing could be a part of the intended architecture of a system, and that system will operate normally and without impact to a service level agreement notwithstanding queuing.

Additionally, in response to the Commission's Request for Comment #32 on page 70 of the Release, DTCC agrees with the Commission that the *systems disruption* should exclude any regularly planned outages occurring during the normal course of business. DTCC does not believe planned events should be within the scope of Regulation SCI.

- "*systems intrusion*"

Proposed Rule 1000(a) defines "*systems intrusion*" as "any unauthorized entry into the SCI systems or SCI security systems of an SCI entity." Under this proposed definition, an intrusion could potentially include both the case where malware sent by the intruder was installed on an SCI security system and was thwarted in its attempt to communicate back to an attacker by controls, which would be an attempted intrusion, as well as when an attacker both successfully delivered a piece of malware to an SCI security system and that malware successfully established a communication back to the intruder. DTCC believes that the first example should only be considered *entry* into a system, but is an unsuccessful intrusion that should not require notification to the Commission, and that only the second example illustrates an actual systems intrusion that should trigger notification to the Commission.

Therefore, DTCC recommends that this definition be limited to any unauthorized entry into the SCI systems or SCI security systems of an SCI entity *where the SCI entity has reason to believe such entry may materially impact its ability to perform its core functions or critical operations.* Unauthorized entries into an SCI system or SCI security systems could very often have no material impact on those systems or on the SCI entity's core functions and critical operations, and would not be sufficiently material to warrant notice under proposed Regulation SCI. DTCC believes it would be more appropriate to limit the definition of this event to those instances when an unauthorized entry into an SCI system or SCI security system has an actual impact on an SCI entity's ability to perform its core functions and critical operations.

In response to the Commission's Request for Comment #41 on page 75 of the Release, DTCC supports the proposal that *systems intrusion* be limited to successful intrusions, and that the scope of this definition not be expanded to attempted intrusions, even in the case of repeated or sophisticated attempts. Unsuccessful intrusion attempts, particularly repeated unsuccessful attempts, demonstrate that the SCI system and the SCI security system are adequately protected, and do not warrant the notices proposed by Regulation SCI. DTCC notes, however, that there can be, in certain circumstances, great value in sharing information regarding attempted, unsuccessful intrusions with other SCI entities, on a secure and confidential basis. This informal information sharing takes place today among certain SCI entities, their regulators, and appropriate law enforcement agencies.

DTCC believes that a materiality threshold that limits the definition of each of these events to when there has been a clear and demonstrated material impact on an SCI entity's ability to perform its core functions and critical operations will ensure that only the most significant events are captured, and will support the stated goals of the Regulation. The reporting of all events regardless of materiality could potentially result in reporting of a large number of minor events that occur in the normal course of business and have no real impact on the critical operations of an SCI entity, or on its participants and the market in which it operates. As currently drafted, the broad scope of the defined terms could trigger a number of unnecessary notifications regarding routine and business-as-usual events, which creates a risk that the most critical events are not as readily apparent, and could tie up valuable resources both at the SCI entity and at the Commission.

With respect to certain events that do not meet the proposed materiality thresholds, DTCC notes that these events, rather than being subject to the notice requirements of proposed Rules 1000(b)(4) and (5), may instead be maintained within the SCI entity's records. The Commission could then have the opportunity to review incident logs and inquire further about these items on a periodic basis.

B. Proposed Rule 1000(b)(4): Notification of SCI Events to Commission / Proposed Rule 1000(b)(5) Notification of dissemination SCI Events to Members and Participants

Proposed Rule 1000(b)(4) would require an SCI entity to notify the Commission, either orally or in writing (e.g., by email), upon any responsible SCI personnel becoming aware of a systems disruption that the SCI entity reasonably estimates would have a material impact on its operations or on market participants, any systems compliance issue, or any systems intrusion ("immediate notification SCI event"), to notify the Commission of such SCI event. Proposed Rule 1000(b)(5) would require information relating to *dissemination SCI events* to be promptly disseminated to an SCI entity's members or participants upon a *responsible SCI personnel* becoming aware of those dissemination SCI events. Proposed Rule 1000(b)(5)(ii) permits a delay in dissemination of information to an SCI entity's members and participants if prompt notification would cause security concerns. DTCC provides its general comments to these proposed Rules below.

- *Timing of Notifications.*

SCI events can occur at any time, including after business hours, during the weekend, or over holidays. DTCC recommends that proposed Rule 1000(b)(4) be revised to provide that immediate notice to Commission staff through a phone call or an e-mail after normal business day hours be triggered only by the most critical events, which the SCI entity has determined, after due investigation, have the most potential to materially impact the core functions and critical operations of the SCI entity, or those events that the SCI entity, in its reasonable discretion believes may potentially have a market-wide impact on the securities markets. All other events that trigger the notice requirement, but that do not have the risk of a material impact on the SCI entity itself, or the larger securities market, should be noticed to Commission staff by e-mail or telephone promptly during the next business day.

Commencement of an SCI Entity's Obligation to Notify the Commission of an SCI Event. The Release notes the Commission's preliminary belief that an SCI entity's obligation to notify the Commission of significant SCI events should begin upon any responsible SCI personnel becoming aware of an SCI event.

As currently proposed, notification would be triggered upon any responsible SCI personnel, defined as including, for example, a junior systems analyst responsible for monitoring the operations or testing of an SCI system or SCI security system, becoming aware that an event occurred. However, in order to comply with the proposed Regulation, each SCI entity would be required to establish, maintain, and enforce sufficient procedures to support the escalation and reporting of events that may, upon further investigation, be determined to be SCI events and subject to these notification requirements. Accordingly, DTCC believes that the SCI entity's obligation to notify the Commission of these SCI events should begin upon the responsible SCI personnel's notification to the officer or senior staff that are determined by the SCI entity to have responsibility for the SCI system, or systems generally.

Timing of SCI Entity Notifications on Form SCI. Rule 1000(b)(4) requires that the SCI entity, within 24 hours of notifying the Commission (orally or via e-mail) of an SCI event, provide written notice of the SCI event through the submission of Form SCI. Once the first point of contact is initiated (orally or via e-mail), that communication will continue, as necessary, until sufficient analysis of an event has taken place and a written description can be provided.

DTCC believes that the proposed requirement could place a burden on SCI entity staff to prepare and submit a Form SCI, and on Commission staff to review and assess the contents of that Form SCI, for SCI events that may not, upon further investigation, be of material interest to the Commission. Accordingly, DTCC believes a Form SCI should be required only in those cases when the Commission staff, after receipt of the verbal or e-mail notice of an SCI event, believes such written information would be beneficial and would promote the intent of Regulation SCI.

In most cases the information available 24 hours after an event has taken place will be premature, and information is very likely to change as an investigation into an event develops. DTCC believes the requirement that written notice on Form SCI be provided to Commission

staff 24 hours after the initial point of contact could create a significant risk that an SCI entity will provide incomplete or unconfirmed data, which would later need to be clarified and/or corrected. As DTCC believes that an SCI entity should have sufficient time to investigate an event and prepare written notification of such event only when there is adequate and reliable information available, DTCC believes that a Form SCI should not be required prior to 72 hours following the initial notice of an SCI event. This time frame should provide the SCI entity with sufficient time to properly investigate the event, thoughtfully assess the relevant information, and carefully prepare the contents of the Form SCI, and reduce the number of interim status updates that may be required.

DTCC fully supports proposed Rule 1000(b)(3), which requires an SCI entity to take appropriate corrective action to mitigate the impact of an SCI event as soon as practicable. However, resources that would be required to gather information during the critical 24 hours following the occurrence of an SCI event will be diverted from their more crucial task of addressing and resolving that event to preparing the notification. In assessing the appropriate time frame within which to require submission of a written notice, the Commission should consider any unintended conflict between this Rule 1000(b)(3) requirement and the proposed time frame for preparing written descriptions of an SCI event.

SCI Entity Notifications and Submission of Form SCI Outside of Business Hours. Regulation SCI notes that responsible SCI personnel may become aware of SCI events outside of normal business hours, and that the SCI entity would be required to notify the Commission at that time rather than, for example, the start of the next business day. DTCC believes that to reduce the potential burden upon the SCI entity and Commission staff, notification outside of normal business hours should be required only for SCI events determined by the SCI entity to have the most potential of causing a material negative impact on the SCI entity's core functions and critical operations, or the larger securities market.

Given the sensitivity of the information surrounding SCI events, preparing these written notices will require some consideration and internal review. This requirement will ensure that there is no unnecessary delay in preparing the written notice, but will not have the unintended consequence of diverting resources during a critical time or of creating the risk that information provided is inadequate or misleading because it has been hastily prepared to meet the 24-hour deadline.

- *Content of Written Notification.*

DTCC believes that SCI entities should not be required to include in their written notification, either to the Commission or to members of the public, an estimation of the markets and participants impacted by an SCI event, or to quantify such impact. This proposed requirement creates the risk that an SCI entity could face civil liability if this information is used against it as admission against interest with respect to potential losses suffered by third parties.

Further, given that the information available immediately after the occurrence of an event, and during the resolution and investigation into an event, will be premature, unclear, and subject to change, DTCC believes that written disclosures provided prior to resolution or

completion of an investigation into an event should be kept strictly confidential. Further, DTCC notes that the details required to be part of a complete Form SCI are very unlikely to be certain or available until this time, and there is a significant risk that the earlier disclosures could be misleading or incomplete. As such, DTCC believes that such details should not be required to be provided in writing until, at the latest, after the investigation into the event is complete and the event has been resolved, when the SCI entity is certain of the scope and impact of the event. Particularly with respect to the notices that are disseminated to members and participants under proposed Rule 1000(b)(5), preliminary notifications create a risk that firms will take market action in response to premature information, either exacerbating the impact of the event or causing other market harm.

Finally, DTCC supports the expectation that disclosures made in Form SCI be protected from public disclosure pursuant to the Freedom of Information Act, as mentioned on page 181 of the Release. DTCC believes the confidential treatment of these notifications should be made explicit in the text of the final Rule 1000(b)(4).

- *Determining Resolution of Event.*

Currently proposed Rule 1000(b)(4)(iii) provides that an SCI entity must continue to update a submitted Form SCI until the SCI event is *resolved.* DTCC believes that the final Rule 1000(b)(4)(iv)(iii) should make explicitly clear when a reporting obligation with respect to an SCI event has ended by defining the resolution of an SCI event as when the effected SCI systems have been *normalized*, or are functioning as they were before the event occurred.

- *Specific Comments on the Scope of Proposed Rule 1000(b)(5).*

DTCC supports the proposal to provide relevant information regarding *dissemination SCI events* to members and participants that could be impacted by those events. In certain circumstances, sharing this information will be important in reaching the collective goal of reducing risk and reducing the number of SCI events that may cause harm to the securities markets. However, DTCC believes that the publication of detailed information regarding certain SCI events and the steps being taken by the SCI entity to address those SCI events raises significant risk and serious security concerns, particularly with respect to information regarding a *systems intrusion* that could potentially reveal a vulnerability of an SCI system or the broader market infrastructure. DTCC believes proposed Rule 1000(b)(5) should make clear that the recipients of information regarding *dissemination SCI events* should be limited to only those members and participants that are actually impacted by the event; and that this information be shared with those parties on a confidential and secure basis. To stress the sensitivity and ensure the confidentiality of this information, these notices could be provided within a closed system or secure data sharing portal maintained by the Commission.

DTCC's recommendation reflects the general understanding that any public communications must necessarily take into careful consideration the recipient's level of understanding of the matters being communicated and the value of that recipient's expected reaction to that information. While DTCC fully supports the need for transparency with respect to these matters, particularly when a member or participant is impacted by an SCI event, DTCC

urges the Commission to recognize the need to craft any public reporting requirements carefully, particularly considering the sensitive nature of this information, to ensure the output is meaningful and the public consuming the information is able to make an informed calculation of the impact. As noted above, and particularly with respect to the notices that are disseminated to members and participants under proposed Rule 1000(b)(5), preliminary notifications create a risk that firms will unnecessarily react to premature information and will exacerbate the impact of the event or cause other market harm. DTCC believes it would be appropriate to require this information be provided only to those members or participants that are impacted by the dissemination SCI event, as well as to other SCI entities that may experience similar events, in a secure manner, and only at a point in time when that information is certain and clear.

3. Proposed Rule 1000(b)(9): Business Continuity and Disaster Recovery Plans Testing Requirements for Members and Participants

Proposed Rule 1000(b)(9) addresses testing of an SCI entity's business continuity and disaster recovery plans, including back-up systems, by SCI entity members or participants, and would require that these tests be conducted on an industry- or sector-wide basis. DTCC's comments to proposed Rule 1000(b)(9) are below.

Member functional and performance testing with an SCI entity as proposed by the Regulation could introduce risk to these tests, and SCI systems may need to be re-built to accommodate this testing structure and mitigate these risks. In proposed Rule 1000(b)(9), the Commission has included within the scope of "testing", both functional testing (e.g., testing as to whether a system operates in accordance with its specifications) and performance testing (e.g., whether a system is able to perform under a particular workload). DTCC believes that the testing structure proposed by Rule 1000(b)(9), specifically the requirement that an SCI entity's members participate in functional and performance testing (as opposed to communication and connectivity testing, which DTCC currently conducts with its members), could expose the SCI entity and its members to risk. For example, during disaster recovery testing, the network around the testing data center is closed to ensure that no production data is inadvertently sent to the test area. At the end of a test all data within that test center is destroyed. Opening a connection to these tests to members creates a significant risk that those members could mistakenly transfer production data into the testing systems during the testing. That production data would necessarily be lost after the test is complete and when systems are reverted to the original configuration.

DTCC believes that the testing proposed by Rule 1000(b)(9) would not be supported by most SCI entities' current systems configurations, which have been developed in a way that protect participants against the inadvertent processing of production data on test systems and test data on productions systems. While DTCC supports the Commission's goals in proposing this enhanced structure for business continuity and disaster recovery testing, it believes that implementation of Rule 1000(b)(9), as currently proposed, would require DTCC and most SCI entities to re-architect their existing IT infrastructures. DTCC believes that this re-architecting could take a significant amount of time and expense, diverting time and resources from other industry initiatives. DTCC asks that the Commission consider these factors in adopting testing requirements.

With respect to the requirement that an SCI entity's backup systems be tested, DTCC notes that extended periods of time would be needed to establish, execute on, and decommission backup systems contained at alternate data centers. During this time, the back-up data center would be required to perform core functions, negating the redundancy of these systems. This could create significant risks in the industry when these tests are being performed simultaneously.

Annual testing. In response to the Commission's Request for Comment #146 on page 161 of the Release, DTCC agrees with the existing proposal to require business continuity and disaster recovery testing once annually, and does not recommend that these tests be mandated more often. Most SCI entities have multiple data centers, and will need to test each during the course of a year. DTCC's existing business continuity and disaster recovery plan testing involves an industry wide test coordinated by the Securities Industry and Financial Markets Association (SIFMA), its own connectivity or communication testing with its members and participants on a rolling basis throughout the year, and connectivity testing with critical third parties. DTCC believes this multi-tier approach to business continuity and disaster recovery plan testing is effective in achieving the objectives of proposed Rule 1000(b)(9) without causing disruption or risk to critical operations, and asks that the Commission consider this model when contemplating the testing requirements proposed by the Regulation. DTCC also believes that further clarification is needed to make clear that any entity that could be considered a "member" or "participant" of multiple SCI entities is not in a position where it is regularly required to participate in multiple, separate testing by multiple separate SCI entities at any time and with little notice.

Coordination of testing among SCI entities. Proposed Rule 1000(b)(9)(ii) would require SCI entities to coordinate testing on an industry- or sector-wide basis with other SCI entities. In response to the Commission's Request for Comment #151 on page 163 of the Release, DTCC believes that the logistics supporting this effort, including the timing, structure, and governance around any industry- or sector-wide testing of business continuity and disaster recovery plans would require coordination by a central entity with regulatory authority over all SCI entities, or by an organization that has been clearly tasked with that responsibility by industry regulatory authorities.

4. Proposed Rule 1000(f): Access to Systems of SCI Entities

Proposed Rule 1000(f) requires SCI entities to provide the Commission staff with reasonable access to SCI systems and SCI security systems. As currently written, proposed Rule 1000(f) could be interpreted to suggest that Commission staff be given full access to these crucial systems, which would create serious security concerns and would be contrary to Regulation SCI's goal of enhancing the control around and security of these critical systems. Any access to these systems introduces significant risk and requires a deep understanding of the impact of every action taken within that system. As an example, even access on a read-only basis has the risk of slowing processing within a system if queries returning a large quantity of data were generated during peak processing times.

One possible alternative approach could be to require that SCI entities provide Commission staff with reports and metrics that provide an assessment of the configuration and vulnerability status of the SCI systems through a security content management protocol. To stress the sensitivity and ensure the confidentiality of this information, these reports could be delivered to the Commission through a secure data sharing portal maintained by the Commission. Alternatively, DTCC believes the goals of this requirement could also be met if SCI entities were required to demonstrate its controls, technology safeguards, and related procedures to Commission staff during the course of regularly scheduled examinations. Each of these recommendations would create a clearly defined, efficient way for Commission staff to perform their supervisory function, and will ensure access to these systems does not compromise the underlying goal of Regulation SCI to maintain the integrity of SCI systems. DTCC recognizes the value in providing Commission staff with transparency regarding the systems that are integral to the core functions of an SCI entity. Accordingly, DTCC believes that proposed Rule 1000(f) should be refined so that it is applied in a way that does not undermine the fundamental principle that any access to SCI systems and SCI security systems could compromise their proper operations, and, as such, must necessarily be restricted and tightly controlled.

5. Additional Comments to Proposed Regulation SCI

A. Proposed Rule 1000(b)(1): Policies and Procedures

Proposed Rule 1000(b)(1) requires SCI entities to establish, maintain, and enforce certain written policies and procedures that are designed to ensure the SCI systems and SCI security 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. In proposed Rule 1000(b)(1)(i)(A)-(F), the Commission sets forth the specific areas these policies and procedures must address. DTCC's comments on these specific requirements are set forth below.

First, DTCC believes it is important to specify that the capacity estimates required within proposed Rule 1000(b)(1)(i)(A) apply to *technology* infrastructure capacity, and recommends that this proposed Rule be revised as follows: "establishment of reasonable current and future *technology infrastructure* capacity planning estimates."

Additionally, DTCC recommends that proposed Rule 1000(b)(1)(i)(B) be revised to take into consideration SCI systems that do not require stress testing to address the risks they may pose. For example, DTCC regularly conducts risk assessments to determine the most appropriate way to test its various systems, and these assessments have shown that stress testing may not be necessary with respect to all systems. As such, DTCC recommends this proposed Rule be revised to make clear that testing of certain systems could be conducted within a scope that is reasonably determined by the SCI entity using risk-based assessment criteria, and either through stress testing in a non-production environment, or through mathematical capacity models.

Further, DTCC notes that proposed Rule 1000(b)(1)(i)(E) has made what is currently a *target* within the 2003 Interagency White Paper that clearing and settling services be resumed within 2 hours of a disruption into a *requirement* that may not be attainable in all circumstances, and may not be necessary to meet the goals of the requirement.[2] SCI entities are unable to predict the nature and scope of future disruptions, and must be prepared to address events they have not experienced in the past. While a 2-hour window for resumption of these services may be possible in some scenarios, it is not possible to ensure an SCI entity may satisfy this requirement following every future disruption. Therefore, DTCC believes that a strict requirement that these services be resumed within this tight time frame is unduly burdensome and not appropriate in all circumstances. The 2003 Interagency White Paper requires clearing and settling services be resumed on an *intraday basis*, and when possible, within 2 hours of a disruption. DTCC believes this requirement adequately meets the stated goal of ensuring that these entities have contingency plans to avoid a scenario in which failure to settle transactions by the end of the day could present systemic risk to the market. Furthermore, securities markets have changed drastically since 2003. Entities that perform clearing and settling services have grown more complex, processing a significantly greater volume of data within shorter timeframes and on a greater number of platforms than any time in the past. While these entities should be obligated to resume clearing and settling services in the fastest, safest possible timeframe, a 2-hour time frame may no longer be feasible in today's markets.

Finally, DTCC notes that proposed Rule 1000(b)(1)(ii) provides a "safe harbor" for SCI entities to ensure compliance with proposed Rule 1000(b)(1)(i) where its policies and procedures are consistent with SCI industry standards that are available at no cost in the financial sector. DTCC believes this criterion would unnecessarily exclude ISO 2700,[3] which is available for a fee and is generally considered to be the appropriate set of standards to apply to *commercial* systems. DTCC recommends expanding the set of industry standards identified in connection with proposed Rule 1000(b)(1)(ii) to allow inclusion of this well-developed and applicable set of standards.

B. Proposed Rule 1000(b)(6): Notification of Material System Changes

- *"material system changes"*

Proposed Rule 1000(a) defines *"material system changes"* as "a change to one or more: (1) SCI systems of an SCI entity that: (i) materially affects the existing capacity, integrity, resiliency, availability, or security of such systems; (ii) relies upon materially new or different technology; (iii) provides a new material service or material function; or (iv) otherwise materially affects the operations of the SCI entity; or (2) SCI security systems of an SCI entity that materially affects the existing security of such systems." DTCC supports this definition, but

---

[2] Specifically, the White Paper states, "... core clearing and settlement organizations should develop the capacity to recover and resume clearing and settlement activities *within the business day on which the disruption occurs* with the overall goal of achieving recovery and resumption within two hours after an event." Available at http://www.sec.gov/news/studies/34-47638.htm.

[3] The ISO 2700 series of standards are available at http://www.27000.org/.

is concerned that the examples provided in the Release as illustrating the types of changes that would trigger the related notice requirement do not have adequate materiality thresholds necessary to capture system changes that occur outside the ordinary course of business.

The Release states that the Commission staff considers a significant system change to include, among other things, reconfiguration of systems that cause a variance greater than five percent in throughput or storage. DTCC believes that a reconfiguration of systems that causes a variance greater than five percent in throughput or storage would be considered an ordinary course of business change that may occur too frequently to be appropriately captured by this notice requirement. Considering the variety of SCI entities and the diversity of their infrastructures, DTCC recommends that the Commission consider permitting each SCI entity to determine a threshold that would capture changes that are material to their systems and impact that entity's core functions and critical operations.

Further, DTCC believes that SCI entities should not be required to speculate when a change *could* increase susceptibility to major outages or *could* increase risks to data security when determining if a notification of this change is required. DTCC recommends that SCI entities be required to include in these notifications only those changes the SCI entity believes, in its reasonable discretion, presents a *significant risk* of increasing susceptibility to major outages and a significant risk of increasing risks to data security.

C. Proposed Rule 1000(b)(7): SCI Review

Proposed Rule 1000(b)(7) would require an SCI entity to conduct an SCI review of its compliance with Regulation SCI not less than once each calendar year, and to submit a report of the report of that SCI review to senior management of the SCI entity no more than 30 calendar days after completion of such SCI review. Further, proposed Rule 1000(a) would define "SCI review" as "a review, following established procedures and standards, that is performed by objective personnel having appropriate experience in conducting reviews of SCI systems and SCI security systems, and which review contains: (1) a risk assessment with respect to such systems of the SCI entity; and (2) an assessment of internal control design and effectiveness to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards."

Certain audit reviews are more appropriately performed on a rotational basis, which may be less often than annually. While proposed Rule 1000(b)(7) requires an annual review of broad areas of technology controls, DTCC believes that separate focused audit reports, that are performed on a rotational basis, rather than annually, provide more value than a separate and consolidated report prepared on an annual basis. DTCC advocates requiring a robust and risk-focused audit plan around technology controls, and notes that the Institute of Internal Auditors, which operates essentially as a self-regulatory organization within the internal audit profession, advocates a risk-based rotational approach to auditing. For example, DTCC's existing annual audit plan is performed in accordance with accepted best practices in the profession and the scope of its audit projects include the areas specified in proposed Rule 1000(7). In any given year DTCC's Internal Audit Group produces more than 20 audit reports of various aspects of technology controls at DTCC. Each of these reports is detailed and focused on a specific area.

As currently written, the proposed Rule 1000(b)(7) does not recognize that risk assessments may suggest that certain areas be reviewed less frequently than annually, due either to the limited inherent risk presented by those areas or due to the quality of the control environment in those areas. As a result, the proposed requirement could result in the internal audit function of an SCI entity needing to dedicate significant resources to areas of potentially lower risk.

Therefore, DTCC recommends that Regulation SCI require focused reviews of certain areas within the security and technology groups performed on a rotational basis, based on the SCI entity's risk-assessment of the reviewed area. DTCC believes that a consolidated report on an end-to-end testing of an SCI entity's technology controls would be more valuable if performed on a less frequent basis, for example once every three years. DTCC also recommends that the individual, focused audit reports be delivered to the Commission in bundles on a quarterly or semi-annual basis, rather than on a report-by-report basis.

Additionally, DTCC notes that penetration testing is a highly technical area, often requiring the use of experts. As such, DTCC recommends that it would be more appropriate for reviews of penetration testing be separated from other auditing of technology controls and reported on separately.

Consider setting a target for delivery of the audit reports to management 45 days following completion. Proposed Rule 1000(b)(7) would require that a report be delivered to management no later than 30 days after completion of the review. DTCC believes that, given the complexity of the issues often raised in an audit review, this timeframe is not likely to be sufficient to ensure that robust action plans can be created. Typically the reporting process for audit reports will require relevant members of management to create action plans to address the issues raised by the Internal Audit team. Those proposed actions are then reviewed by the Internal Audit team before the report is completed. Further, DTCC believes that it is not appropriate to set absolute deadlines in these circumstances, as that requirement could lead the auditors or reviewing parties to take short-cuts in the report clearance process, which would hurt the quality of the end product. Therefore, DTCC recommends that the final Rule 1000(b)(7) set a target delivery date for each audit report of *45 days* following completion of the review, and further provide that in the circumstances when a report fails to be delivered to management within that target timeframe, the Board of Directors Audit Committee, or a similar governing body within the SCI entity, be informed of the reason the target delivery date was not met.

Additional Comments on Rule 1000(b)(7). Proposed Rule 1000(b)(7) suggests the annual review be consistent with "established procedures and standards", which would include, according to Table A on pages 100-102 of the Release, standards issued by the Federal Financial Institutions Examination Council (FFIEC) and standards issued by Institute of Internal Auditors (IIA). DTCC understands that the FFIEC may be issuing new standards in 2013, and those new standards will need to be reviewed and analyzed before DTCC will be in a position to provide comments to this requirement.

Finally, SCI entities that are registered clearing agencies also follow the Commission's guidelines in the Announcement of Standards for the Registration of Clearing Agencies,[4] which call for an annual report on internal controls performed by a designated third party. The work to support that annual review, which, for DTCC, is currently performed by its external auditors, includes certain technology controls and therefore partially overlaps with proposed Rule 1000(b)(7). DTCC believes that the Commission should consider coordination with these separate requirements to avoid redundant regulatory requirements.

D. Application of Regulation SCI to SB SDRs

DTCC is in a unique position to discuss whether the requirements proposed under Regulation SCI should be applied to security-based swap data repositories ("SB SDRs"), as well as other enumerated SCI entities, because DTCC, through its subsidiaries, operates one of the swap data repositories, which will apply to become as SB SDR once the Commission's proposed SB SDR regulations are final.[5] DTCC believes the role SB SDRs will play in the securities markets are different and should have standards that are consistent with, but not identical to, those of other SCI entities. Some of the critical distinctions between the SB SDRs and other SCI entities include that SB SDRs are not involved in trade matching or execution, netting, or settlement or post-trade processing. Although SB SDRs will provide market transparency by disseminating real-time pricing information to the public, the primary function of the SB SDRs is to accept security-based swaps data and act as a repository for such data. Therefore, the functions that the SB SDRs perform are significantly different than those performed by other SCI entities.

Although DTCC does not believe that the requirements of the proposed Regulation SCI should be applied in their entirety to SB SDRs, DTCC does support the application of certain provisions to SB SDRs in order provide appropriate system safeguards to the security-based swap markets. DTCC supports the application of the following elements of the proposed Regulation SCI, subject to the comments made in this Letter, to SB SDRs:

- *Capacity, Integrity, Resiliency, Availability and Security*: DTCC agrees that SB SDRs should establish, maintain and enforce written policies and procedures that are designed to meet the requirements of proposed Rule 1000(b)(1)(i)(A)-(E). DTCC believes that specific industry standards should be adopted for SB SDRs, rather than adopting existing standards that were largely developed before repositories were developed and were not intended to cover these types of entities.

- *Notifications to the Commission*: DTCC supports the requirement to provide the Commission with notification of various types of events impacting the SB SDRs' systems, but would recommend that, as this requirement is applied to SB SDRs,

---

[4] *See* Securities Exchange Act Release Nos. 16900, 45 FR 41920 (June 23, 1980), *available* at http://www.sec.gov/rules/other/34-16900.pdf.

[5] Securities Exchange Act Release Nos. 63347 (November 19, 2010), 75 FR 77306 (December 10, 2010) (proposing new Rule 13n-6 under the Exchange Act applicable to SB SDRs) (the "proposed SB SDR Regulations").

the Commission adopt the notification provisions that are described in Section 13n-6(3) of the proposed SB SDR Regulations.

- *Business Continuity Planning & Testing*: DTCC does not believe that conducting testing with other SB SDRs is necessary given the structure of the proposed SB SDR Regulations.

DTCC believes that these provisions, in addition to those that have already been incorporated into the proposed SB SDRs Regulations, will provide appropriate system safeguards to the security-based swap markets and are appropriate for the function that SB SDRs serve in this market. In order to avoid confusion and provide greater consistency with the existing CFTC regulations applicable to SDRs, DTCC would recommend that these provisions be incorporated into the final version of the proposed SB SDR Regulations by incorporating these requirements into section 13n-6 of those final regulations, rather than make Regulation SCI applicable to these entities. Not only would this approach avoid confusion for other SCI entities, but it would also further harmonize the Commissions systems safeguards with the requirements that are imposed on entities that are already registered as an SDR and those that will seek to register as an SB SDR once the Commissions proposed SB SDR regulations are final.

Conclusion

DTCC appreciates the opportunity to comment on the proposed Regulation SCI and looks forward to participating in continuing development of these important proposals. Should you wish to discuss these comments further, please contact me at (212) 855-3240 or lthompson@dtcc.com.

Regards,

Larry E. Thompson

Larry E. Thompson
Managing Director and General Counsel