55 WATER STREET
NEW YORK, NY 10041-0099

TEL: 1-212-855-2670
Mcollazo@dtcc.com

February 22, 2016

Mr. Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, D.C. 20581

Re: System Safeguards Testing Requirements [RIN 3038-AE30]

Dear Mr. Kirkpatrick,

The Depository Trust & Clearing Corporation ("DTCC"),[1] in conjunction with its provisionally registered swap data repository ("SDR"), DTCC Data Repository (U.S.) LLC ("DDR"), appreciates the opportunity to provide comments to the U.S. Commodity Futures Trading Commission ("CFTC" or "Commission") regarding proposed amendments to existing regulations addressing cybersecurity testing and safeguards for designated contract markets, swap execution facilities, and SDRs.

DTCC commends the CFTC for its efforts in strengthening system safeguards and cyber security testing. The proposed amendments are constructive steps in addressing key issues and serve to establish a common baseline level of protection.

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 industry, we maintain and invest in elaborate and sophisticated information security programs to protect against cybersecurity attacks. DTCC strongly believes that comprehensive testing programs and safeguards are necessary components in the ability of SDRs to strengthen cyber defenses, mitigate risk, maintain cyber resilience and recover from cyber attack.

[1] The Depository Trust & Clearing Corporation ("DTCC") provides critical infrastructure to serve all participants in the financial industry, including investors, commercial end-users, broker-dealers, banks, insurance carriers, and mutual funds. DTCC operates as a cooperative that is owned collectively by its users and governed by a diverse Board of Directors. DTCC's governance structure includes more than 300 shareholders.

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.[2] Operationally, DTCC has implemented redundant systems at alternate locations and frequently tests core system availability in the event of an emergency. Through a redundant and geographically dispersed operations infrastructure, DTCC's technology infrastructure and IT platform enable it to effectively provide support to the financial markets.

GENERAL COMMENTS

As a general matter, DTCC commends the Commission for adopting an approach to enhance system safeguards for registered entities – such as SDRs – that acknowledges the evolving risk environment by avoiding a rigid or overly prescriptive regulatory framework. The CFTC rightly notes that the risk environment for firms has expanded from events such as storms or physical attacks to encompass cybersecurity threats that could potentially result in loss of data integrity or long-term cyber intrusion. Likewise, the nature of cybersecurity threats will continue to change as well, requiring nimble and discretionary operational responses from the Commission's registered entities. A regulatory framework for providing for appropriate system safeguards that relies on principles as well as continually updated industry best practices – as proposed by the Commission's release – is the most appropriate way to allow for the requisite vigilance, discretion and nimbleness that today's and tomorrow's threats require.

DTCC notes that the CFTC's proposal distinguishes between resumption of an SDR's operations, duties and obligations on the one hand, and recovery on the other,[3] and provides a reasonable objective for an SDR to meet regarding resumption that is commensurate with an SDR's current regulatory responsibilities.[4] The distinction is important because while a cyber event might have impaired an SDR's capabilities, it might not have led necessarily to a processing outage or disruption. The Commission's release also appropriately recognized the differences among financial market infrastructures and the varying requirements for resumption and recovery timeframes. Again, these types of distinctions collectively create a regulatory framework that better provides the necessary discretion needed by operators of registered entities to respond nimbly to cyber events while continuing to meet their various regulatory obligations, which in the case of SDRs includes providing regular access to swap data to the Commission.

SPECIFIC COMMENTS

DTCC has identified several areas in the release that we encourage the CFTC to carefully consider when working to finalize the proposal. DTCC welcomes the opportunity to further discuss

---

[2] DTCC provides services for a significant portion of the global over-the-counter ("OTC") derivatives market and through its trade repository subsidiaries, supports regulatory reporting in the U.S., Europe, Japan, Australia, Singapore, Hong Kong and Canada.

[3] DTCC notes that this distinction is consistent with definitions provided in the Glossary to the Consultative Report released by CMPI-IOSCO on November 24, 2015, where "recover" means to "restore any capabilities or services that have been impaired due to a cyber event" and "resume" means to "recommence critical functions following a cyber incident."

[4] *See* Federal Register 17 CFR 49.24 referring to SDR resumption of operations and ongoing fulfillment of duties and obligations during the next business day following the disruption, available at https://www.gpo.gov/fdsys/pkg/CFR-2012-title17-vol1/pdf/CFR-2012-title17-vol1-sec49-24.pdf

any of these comments and to provide additional recommendations related to system safeguards testing requirements.

1. *Alignment with Industry Best Practices*

DTCC agrees that any proposed rulemaking on this subject of cyber testing should closely align with industry best practices for cybersecurity, including for example the National Institute of Standards ("NIST") Technology Framework for Improving Critical Infrastructure Cybersecurity ("NIST Cybersecurity Framework") and the International Organization for Standardization ("ISO") Framework.

DTCC encourages the Commission, therefore, to make clear in the finalized rule that abiding by or relying on any generally accepted industry framework, such as the NIST Cybersecurity Framework or the ISO Framework, as they exist today and later evolve in response to newly identified cyber security threats, when an SDR develops its own policies, procedures and controls will result in compliance with the Commission's cybersecurity regulatory framework. Providing this clarification would appropriately encourage reliance on a consensus-based and industry-accepted framework that embodies the requisite baseline of risk management for SDRs, and discourage an unnecessary proliferation of risk-management approaches that ultimately could create confusion for both the community of registered entities as well as the official sector supervising it.

2. *Clarification Regarding Acceptable Use of Independent Contractors*

As stated in the CFTC's proposed rulemaking, independent testing by third party service providers is an essential component of an adequate testing regime. The use of third parties for testing under the appropriate circumstances provides an external perspective and scalability that exclusive reliance on internal testing would not afford. DTCC, therefore, supports the use of independent contractors to perform specific system safeguards and cybersecurity testing.

There is, however, a point when too much reliance on independent contractors to perform certain types of testing could introduce unnecessary risk into critical infrastructure. For example, to perform vulnerability testing, an independent contractor must be provided access to an SDR's critical infrastructure and the testing would involve connecting hardware and the usage of external software to execute the tests. Consequently, each instance of such third party-performed testing presents heightened risks of system outages at the SDR due to its system's exposure to the vendor's uncontrolled testing environment, and therefore increases the risk that the SDR's reporting obligation would be frustrated, thus impairing the Commission's ability to meet its own regulatory responsibilities.

For these reasons, DTCC strongly recommends against requiring the use of independent contractors for any of the quarterly vulnerability tests. To mitigate risk while still maintaining an independent view of vulnerability testing, DTCC recommends that SDRs conduct vulnerability testing and that independent contractors validate that the SDR's testing procedures are in line with industry standards. This approach would allow independent contractors to evaluate the effectiveness of testing while avoiding risks stated above.

In addition, DTCC believes that SDRs should have flexibility regarding the use of independent contractors or an independent group within the SDR, such as an Internal Audit or

Compliance department, for other testing based on the risk the systems pose to an organization and the structure of the organization. Such a determination would be based upon an SDR's risk assessment.

3. Board of Directors and Management Oversight of System Safeguards

DTCC agrees with the Commission that active supervision by senior management and an SDR's board of directors promotes a more efficient, effective, and reliable SDR risk management and operating structure and that consequently, SDRs should be better positioned to strengthen the integrity, resiliency, and availability of their automated systems.

DTCC further believes it is the responsibility of an SDR to provide its board access to the appropriate system safeguards and cyber resiliency information in order to perform effective oversight. DTCC recommends that the Commission, in its final adopting release, continue to acknowledge that there are many ways in which an SDR can ensure its board remains appropriately informed, and likewise many ways an SDR's board as a whole can adequately reflect the necessary expertise and knowledge in cybersecurity matters to properly exercise its authority.

Conclusion

DTCC appreciates the opportunity to comment on the proposed system safeguards testing requirements rulemakings and looks forward to participating in continuing development of these important proposals. Should you wish to discuss these comments further, please contact me at MCollazo@dtcc.com or at 1-212-855-2670.

Regards,

Marisol Collazo
Chief Executive Officer, DTCC Data Repository (U.S.) LLC