DTCC
ADVANCING FINANCIAL MARKETS. TOGETHER.™

Stephen Scharf
Managing Director &
Global Chief Security Officer

DTCC Boston
55 Thomson Place
Boston, MA 02210

Tel: +1 212 855 4844
sscharf@dtcc.com

July 20, 2020

Via electronic mail

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
CIRR@fsb.org

Re: FSB Consultative Document "Effective Practices For Cyber Incident Response and Recovery"

Dear Sir/Madam:

The Depository Trust and Clearing Corporation ("DTCC") welcomes the opportunity to respond to the Financial Stability Board ("FSB") Consultative Document, "***Effective Practices For Cyber Incident Response and Recovery***" ("Consultation" or "CIRR Toolkit").[1] DTCC commends the FSB on its continued efforts to strengthen cybersecurity and cyber resilience through its prior works such as the ***Stocktake Of Publicly Released Cybersecurity Regulations, Guidance, and Supervisory Practices*** (2017)[2] and the ***Cyber Lexicon***, which created a "[c]ross-sector common understanding of relevant cyber security and cyber resilience terminology" to "provide guidance related to cyber security and cyber resilience, including identifying effective practices."[3]

[1] FSB, Effective Practices For Cyber Incident Response and Recovery (20 April 2020), available at https://www.fsb.org/wp-content/uploads/P200420-1.pdf.

[2] FSB, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices (13 October 2017), available at https://www.fsb.org/wp-content/uploads/P131017-2.pdf (outlining the proliferation of supervisory texts and demonstrating the significant number of global approaches to managing financial services sector risk to cybersecurity incidents).

[3] FSB, Cyber Lexicon (12 November 2018) ("Cyber Lexicon"), available at https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

The comments below are intended to further this work by providing (i) several high-level suggestions that could help clarify and improve the usefulness of the document for practitioners and regulators and (ii) specific feedback on the CIRR Toolkit's recommended practices.

I. AN OVERVIEW OF DTCC

DTCC, through its subsidiaries, is the largest post-trade market infrastructure for the global financial services industry and supports its mission to protect clients, the financial markets and systems as a whole through a sophisticated technology infrastructure.[4] Given DTCC's critical role in the industry, we maintain and invest in sophisticated information security programs to protect against cybersecurity attacks and provide thought leadership on cyber topics.[5] DTCC has a comprehensive cyber resilience program, which includes internal cybersecurity policies and procedures as well as thorough system safeguards and testing programs. These efforts are intended to strengthen our cyber defenses, mitigate risk, maintain cyber resilience and recover from a cyber-attack.

II. General Comments

It is our understanding that the FSB seeks to provide the following benefits to financial institutions through the CIRR Toolkit:

1. access to effective cyber incident response and recovery ("CIRR") practices that may be used by financial institutions that lack access to the expertise to develop an effective CIRR program;
2. access to effective CIRR practices that financial institutions may consider adopting to enhance their current programs;

[4] DTCC is the parent company and operator of the U.S. cash market securities CCPs, National Securities Clearing Corporation ("NSCC") and Fixed Income Clearing Corporation ("FICC"), both of which have been designated as systemically important financial market utilities ("SIFMUs") by the U.S. Financial Stability Oversight Council ("FSOC") pursuant to Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank"). NSCC and FICC provide critical clearing and settlement services for multiple asset classes, including US equities, corporate and municipal bonds, and government and mortgage-backed securities. DTCC is also the parent company of The Depository Trust Company ("DTC"), the U.S. central securities depository. NSCC, FICC, and DTC are registered under the Securities Exchange Act of 1934, as amended, as clearing agencies, and are supervised by the U.S. Securities and Exchange Commission ("SEC").

[5] See the Joint DTCC-Oliver Wyman White Paper titled "Large-Scale Cyber-Attacks on the Financial System: A Case for Better Coordinated Response and Recovery Strategies" (March 2018), available at https://www.dtcc.com/-/media/Files/Downloads/WhitePapers/Cyber-White-Paper-DTCC-OW.pdf.

3. information that a board of directors can use to gain greater understanding of its institution's CIRR program; and
4. information that supervisors/regulators can use to understand the different practices employed by financial institutions to address cyber incidents.

These are laudable goals that we support. However, it is important that the FSB underscore that the absence of one or more of these practices does not suggest that a financial institution's CIRR program is deficient. While the Consultation's Executive Summary states that these practices should not be considered as a one-size-fits-all, DTCC recommends that the FSB make clear that CIRR programs may differ based on the size, type, and complexity of business operations; customers and counterparties; markets and products traded; access to trading venues; and market interconnectedness. Further emphasizing that the toolkit is a voluntary set of practices that may be used by financial institutions to enhance their programs should both help avoid confusion and encourage participation, which would raise the Sector's preparedness to respond and recover from cyber incidents.

In addition, the Consultation notes that "[t]he toolkit may also be useful for authorities as they consider the approaches that they may undertake with respect to regulation or supervision, or in responding to a cyber incident within the Sector."[6] Although we agree with this statement, since the CIRR Toolkit reflects a voluntary set of tools derived from a wide set of financial institutions with varying maturity, we believe it is important to underscore the flexibility of these practices and the fact that they are not intended to be prescriptive requirements. DTCC recommends that supervisory approaches derived from these practices be globally coordinated, aligned to industry standards and best practices, and principles-based to give financial institutions flexibility in the development and implementation of comprehensive CIRR programs. When financial institutions follow flexible principles-based regulatory requirements and proven industry standards and best practices, the result is a solid foundation for a robust cyber defense system.

A. Alignment to Industry Standards and Best Practices

DTCC recommends that the CIRR Toolkit align more closely with other widely adopted and utilized industry standards and best practices. Industry standards and best practices promote consistency in the development and promulgation of principles, guidance, rulemaking, and rule

[6] Consultation at 2.

interpretation. When these standards and best practices are not followed, regional, national, or jurisdictional approaches tend to diverge, which introduces market fragmentation. In developing the Cyber Lexicon, the FSB recognized the importance of a "Cross Sector common understanding of relevant cyber security and cyber resilience..."[7] DTCC supports the FSB in the implementation of this principle and has identified ways that the CIRR Toolkit can be improved to better advance the principle.

Specifically, we are concerned by how the structure of the FSB's Toolkit is broken out into the following areas: '*Governance*', '*Preparation*', '*Analysis*', '*Mitigation*', '*Restoration*', '*Improvement*', and '*Coordination and Communication*'. While these terms closely approximate commonly used frameworks such as NIST Cybersecurity Framework (NIST CSF)[8] and the draft ISO 27101 – Cybersecurity Framework Development Guidelines,[9] they still deviate from the terminology used in those frameworks.[10] These deviations in terminology could lead to disparate supervisory interpretations and thereby undermine the aforementioned principle of promoting a common lexicon. They can also be costly for financial institutions that operate in multiple jurisdictions.

Disparate supervisory approaches to cybersecurity and the existence of multiple frameworks result in financial institutions re-allocating cyber resources towards resource-intensive mapping exercises and away from activities supporting the institution's cyber strategy, goals, and objectives. DTCC urges the FSB to consider utilizing the Financial Services Sector Cybersecurity Profile (the "Profile")[11] as a tool to promote use of a common lexicon. The Profile is an industry-developed convergence instrument that is based on commonly accepted cybersecurity frameworks (*e.g.*, NIST CSF, ISO 27000). Financial institutions can use the tool for internal and third-party cyber risk management assessment and to evidence compliance with regulatory requirements that are based on commonly accepted cybersecurity frameworks. As such, the Profile could similarly be used to showcase the effective practices a financial

[7] Cyber Lexicon at 3.

[8] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[9] The draft ISO 27101 – Cybersecurity Framework Development Guidelines can be found at: https://www.iso27001security.com/html/27101.html

[10] *See infra* at 5.

[11] FSSCC Financial Sector Cybersecurity Profile available at: https://fsscc.org/Financial-Sector-Cybersecurity-Profile

institution adopts into its CIRR framework. Use of the Profile would also allow supervisory authorities to acquire a deeper understanding regarding the types and contours of such effective practices, and how they are integrated into a financial institution's overall risk framework. This will provide a more accurate representation of a practice's effectiveness and a means to understand differences among CIRR programs across institutions that have similar impacts to market stability or consumer harm. DTCC supports additional public-private partnerships to demonstrate how the Profile could support both supervisor and financial institution effectiveness when reviewing and implementing cyber risk management programs.

B. CIRR Program Proportionality

DTCC commends the FSB on its collection of effective practices from across market participants. These practices reflect approaches that have been demonstrated, by the financial institutions that proposed them, to provide the greatest benefit to their CIRR programs. However, there are some practices that while effective, may be cost-prohibitive, resource-intensive, or require a level of CIRR program sophistication to implement, which may limit the availability of that practice for some financial institutions. As an example, participation in cross-sectoral tabletop exercises requires a certain level of program sophistication to derive actionable value from participation in these exercises. In addition, Red/Blue Team testing requires access to specific expertise and is resource-intensive, complex, highly technical, and costly. The implementation of these practices will therefore depend on the size, type, and complexity of business operations, clients and counterparties, markets and products traded, market interconnectedness and systemic impact. As such, it is important to emphasize the importance of proportionality[12] for institutions looking to adopt any of the practices set forth in this Consultation.

C. Definition and Reference Glossary

As noted previously, DTCC believes that the terms set forth in the CIRR Toolkit should be aligned with the definitions in the Cyber Lexicon. In addition, where the CIRR Toolkit includes terms that are not defined in the Cyber Lexicon, including a glossary of terms would provide

[12] Proportionality, in this context, means a limited applicability taking into consideration the goals the institution is seeking to achieve and the relative importance to financial stability. In other words, the costs of using a particular practice should not be outweighed by the value of what the practice intends to accomplish to avoid overly excessive costs and burdens, which could disproportionately harm smaller or less sophisticated financial institutions.

relevant stakeholders with a more consistent interpretation of the practices. For example, the term, "*Unity Of Command"* is not universally understood. Similarly, "cyber resilience" is used in a manner that appears to be synonymous with cyber incident response and recovery. A glossary defining these terms and ensuring consistent use should lower the probability for misinterpretation. This glossary should also include references to widely used resources that provide additional details for the listed practice areas to provide financial institutions with limited expertise in CIRR with useful starting point and additional information that would be useful as they seek to implement these practices within their institutions.

D. Supervisory Incident Reporting

Material cyber incidents[13] place significant stress on a financial institution to quickly restore operations and provide business services to its clients, participants and counterparties. These events may trigger multiple reporting requirements across national, regional, and local jurisdictions, which often differ in the information requested for reporting, the timeframe provided to report the incident, and the reporting approach (*e.g.*, some jurisdictions require an initial notification of the incident followed by a full report within a specified timeframe). Disparate regulatory requirements increase the probability that financial institutions will not meet all of their reporting obligations in an accurate and timely manner and take valuable resources away from resolving an incident in a ***rapid but safe*** manner. Accordingly, DTCC recommends that the FSB form a working group of supervisors, international standards setting bodies, and the private sector to develop a reporting strategy that would better coordinate these reporting requirements, reduce the reporting burden for affected institutions, and increase the resilience of financial institutions by freeing valuable resources to focus on the protection of such institutions and the sector as a whole .

III. EFFECTIVE CIRR PRACTICES

The CIRR Toolkit provides a set of 46 effective CIRR practices. Where possible, DTCC's comments focus on how CIRR Toolkit practices could be amended to further bolster the objectives of the expressed in the Consultation.

[13] Currently, regulatory supervisors do not have a common or shared definition of materiality. Supervisors define and assess materiality differently depending on their laws, regulations and other relevant standards. For the purposes of the Consultation, the definition of "material" should align with the definition used in other contexts for measuring systemic importance.

A. Governance: Role and responsibilities of the board.

The delineation between the accountability of a Board of directors (“Board”) and the responsibility of senior management is somewhat ambiguous so clarity in this regard would be beneficial. For example, the CIRR Toolkit attributes to the board and senior management the “responsibility of implementing the required improvements, including the funding and overseeing the set-up of new solutions within an acceptable timeframe.”[14] This responsibility should lie with senior management alone.

Specifically, DTCC believes that at its core, the Board is generally accountable for (1) confirming that the organization has a comprehensive plan that addresses material cyber and operational risks and can recover business operations in a ‘***rapid but safe****’* manner; (2) understanding that individuals are empowered and have the right level of expertise for conducting CIRR responsibilities; and (3) providing credible challenge to the financial institution’s CIRR strategy. Senior management, on the other hand, is responsible for the development, implementation and management of policies, standards, and controls that support the CIRR strategy, testing and implementation of the required improvements, funding and overseeing the implementation of the strategic and tactical elements of the CIRR. Including this level of clarity in the CIRR Toolkit would help align expectations among supervisory authorities and market participants across jurisdictions.

B. Governance: Roles, responsibilities, and accountabilities of CIRR.

As drafted, this practice appears to suggest taking the same incident response approach for incidents that may have low operational impact (*e.g.*, server outage) and incidents that may have a material operational disruption. While minor incidents may have an assigned “Incident Owner”[15] to manage the incident to closure, material operational disruptions may involve several organizational roles including, but not limited to: impacted business units, general counsel, communications/public relations, risk group, and information technology group. Combining the approaches to minor incidents and material operational disruptions may cause ambiguity for financial institutions that do not have access to CIRR expertise. By prescriptively defining the roles of the multidisciplinary incident coordination team, this practice leaves out the other organizational roles that may be involved in a cyber incident, which may differ depending on the incident. DTCC believes that this practice should take a more principles-based approach

[14] Consultation at 3.
[15] *Id.*

and state that organizations should clearly define role responsibilities and accountabilities for all organizational areas that may be involved in the recovery and response capabilities of a material cyber event.

C. Governance: Funding.

This practice includes several undefined terms. As discussed above, DTCC urges the FSB to include a glossary of terms, especially for terms that are not defined in the FSB's Cyber Lexicon, to promote consistent interpretation of this practice. For example, terms like "reliability" that can be a synonym of "resilience" or "critical functions" may be interpreted differently among financial institutions and by individual supervisory and regulatory agencies.

D. Preparation: Policies.

The description of policies in this practice appears to overlap with, and duplicate in part, the description of plans and playbooks in the "Plans and Playbooks" practice. For example, under this practice, the policies should "include a clear communication strategy and plan, which describe whom to inform of the cyber incident within a given timeframe, the information to be furnished and the channel used for notification."[16] However, policies are typically high-level statements that are supported by more detailed standards. Policies are normally more static than a plan or strategy. More specifically, policies identify the risk to be managed and the standards identify the minimum controls needed to manage the risk, while a plan may be specified as required by policy but managed outside of the policy document.

E. Preparation: Plans and Playbooks.

The language in this section introduces the term "cyber resilience" and it is unclear if cyber resilience and cyber incident response and recovery are being used interchangeably. Defining this term in a glossary, as discussed above, would avoid confusion and provide greater clarity.

F. Preparation: Disaster Recovery Sites.

This practice specifically requires a daily replication strategy. While this may be appropriate for some financial institutions, the practices in the CIRR toolkit should be less prescriptive. Replication frequency may depend upon the risk to the business operations if the data is

[16] Consultation at 5.

altered, unavailable for a certain period of time or otherwise destroyed. Accordingly, we suggest that this practice should take a more principles-based approach.

G. Preparation: Forensic Capabilities.

The practice states that "[t]he types of logs to be collected and retention period of logs are pre-determined"[17], however, the factors that may dictate collection and retention periods for log information are unclear. Examples or additional principles-based guidance in this regard would be beneficial.

H. Preparation: Third Party Cyber Services Provider.

DTCC fully supports the recommendation set forth in this practice and believes it is an important practice to highlight. Specifically, DTCC recommends including a statement to make clear that this practice may prove useful in the case of a system-wide cyber incident where a service provider may not be able to conduct a service with sufficient capacity to support all its clients.

I. Restoration: Prioritisation.

The toolkit recommends that "[o]rganisations prioritise restoration activities based on business, security and technical requirements."[18] DTCC does not agree with this statement and believes that organizations should prioritize restoration based on the criticality of a business and its services. This criticality drives the security, technical, and restoration requirements.

J. Restoration: Key Milestones.

The FSB should consider revising its guidance on key milestones. The redesign, reinstall, and reconfiguration of systems would not be key milestones in a CIRR plan. Rather, financial institutions would identify and define key times when important market activities need to occur and these times would drive the decision-making for restoration activities (*e.g.*, system reconfiguration/rebuild). In addition, the last sentence in this practice suggests incorrectly that the focus should be on restoring systems. Instead, the focus should be on resuming or continuing operations. Specifically, to better provide guidance to practitioners and supervisors, we recommend that the last sentence be amended to make clear that organizations should also

[17] Consultation at 7.

[18] Consultation at 10.

consider developing interim restoration goals/measures, such as continuing operations in a diminished capacity.

K. Improvement: Exercises, tests and drills.

DTCC supports the importance of exercises, tests, and drills as an effective practice to strengthen CIRR. We also agree that internal and external stakeholders should be engaged as part of these tests. However, in addition to these important points, we believe it is important for financial institutions to consider the timing of an incident as an input to these exercises. Time of day, day of week, week of month, month of year can significantly alter an organization's response. By exercising scenarios with differing assumptions around time, financial institutions can understand how their response may be altered based on the product, market, and other economic factors. The key to all cyber incident response and recovery strategies is the ability to restore services in a rapid but safe manner in the face of a material operational event. The ability to simulate these events and work through organizational and Sector responses increases the muscle memory for response and decreases the operational friction when an incident occurs. It is important that developed scenarios closely resemble the operational environment that may exist during an incident. Accordingly, DTCC recommends that this practice include the information discussed above regarding the importance of including timing inputs when exercising scenarios.

L. Additional Cyber Incident Response and Recovery Practices

While DTCC believes that the CIRR toolkit offers a robust set of practices, DTCC recommends the addition of a practice specific to Hybrid Testing. A financial institution could improve the benefits it receives from exercises and drills by integrating these activities into a single simulated event. Such an event could be in the form of a tabletop exercise of a simulated disaster scenario with the activation of a crisis management team. It could also include forced absenteeism (i.e., a condition where key personnel are not allowed to participate in the exercise). Because these exercises can more closely simulate a real event, they can better prepare secondary and tertiary resources for crisis situations and decrease operational friction when a real incident occurs.

* * *

We appreciate this opportunity to comment on the Consultation and your consideration of the views expressed in this letter. Many of these matters are complex, and we would welcome the opportunity to discuss the CIRR Toolkit and our comments. If you have any questions or need further information, please contact me at sscharf@dtcc.com.

Sincerely,

Stephen Scharf
Managing Director &
Global Chief Security Officer