July 20, 2020

Via Electronic Mail

Ms. Grace Sone
Member of FSB Secretariat
Bank of International Settlements

Re: Comments in Support of FSB consultative document: *Effective Practices for Cyber Incident Response and Recovery*

Dear Ms. Sone:

The Bank Policy Institute ("BPI"), through its technology policy division known as BITS, together with the American Bankers Association ("ABA") (collectively, "the Associations")[1], appreciates the opportunity to comment in support of the Financial Stability Board ("FSB") Consultative Document, "*Effective Practices for Cyber Incident Response and Recovery*" ("CIRR Toolkit").[2] The Associations would also like to thank the FSB for including member firms in an ongoing exchange of views as a part of FSB global outreach meetings with industry stakeholders.

Cyber-attacks targeting the global financial system and its institutions are prevalent and persistent, and financial institutions are expending considerable bandwidth and resources to address the risks that these threats may bring to bear on the global financial system. Upon incident detection, institutions must respond, mitigate, and resolve the incident while also moving rapidly to restore capabilities and services that will provide market confidence in the individual institution and market stability to the broader financial system.

The Associations commend the FSB for collaborating with other standards-setting bodies, regulators, and the private sector to publish the FSB CIRR toolkit. The CIRR toolkit features 46 cyber incident response and recovery practices spread across seven groupings: governance, preparation, analysis, mitigation, restoration, improvement, and coordination and communication. This flexibility permits the ongoing development of common best practices for an institution or industry sector without creating new and prescriptive regulatory obligations for financial institutions of every size and maturity.

[1] See Annex A for a description of the Associations

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

Writing in general support of the goals and intentions underlying the FSB toolkit, the Associations:

1. Affirm on the industry position that objective-based principles reflecting accepted international cybersecurity standards encourage flexibility of response and enable a more resilient and responsive financial services sector;
2. Emphasize that within industry it is common to deploy NIST in parallel with ISO as complementary frameworks in conjunction with other standards, as governed by a firm's resources, preferences, and needs;
3. Encourage the recognition and acceptance of private sector approaches to cybersecurity and resiliency, including the Financial Services Cybersecurity Profile assessment tool, collaborative data vaulting of Sheltered Harbor, and enhanced domain security embodied in the acquisition and management of the .bank and .insurance domains as an anti-phishing and security measure;
4. Confirm the ongoing need for regulatory coordination as a foundational element of global supervision.

The CIRR toolkit offers institutions across the cyber incident maturity spectrum a suite of options to consider in evaluating effective response and recovery approaches. While it is flexible enough to enhance cyber resilience for any financial institution operating characteristics, it is critical to emphasize that the CIRR Toolkit "does not constitute standards for organisations or their supervisors and is not a prescriptive recommendation for any particular approach."[3] Additionally, while mature institutions have substantially implemented these response and recovery practices, other firms have not or do not have the in-house capability to holistically deploy them. Accordingly, regardless of a financial institution's operating characteristics, it can make use of the CIRR toolkit without fearing that a lack of engagement on one or more enumerated practices could result in a determination of deficiency of performance.

An institution that does not presently utilize the full suite of practices contemplated within the CIRR toolkit may encounter more complex threats as it grows. Therefore, to be maximally useful it is important for incident response and recovery guidance like the CIRR Toolkit to enable an institution to understand its growth as it relates to its corresponding risk profile. In pursuit of responsive and resilient cyber regulatory coordination, the Associations, in collaboration with the recently formed Cyber Risk Institute ("CRI"), have partnered with the global supervisory community and multinational industry stakeholders to develop an industry-led Financial Sector Profile ("the Profile"). The Profile is a compliance convergence instrument modeled on accepted global frameworks such as to offer a common approach to the development of a cybersecurity program. Specifically, the Profile uses a common vocabulary and taxonomy that enables supervisors/regulators and industry to communicate with each other to establish a universal understanding of a financial institution's cybersecurity posture. It also helps regulators and firms to prioritize resources and focus on cyber risks of greatest concern.

[3] Id.at 2.

While many sectors, including the financial sector, continue to use both the ISO ("International Organization for Standards") 27000 series and the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("NIST CSF") in conjunction with each other, the Profile empowers financial institutions by going a step further to set forth a cybersecurity framework that is specific to the needs and regulations of the financial sector and based off of global industry best practices including: ISO 27000, NIST CSF, CPMI IOSCO's cyber resilience guidance for FMIs, COBIT, and others. Indeed, IOSCO's "*Cyber Task Force June 2019 Final Report*"[4] points to the Profile as a prime example of a sector-specific cybersecurity framework that can pull from global best practices to create a framework that addresses sector-specific needs.

Because of the substantial industry cooperation in developing the Profile, the FSB should evaluate the possibility of more directly incorporating the Profile into its existing efforts or integrating it as a companion tool to enhance the goals of the CIRR toolkit. The Associations would also like to emphasize that in contemplating existing international standards, the industry commonly deploys both ISO and NIST standards concurrently and does not view them as in conflict or competing approaches in need of resolution. ISO and NIST recently engaged international partners in an open, transparent, and collaborative standards development process to develop ISO/IEC 27101, a technical specification on guidance for developing cybersecurity frameworks that leverages the content and approach of the NIST Cybersecurity Framework. Moreover, the NIST standard maps its higher-level framework to ISO 27000, allowing firms to enjoy the technical control focus of NIST with the ISO's risk-driven dimension.

In further seeking cyber regulatory coordination, the Associations suggest that FSB acknowledge that the global financial sector commonly organizes its recovery and response efforts utilizing a substantially similar and preexisting taxonomy to the CIRR toolkit's seven components.[5] The CIRR toolkit strays from the industry organization by replacing the word "planning" with "preparation," and adds a "restoration" category between "mitigation" and "improvement.". While the differences may appear trivial, the incremental deviation from, or addition to existing industry-adopted lexicon can deteriorate into regulatory fragmentation and burden on firms. We urge the FSB to ensure that its groupings are coordinated with existing industry lexicon.

In closing, the Associations look forward to continuing to engage on the important operational resilience considerations highlighted by the CIRR toolkit. As a guiding consultative document with global impact, it is critical that the CIRR toolkit ensures maximum flexibility and coordination in the least-prescriptive manner possible. As it progresses toward publication to the G20 and beyond, the toolkit should incentivize institutions across the maturity spectrum to formulate an agnostic incident response plan that builds out enduring resiliency capacity and capability. With

[4] OICV-IOSCO Cyber Task Force Final Report FR09/2019, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf

[5] Existing industry guidance contemplates the six groupings: governance, planning, analysis, mitigation, improvement, and coordination and communication while the FSB CIRR toolkit employs seven: governance, preparation, analysis, mitigation, restoration, improvement, coordination and communication.

that goal in mind, we support these continued efforts to coordinate standards and expectations to appropriately stabilize and secure the financial system.

Thank you for the opportunity to partner in this endeavor. If you have any questions please contact Brian Anderson, Senior Vice President, Regulatory Technology, BPI/BITS at brian.anderson@bpi.com or (202) 289-4322; or Denyette DePierro, Vice President & Senior Counsel, Cybersecurity and Digital Risk, Office of Advocacy and Innovation, American Bankers Association at ddepierr@aba.com or (202) 663-5333.

Respectfully submitted,

Christopher Feeney
EVP and President, BITS
Bank Policy Institute

Denyette DePierro
VP & Senior Counsel,
Cybersecurity and Digital Risk
Office of Advocacy and Innovation
American Bankers Association

cc: Mr. Ong Chong Tee
Deputy Managing Director for Financial Supervision
Chair of the FSB CIRR Working Group
Monetary Authority of Singapore

Ms. Nida Davis
Associate Director, Division of Supervision and Regulation
Co-Lead of the FSB CIRR Working Group
Federal Reserve Board

Mr. Giuseppe Siani
Deputy Director General, Macroprudential Supervision IV
Co-Lead of the FSB CIRR Working Group
European Central Bank

Annex A

The Bank Policy Institute (BPI) is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks. Its members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ nearly 2 million Americans, make 68% of all loans and nearly half of the nation's small business loans and serve as an engine for financial innovation and economic growth. The Business-Innovation-Technology-Security division (BITS) of BPI brings BPI's banks and other affiliate members together in an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud and improve cybersecurity and risk management practices for the nation's financial sector. For more information on BPI and BITS, visit http://www.bpi.com.

The American Bankers Association is the voice of the nation's $20.3 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $15.8 trillion in deposits and extend nearly $11 trillion in loans. For more information, visit http://www.aba.com.