February 15, 2019

Via electronic submission to: maromero@naic.org

Miguel Romero
National Association of Insurance Commissioners
1100 Walnut, Suite 1500
Kansas City, MO 64106

Mr. Miguel Romero:

The American Bankers Association (ABA)[1], Bank Policy Institute (BPI) – BITS[2], Futures Industry Association (FIA)[3], Institute of International Bankers (IIB)[4], Institute of International Finance (IIF)[5] (hereafter the "Associations"), appreciate the opportunity to provide comments in response to the December 10, 2018 email solicitation to the National Association of Insurance Commissioner's IT Examination Working Group stakeholders. In the solicitation, the NAIC notes BPI-BITS leadership in the development of the Financial Services Sector Cybersecurity Profile and asks the following three questions:

- ***What is your view of the best way the Assessment Tool should be incorporated into the financial exam regulatory review?***
- ***For insurers and trade groups, will your organizations be considering use of the tool?***

[1] The ABA is the voice of the nation's $17 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $13 trillion in deposits and extend nearly $10 trillion in loans. Learn more at www.aba.com.

[2] BPI is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks. Our 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 72% 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 (better known as BITS), is a division of BPI that brings BPI members and BITS affiliate members, such as insurers, asset managers, sector utilities, etc., 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, visit http://www.bpi.com and https://bpi.com/category/bits/.

[3] FIA is the leading global trade organization for the futures, options and centrally cleared derivatives markets, with offices in Brussels, London, Singapore and Washington, D.C. FIA's membership includes clearing firms, exchanges, clearinghouses, trading firms and commodities specialists from more than 48 countries as well as technology vendors, lawyers and other professionals serving the industry. FIA's mission is to support open, transparent and competitive markets, protect and enhance the integrity of the financial system, and promote high standards of professional conduct. As the principal members of derivatives clearinghouses worldwide, FIA's member firms play a critical role in the reduction of systemic risk in global financial markets. Learn more at www.fia.org.

[4] The IIB is the only national association devoted exclusively to representing and advancing the interests of internationally headquartered banking organizations operating in the United States. The IIB's membership consists of approximately 90 banking and financial institutions from over 35 countries. In the aggregate, IIB members' U.S. operations have approximately $5 trillion in U.S. banking and non-banking assets, and provide approximately 25 percent of all commercial and industrial bank loans made in this country. Collectively, the U.S. branches and other operations of IIB member institutions enhance the depth and liquidity of the U.S. financial markets and are an important source of liquidity in those markets, including for domestic borrowers. Learn more at www.iib.org.

[5] The Institute of International Finance is the global association of the financial industry, with close to 450 members from more than 70 countries. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, sovereign wealth funds, hedge funds, central banks and development banks. Learn more at www.iif.com.

- ***As draft guidance is developed, are there any specific items that you wish for the Drafting Group to consider?***

In addition to responding to these three questions, the Associations will describe the reason for the Profile's development as well as how it was developed by the larger FSSCC with participation of its member trade associations and over 150 financial institutions.

The Rationale for the Profile's Development and the FSSCC's Profile Development Process

In 2016, the FSSCC in collaboration with the FS-ISAC surveyed member firms about the percentage of time their teams were spending on cybersecurity compliance activity. The results were remarkable: Chief Information Security Officers for financial services institutions reported that up to 40% of their time was spent on the compliance requirements of various regulatory frameworks, not cybersecurity. This finding, coupled with the well-documented shortage of available cybersecurity professionals, led the FSSCC to develop a solution – the Profile – that supervisory agencies could use for enhanced visibility across institutions, subsectors, and third parties to better identify, analyze and mitigate cybersecurity risk and that financial institutions could use to refocus their cybersecurity experts' time on protecting financial platforms.

To achieve these objectives, the FSSCC organized the Profile based on widely used frameworks and standards, as well as supervisory guidance and assessment tools, such as the NIST Cybersecurity Framework, the ISO/IEC 27001/2 controls, the NAIC Insurance Data Security Model Law, the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT), among others. This principle of leveraging what existed – and not "starting from scratch" – extended into the creation of the Impact Tiering scaling methodology, with the use of existing criteria for financial sector criticality. It also extended to the formulation of the diagnostic statements, which reference current supervisory expectations. If assessment language existed that did not overlap or have redundant phrasing, that language was used. However, where supervisory agencies used similar, overlapping, or duplicative language or phrasing, the simplest or most ubiquitous language was selected for the Profile.

In late 2016, the work began. Over the course of two years, the FSSCC held in excess of 50 working sessions, with over 150 financial institutions and trade associations and 300 subject matter experts participating. There was broad representation both by subsector (e.g., insurance, banking, asset management, market utilities, broker-dealers) and functional role (e.g., Board Directors, CEOs, CISOs, Chief Information Risk Officers, cyber and privacy attorneys).

Further input was solicited, received, and integrated from a myriad of U.S. and international financial services regulatory bodies. In April 2018, NIST hosted an open workshop to further develop a scaling methodology for the Profile. Over 100 individuals attended the workshop, with representation from financial services institutions and the state and national supervisory community.

From these sessions, the inputs, feedback, and recommendations provided were reviewed, discussed, and incorporated based on consensus. The result was release of the Profile, Version 1.0, on October 25th. The Profile and associated content can be found by visiting the following FSSCC webpages:

- https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile
- https://www.fsscc.org/The-Profile-FAQs

At the release event, the Federal Reserve Board of Governors, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Securities and Exchange Commission, and NIST all made statements of support. In a letter to the FSSCC, NIST stated that the Profile was "supportive of a risk-based approach to cybersecurity, and [] one of the more detailed Cybersecurity Framework-based, sector regulatory harmonization approaches to-date."[6]

It is with this history and context that we offer the following responses.

- ***What is your view of the best way the Assessment Tool should be incorporated into the financial exam regulatory review?***

The Profile was designed to be voluntarily adopted by firms seeking to optimize their examination processes. Before completing the Profile, firms electing to use it would first notify their supervisory agencies that they intend to use it as their preferred, singular assessment for regulatory review (rather than using numerous bespoke self-assessments), thereby reducing the number of topically overlapping compliance questionnaires and questions. During this conversation, firms would also discuss with their supervisor or supervisors the appropriate impact tier and corresponding diagnostics expected for completion that particular examination review cycle. If the supervisor or supervisors disagree with a firm's self-assessed impact tier, they are free to require the firm to select a particular impact tier and corresponding set of questions. The use of the Profile in no way abridges a supervisor's authority, and use of the Profile does not limit what a supervisor can review or require.

In short, if firms elect to use the Profile in lieu of other assessments, it enables financial institutions to confidently produce baseline evidence for review using a standardized classification structure and taxonomy and allows for quicker responses to iterative, follow-up questions from the supervisor. It benefits the firm and supervisor alike by producing a more efficient and consistent examination process thereby creating more time for firm security and supervisory analysis.

Accordingly, the Associations request that the NAIC support the Profile's use as an acceptable cybersecurity assessment to satisfy such self-assessment requirements.

- ***For insurers and trade groups, will your organizations be considering use of the tool?***

The Associations are fully supportive of the Profile's voluntary use as cybersecurity assessment. This month, the FSSCC facilitated an "implementers workshop," wherein firms that were considering use could learn from other firms that were using the Profile as their cybersecurity assessment. Financial institutions providing insurance products and services considering use of the FSSCC Cybersecurity Profile as an assessment include, but are not limited to:

- BB&T Corp (distributing insurance products and providing insurance services through BB&T Insurance Holdings)
- Nationwide
- New York Life
- Prudential

[6] See: https://www.fsscc.org/files/galleries/NIST_Letter_of_Support_re_FSSCC_Financial_Services_Sector_Cybersecurity_Profile.pdf

- State Farm
- USAA

- ***As draft guidance is developed, are there any specific items that you wish for the Drafting Group to consider?***

Specific items that the Drafting Group might consider include –

- Stating that the Profile is an acceptable form of assessment to satisfy cybersecurity self-assessment,
- Stating that firms can choose to use it among other acceptable forms of self-assessment, and
- Stating that it was developed by broadly representative group of financial institutions and subject matter experts under the auspices of the FSSCC.

The Associations also request that current and future guidance, examination expectations, questionnaires, etc., be mapped to and expressed in the Profile's organizational structure and taxonomy; we are not asking for reduced regulatory expectations, but a consistent approach to future issuances (and the examination process).

Thank you for this opportunity to provide comment,

American Bankers Association (ABA)
Bank Policy Institute (BPI) – BITS
Futures Industry Association (FIA)
Institute of International Bankers (IIB)
Institute of International Finance (IIF)