Summary of Comments Received

General Description:

The comments received were compiled from January to April - prior to the work performed by the Drafting Group. These comments were primary drivers of the Drafting Group's initiatives and goals in creating the edit suggestions for the IT guidance in the Exam Handbook. Interested parties requested that the work of the group not result in the creation of any new mandatory requirements for IT examiners.

Appendix Table of Contents:

Hello Miguel;

Hope you are doing well.

Below is the Tennessee DOI response to your inquiry:

We have reviewed this and it seems like a useful tool our companies could be using to ensure they're on the right track with regard to establishing and maintaining an effective cybersecurity program based upon NIST Cybersecurity Framework and ISO 27001 guidance.

We could see this being used to augment the IT examination process in order to provide a more comprehensive review of cybersecurity initiatives. It appears it would provide useful information about a Company's controls related to information security. It would be most useful as a self-assessment that our larger insurers or insurers dealing with PHI complete on a regular basis, but it could still be something that we have them complete in conjunction with the ITPQ as part of an overall assessment of their information systems.

We don't have any specific suggestions for the Drafting Group, but we do think that using this to enhance the IT examination process could be beneficial.

Thanks,

Jay

Jay Uselton | Insurance Examiner, CFE, EIC
Tennessee Department of Commerce and Insurance
500 James Robertson Parkway
Nashville, TN 37243-1135
(615) 741-0123
jay.uselton@tn.gov

Kate Kiernan
Vice President & Chief Counsel, Insurance Regulation

February 4, 2019

Chief Examiner Pat McNaughton, Chair
IT Examination (E) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106
Via email: maromero@naic.org

Re: Comments – Use of Bank Policy Institute (BPI) Cybersecurity Assessment Tool

Dear Mr. McNaughton:

Thank you very much for the opportunity to provide preliminary comments on the use of the Bank Policy Institute (BPI) Cybersecurity Assessment Tool in regulatory and compliance reviews. We appreciate the work that the NAIC IT Examination (E) Working Group is doing to develop handbook guidance on appropriate use of the assessment tool.

A number of our member companies support the use of the tool, while others are still examining how it will comport with their systems. The majority believe that the use of the tool should be voluntary and, if it is incorporated into the handbook, that guidance is provided to ensure that it does not become required by default. Below are comments based upon the questions posed by the Working Group:

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

   The NAIC Data Security Model law acknowledged and provided for differing security programs based upon a licensee's risk assessment. While perhaps not one-size fits all, the tool can be one device for facilitating the discussion between regulators and licensees.

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

   Some, but not all, ACLI members have said that they will be considering use of the tool.

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

   Not at this time though we look forward to engaging with the Working Group as efforts on development of the guidance progresses.

Sincerely,

Kate Kiernan

Kate Kiernan

American Council of Life Insurers
101 Constitution Avenue, NW, Washington, DC 20001-2133
(202) 624-2463 t katekiernan@acli.com
www.acli.com

January 21, 2019

Chief Examiner Pat McNaughton, Chair
IT Examination (E) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106

Attn: **Miguel Romero**
Via e-mail: **MRomero@naic.org**

Re: **Use of FSSCC Cyber Assessment Tool**

Dear Mr. McNaughton:

America's Health Insurance Plans appreciates this opportunity to offer comments in response to the questions on the proposal to incorporate the Financial Services Sector Coordinating Council Cyber Assessment Tool into the *Examiners Handbook* to be used by examiners as part of the IT examination processes.

As requested to assist the Drafting Group in developing initial guidance, we offer the following answers:

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

  AHIP believes the Assessment Tool is best used as a reference for examiners, and that the use of the tool be a strictly voluntary decision by companies. In early information gathering, examiners might ask if the subject company uses the tool, and if so, the examiner can follow the tool's framework as a guide. However, we would caution against the use of the tool to develop a simple checklist, since each company's Information Security Program will be based on the company's risk assessment, and commensurate with the size and complexity of the company, the nature and scope of its activities, and the sensitivity of the Nonpublic information it uses.

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

  Although we support the NAIC's efforts to locate effective tools to assist companies in their cybersecurity efforts, nearly all of AHIP's members must comply with the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH). Tools for self-assessment are available for such HIPAA plans, and they appear to more directly correlate with HIPAA's requirements than the FSSCC Tool. So, it isn't likely that many AHIP member companies would find the FSSCC Tool particularly helpful.

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

  It is AHIP's understanding that this tool is to be included in the *Examiners Handbook* as a purely voluntary measure companies may choose to use to enhance and maintain their own cybersecurity efforts. Although as stated above, AHIP members are unlikely to use the FSSCC Tool, AHIP believes the NAIC's consideration of tools which may be helpful to Industry is definitely preferred over, for example, new prescriptive requirements or standards which may overlap or conflict with the massive volume of existing laws and regulations and which would do little to provide additional assistance to companies' efforts to protect consumer information.

We thank you, the Drafting Group, and the IT Exam (E) Working Group members for your consideration of our comments, and we look forward to discussing them further with you at your convenience.

Sincerely yours,

Bob Ridgeway
Bridgeway@AHIP.org
501-333-2621

American Property Casualty
Insurance Association

January 25, 2019

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

VIA EMAIL: maromero@naic.org

RE: Financial Service Sector Coordinating Council (FSSCC) Cybersecurity Assessment Tool

Dear Mr. Romero:

The American Property Casualty Insurance Association (APCIA)[1] appreciates the opportunity to comment on the incorporation of the FSSCC's voluntary cybersecurity assessment tool (assessment tool) into the financial exam regulatory guidance. APCIA strongly supports the need for uniformity and consistency in data security standards and the examination of such measures. Such an approach fosters corporate resiliency through efficient and risk-based reviews.

FSSCC and the Bank Policy Institute (BPI)'s Frequently Asked Questions note that the assessment tool is a "mechanism to evidence compliance with various regulatory frameworks both within the United States and globally." To the extent a company has voluntarily utilized the assessment tool to determine compliance with U.S. and global regulations, it would be beneficial for insurance examiners to have guidance on how to acknowledge and utilize this comprehensive self-assessment in the IT examination process. Therefore, we support the NAIC moving forward with draft guidance and recommend that the key elements of any guidance should highlight the use of the cyber assessment is voluntary, risk-based and scalable.

Thank you for the opportunity to provide feedback and we look forward to working with you on this matter.

Respectfully,

Angela Gleason Alex Hageli

[1] Representing nearly 60 percent of the U.S. property casualty insurance market, APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA members represent all sizes, structures, and regions, which protect families, communities, and businesses in the U.S. and across the globe.

The Cypress Group

March 8, 2019

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

Re: National Association of Insurance Commissioners' Request for Comment on Developing Guidance in Incorporating Cybersecurity Assessment Tool into its Regulatory Review.

Dear Mr. Romero,

I write on behalf of The Insurance Coalition, a group of insurance companies that share a common interest in federal regulations that impact insurance companies. In this case, I am writing in response to your request for comment on the Financial Services Sector Cybersecurity Profile (the Profile).[1] The Profile was developed by the Financial Services Sector Coordinating Council (FSSCC) in cooperation with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and various industry groups and companies. We support the development of a tool to help companies complete self-assessments, and we believe that the Profile is a good tool under development. Furthermore, we emphasize the importance of harmonization in developing any tool to help companies complete self-assessments.

I. We support the development of a tool to help companies complete effective self-assessments, and we believe the Profile is a good tool under development.

Financial institutions can voluntarily adopt the Profile. Before completing the Profile, an institution will have to notify its supervisory agency of its intention to use the Profile as its preferred, singular assessment for regulatory review. This will reduce the number of topically

[1]The Profile provides a framework that integrates widely used standards and supervisory expectations to help guide financial institutions in developing and maintaining cybersecurity risk management programs. The Profile is the result of collaboration among financial institutions, trade groups, and government agencies. The Profile was spearheaded by FSSCC, the American Bankers Association, Bank Policy Institute's technology policy subdivision BITS, Futures Industry Association, Global Financial Markets Association (and its member associations of the Association for Financial Markets in Europe, the Asia Securities Industry & Financial Markets Association, and the Securities Industry and Financial Markets Association), and the Institute of International Bankers.

.

overlapping compliance questionnaires and questions. The institution will also have to discuss with its supervisory agency the appropriate impact tier and corresponding diagnostics expected for the particular examination review cycle. The agency can require the institution to select a particular impact tier and corresponding set of questions if the agency disagrees with the institution's self-assessed tier. The Profile will not reduce an agency's supervisory authority, nor will it limit the scope of an agency's review or requirements.

The Profile will enable insurers that elect to use it to confidently produce baseline evidence for review. The Profile implements a standardized classification structure and taxonomy that allows for timely responses to follow-up questions from the supervisor. The Profile benefits institutions and supervisory agencies by creating a more efficient and consistent examination process, which enhances security and supervisory analysis.

We support the development of a cybersecurity assessment tool that will help companies effectively complete self-assessments. All of the reasons mentioned support that the Profile is an effective tool under development, and we believe it represents a good start in the process of developing a tool to help companies complete self-assessments.

II. Regulatory harmonization regarding approaches to consumer privacy and cybersecurity assessment tools is critical.

We believe that any tool developed should harmonize approaches to consumer privacy across federal and state jurisdictions through a national standard. Regulatory harmonization eliminates fragmentation and avoids creating a patchwork of different standards. While the state-based insurance regulatory regime is effective, harmonization is essential in the context of a cybersecurity assessment tool. A harmonized tool would ensure consistent privacy protections and avoid a state-by-state approach to consumer privacy regulation. Regulatory harmonization based on existing knowledge, standards and frameworks eliminates fragmentation and maximizes consistency in approach domestically and abroad by avoiding the creation of a patchwork of different standards. Failure to harmonize could result in multiple, conflicting standards. This would ultimately undermine the goal of implementing a tool to better protect consumer data and could result in unnecessary industry confusion.

III. Conclusion

We support the development of a cybersecurity assessment tool that will better enable companies to efficiently and effectively complete self-assessments. Furthermore, we believe the Profile is an effective tool under development. Finally, we emphasize the importance of

regulatory harmonization in developing a cybersecurity self-assessment tool. We appreciate the opportunity to comment and look forward to continued dialogue.

Sincerely,

Bridget Hagan
Executive Director, The Insurance Coalition

March 1, 2019

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

Submitted electronically to maromero@naic.org

Mr. Miguel Romero:

The Financial Services Sector Coordinating Council (FSSCC)[i] welcomes the opportunity to provide additional insight into the development of the Financial Services Sector Cybersecurity Profile ("Cybersecurity Profile").

The FSSCC focuses on strengthening the resiliency of the financial services sectors, and we are encouraged by the NAIC's inquiry into the origination of the Cybersecurity Profile. The FSSCC developed the Cybersecurity Profile to provide a single tool for based on the widely-used frameworks and standards, as well as supervisory guidance and assessment tools (e.g., NIST Cybersecurity Framework, the NAIC Insurance Data Security Model Law).

The development of the Cybersecurity Profile work extended over two years, beginning in late 2016, with numerous conversations and working sessions with financial institutions, trade associations, and subject matter experts. Participants included a broad representation both by subsector and functional role (e.g., Board Directors, CEOs, CISOs, Chief Information Risk Officers, cyber and privacy attorneys).

The Profile was designed as another "tool in the toolbox" for financial institutions to use as part of their own risk management approach to cybersecurity. It is not intended to be used as a requirement for any institution or subsector, as the FSSCC and its members encourage institutions to develop implement and develop controls based on their own risk.

Thank you for the opportunity to provide comment to the NAIC's IT Examination Working Group. We look forward to continuing to work with you and the broader financial sector on this important issue. If helpful, FSSCC members would be happy to provide more insight into the conversations that led to the Cybersecurity Profile's development and the lessons learned.

Sincerely,

Craig Froelich
Chair, Financial Services Sector Coordinating Council

[i] **About FSSCC:** Formed in 2002 as a public/private partnership with the support of the U.S. Department of Treasury, FSSCC collaborates with the Treasury and the financial regulatory agencies at the federal and state levels through the Financial and Banking Information Infrastructure Committee, which also formed in 2002 under Treasury's leadership. FSSCC members include 72 of the largest financial institutions and their industry associations representing banking, insurance, credit card networks, credit unions, exchanges, and financial utilities in payments, clearing and settlement.

Hi Miguel,

These are my immediate thoughts on the tool based upon the requested feedback criteria. Please let me know if you have any questions.

To assist the Drafting Group in developing initial guidance, we are asking comments be provided on the following matters:

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

I also perform IT and cybersecurity reviews for banks and have seen this tool used by banks as well as (only a few mid-sized) insurance companies. As far as the best way to be incorporated into the financial exam regulatory review, I definitely think the process here is much more detailed than the current CObIT-based assessment tool that is used within Exhibit C and therefore, the testing under this Assessment Tool would be much more detailed and most likely extend the timing and extent of IT reviews.

Under current threat-based scenarios related to data breaches and the unknown number of breaches that most likely go undetected, adoption of this Assessment Tool would be beneficial to NAIC reviews. However, steps to be more efficient would have to be implemented to offset the time associated with those additional steps. As far as implementing theTool is concerned, I would think it would be best to take a risk-based approach by requiring some (high level) inherent risk areas be fully assessed, while others areas be tested to a lesser degree after initial (high) inherent risks are fully assessed and compensating controls considered. It would be similar to the overall risk-based approach now, but some areas of consideration would be "mandated/required" (high), while others would be "optional" (moderate, low) depending on the residual risk after the initial assessment.

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

N/A

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

Although the following items are mentioned in some parts of the assessment tool, I don't see much information on patching, version control of databases/software/operating systems and firmware updates within the Tool. These items should be given a higher priority as well as overall attention be given more to the development process as change/configuration management has a larger impact on breach risk than what is reflected in the overall Assessment Tool.

Thanks,

Dave Gordon, MBA, CISA, CFE (Fraud), CIA, CDFE
INS Services, Inc.
330-606-6445

From: Uso Sayers
To: Romero, Miguel
Subject: Comments: IT Examination (E) Working Group - Request for Comment
Date: Monday, January 21, 2019 9:31:48 PM

Hello Miguel,

The Cybersecurity Assessment Tool looks to be a great addition to the IT Review resources. Below are some questions/comments regarding the tool.

1. How will this affect the states that modify the Dodel security law? Will the tool be modified based on each state's Model Security Law?
2. When executing an IT review, would we be only looking at the NAIC lines in the diagnostic statements of the tool?
3. It may be helpful to incorporate the diagnostic questions from the tool into the ITPQ.
4. What will be the plan for companies who do not complete the assessment via the tool? Will examiners be expected to complete the tool?

I look forward to hearing the updates on the next IT Working Group call.

Thanks!
Uso

Uso Sayers, CISA

Johnson Lambert LLP

Principal

7000 Central Parkway | Suite 1500 | Atlanta, GA 30331

USayers@johnsonlambert.com | p: 678-894-4271 | c: 646-235-4448

On Thu, Jan 17, 2019 at 2:02 PM Romero, Miguel <MARomero@naic.org> wrote:

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)

NAMIC®
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | [F] 317.879.8408
3601 Vincennes Road, Indianapolis, Indiana 46268

202.628.1558 | [F] 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

February 18, 2019

NAIC IT Examination Working Group
c/o via electronic submission to: maromero@naic.org
National Association of Insurance Commissioners
1100 Walnut, Suite 1500
Kansas City, MO 64106

Dear Working Group Chair, Working Group Members, and Interested Regulators,

The National Association of Mutual Insurance Companies (NAMIC)[1] appreciates the opportunity to provide comments in response to the December 10, 2018 email solicitation of the National Association of Insurance Commissioner's IT Examination Working Group to interested parties. In the request, the NAIC discusses the development of the Financial Services Sector Cybersecurity Profile (Profile) by the Financial Services Sector Coordinating Council (FSSCC) 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?*
- *As draft guidance is developed, are there any specific items that you wish for the Drafting Group to consider?*

Any analysis of this inquiry starts with the root of the problem. A concern in the financial and insurance sectors includes a deficiency in the population of cybersecurity professionals. Additionally, compliance standards consume a large portion of assigned duties. Solutions exhibiting innovation and ingenuity must lead the way in combating this lack of qualified expertise and more effectively create efficiencies for those professionals.

The creation of the FSSCC Profile designed for regulatory agencies to use to enhance their visibility across institutions, subsectors, and third parties appears to be at the forefront of this concept. The Profile allows financial institutions including insurers to better identify, analyze, and mitigate cybersecurity risk. As a result, reallocation of the cybersecurity experts' time and focus to protecting appropriate platforms and addressing critical risks can be accomplished.

[1] NAMIC is the oldest property/casualty insurance trade association in the country, with more than 1,400-member companies representing 41 percent of the total market. NAMIC supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers. NAMIC member companies serve more than 170 million policyholders and write more than $253 billion in annual premiums. Our members account for 54 percent of homeowners, 43 percent of automobile, and 35 percent of the business insurance markets. Through our advocacy programs we promote public policy solutions that benefit NAMIC member companies and the policyholders they serve and foster greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

To effectuate these stated goals, the FSSCC arrived at the Profile based on widely used frameworks and standards, had numerous working sessions with financial and trade associations, discussed with hundreds of subject matter experts across all sectors including insurance, and sought out U.S. and international financial services regulatory bodies including NIST for consultation and guidance.

When the Profile was finally released, many U.S. governmental regulatory bodies and agencies including 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 made overtures of support. In a correspondence 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."[2]

Based upon this history, NAMIC would lend its support to this critical tool as its development continues to grow and be utilized in not only the financial realm but inclusion in the insurance sector as well. By way of more specific responses to your inquiry, NAMIC would posit the following.

- *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 utilized by entities in seeking to enhance their examination processes. Therefore, if an entity elects to use the Profile instead of other assessments, it enables insurers to expertly produce baseline evidentiary support for review using a standardized classification structure and allows for a timelier and more efficient response to exceptions from the regulator. A consistent platform that all parties can utilize is most desirable. Consequently, NAMIC would support the NAIC's adoption or recognition of the Profile's use as an acceptable cybersecurity self-assessment tool.

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

It is believed by NAMIC that a number of its members are reviewing and beginning to discuss utilization and implementation of the Profile into their organizational structures. Uptake and acceptance appear to be highly anticipatory and growing as evolution and knowledge of the Profile manifests itself.

- *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 –

- Adoption and/or recognition that the Profile is an acceptable form of assessment to satisfy cybersecurity self-assessment,

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

- While by no means necessary to make it exclusive, the Profile should be included in a menu of options for self-assessment in this regard, and
- Establish procedures and protocols if the Profile is accepted and utilized as a self-assessment tool option to avoid redundancy and unnecessary duplication in overall examination review, analysis, conduct and implementation.

In closing, NAMIC wishes to thank the NAIC IT Examination Working Group for its comprehensive inquiry of relevant solutions regarding Cybersecurity self-assessment and believes consideration of the Profile to be a value-add for all parties involved in these processes.

Best regards,

Andrew Pauley, CPCU
Government Affairs Counsel