September 21, 2015

Via Electronic Submission to prainfo@occ.treas.gov

Ms. Shaquita Merritt, OCC Clearance Officer
Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
Attention: 1557-0328
400 7th Street, NW, Suite 3E-218
Mail Stop 9W-11
Washington, D.C. 20219

RE: FFIEC Cybersecurity Assessment Tool

Dear Ms. Merritt:

The Financial Services Sector Coordinating Council ("FSSCC") appreciates the opportunity to provide comments in response to the Paperwork Reduction Act notice and request for comment, published in the Federal Register, Vol. 80, No. 140, on July 22, 2015, by the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA") (collectively, "the Agencies") with regard to the renewal of the information collection authored by the Federal Financial Institutions Examination Council ("FFIEC"), entitled the FFIEC *Cybersecurity Assessment Tool ("Assessment* or "*Assessment Tool*").

The FSSCC would like to thank the FFIEC and its member agencies for the time and effort that they have devoted to constructing the *Assessment*. Given the *Assessment's* detailed and comprehensive nature, it is clear that the FFIEC's objective is to improve the overall cybersecurity posture of the sector and the nation as whole.

On behalf of the financial services sector ("sector"), the FSSCC submits the attached letter.[1] The letter reflects the coordinated input from across the regulated financial institutions, the input from the sector trade associations representing their members, and the deep mutual commitment of the financial services sector to cybersecurity. The letter includes suggestions for consideration by both the FFIEC and the prudential regulators. As a sector, we share the

[1] Established in 2002 by the private sector, the FSSCC was created to coordinate critical infrastructure and homeland security activities in the financial services industry. The members of the FSSCC are listed in Appendix A. For the purposes of this letter, we consider small institutions as those $10B and below in assets, mid-sized institutions as $10B-$50B and large institutions as $50B and above.

objective of improving the security and resiliency of the nation's critical infrastructure from cyber-attacks and other adverse events and support methods and approaches to this end.

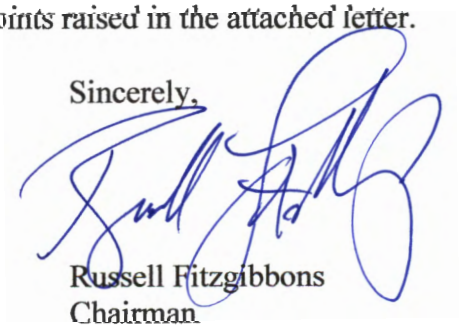
We appreciate the opportunity to provide comments, and would like for this letter to serve as a vehicle for future collaboration on the *Cybersecurity Assessment Tool* ("Assessment"). In the attached comments, we suggest that:

- FFIEC member agencies clarify and preserve the voluntary nature of the *Assessment*;
- The current *Assessment* be treated as an initial version – a Version 1.0 – and not as a finalized tool that examiners use as part of the formal examination process;
- During the next 12-18 months the FFIEC member agencies and the sector collaborate in a fashion similar to that which was employed to develop the National Institute of Standards and Technology ("NIST") *Cybersecurity Framework* in order to work through usage issues and refine a subsequent iteration – a Version 2.0;
- A collaboratively-developed Version 2.0 be more fully aligned with the NIST Cybersecurity Framework;
- A collaboratively-developed Version 2.0 align action and investment to address residual risk (following the deployment of compensating controls);
- A collaboratively-developed Version 2.0 be more objective-based in its assessment of maturity;
- A collaboratively developed Version 2.0 would better enable effective boardroom engagement; and,
- The FFIEC member agencies, other financial sector regulatory agencies, and the sector work together to synchronize initiatives and frameworks.

As such, the FSSCC and its member firms welcome an opportunity for an in-person meeting with the FFIEC and member agencies in order to initiate a dialogue.

In conclusion, we would like to reiterate our thanks to the FFIEC and its member agencies on its continued focus on cybersecurity. We would also like to thank the FFIEC for considering our comments. On behalf of FSSCC organizations, we look forward to an in-person meeting to further discuss the points raised in the attached letter.

Sincerely,



Russell Fitzgibbons
Chairman

Attachment

ATTACHMENT:

Detailed Comments on the FFIEC *Cybersecurity Assessment Tool*

I. Introduction and Executive Summary

As owners and operators of the world's financial infrastructure and as guardians of some of the most sensitive personal and corporate data, the financial services sector has recognized that in order to protect itself from fraudsters, hacktivists, criminal syndicates, and even nation states, cybersecurity collaboration is essential. In order to achieve the FFIEC's desired outcome of increased cybersecurity, appreciation for cyber risk, and engagement of senior executives and boards of directors in cyber risk oversight, the sector requests that the FFIEC treat its *Assessment* as, in effect, an initial version – a Version 1.0 – that will be collaboratively explored by individual sector institutions, the sector as a whole, and the FFIEC member agencies over the course of 12-18 months to further consider its utility and areas for refinement, rather than as a finalized tool that examiners use as part of the formal examination process. Such an approach has precedent and would allow for a consistent and sustainable implementation and would only lead to a more cyber secure sector, the ultimate goal of banking institutions and their regulators alike.

Comments with regard to the *Assessment* were invited on the following topics through a PRA Notice and Comment Federal Register solicitation, and our letter addresses each of these topics:

- PRA Topic 1: Whether the collection of information is necessary for the proper performance of the functions of the Agencies, including whether the information has practical utility;
- PRA Topic 2: The accuracy of the Agencies' estimate of the burden of the collection of information;
- PRA Topic 3: Ways to enhance the quality, utility, and clarity of the information to be collected;
- PRA Topic 4: Ways to minimize the burden of the collection on respondents, including through the use of automated collection techniques or other forms of information technology; and
- PRA Topic 5: Estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information.

As noted above, the sector requests the opportunity to collaborate alongside the FFIEC member agencies in considering one or more subsequent versions of the *Assessment* that aligns action and investment to residual risk.

The sector further urges the FFIEC to consider several "General Policy Principles for Improvement," including the preservation of the voluntary nature of the *Assessment* and using a transparent, collaborative, and iterative process for working with the sector to create an enhanced subsequent version. The sector also provides specific requests and recommendations in relation to the Inherent Risk Profile and Cybersecurity Maturity, including a request for more interpretive

guidance and a recommendation for a more risk-based and less binary approach to achieving cybersecurity maturity.

Additionally, the sector recommends that the FFIEC coordinate with non-FFIEC agencies and bodies that also have financial sector regulatory, oversight, and examination functions so as to reduce overall regulatory and examination burden, simplify compliance, and increase the effectiveness and management of cybersecurity activities.

II. A Response, in part, to PRA Topic 1: "Whether the collection of information is necessary for the proper performance of the functions of the Agencies, including whether the information has practical utility"

A. Overview of Current Cybersecurity Requirements

With the passage of the Gramm-Leach-Bliley Act in 1999 and the subsequent issuance of the *Interagency Guidelines Establishing Information Security Standards* ("Guidelines"), covered financial institutions from the smallest in asset size to the largest have been required to develop a "comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the [covered financial institution] and the nature and scope of its activities."[2] Under the Guidelines, such a program must assess and manage for risk and be overseen by the financial institution's board of directors. In particular, the board is expected to approve and oversee the information security program and receive annual reports of the program's status.[3] If there are changes in technology, the threat landscape, or if the financial institution is undergoing a merger, joint venture, etc., "adjustments" to the program may be required.[4] The FFIEC *IT Examination Handbook Booklets*, which were issued contemporaneously, further describe regulatory expectations regarding information security programs[5] and board and senior executive engagement,[6] among other things.[7]

---

[2] The *Interagency Guidelines Establishing Information Security Standards* were jointly issued by the Board, the FDIC, the OCC, and the Office of Thrift Supervision ("OTS"). This jointly issued guidance is promulgated under 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS). See also the *Gramm-Leach-Bliley Act*, 15 U.S.C. §§ 6801-6809.

[3] *Interagency Guidelines Establishing Information Security Standards*, Section III.

[4] Id. at Section III, Paragraph E.

[5] Federal Financial Institutions Examination Council. *IT Examination Handbook: Information Security*. July 2006. FFIEC InfoBase. Web. <http://ithandbook.ffiec.gov/it-booklets/information-security.aspx>.

[6] Federal Financial Institutions Examination Council. *IT Examination Handbook: Management*. June 2004. FFIEC InfoBase. Web. <http://ithandbook.ffiec.gov/it-booklets/management.aspx>.

[7] Federal Financial Institutions Examination Council. *FFIEC IT Examination HandBook InfoBase*. Web. <http://ithandbook.ffiec.gov/it-booklets.aspx>.

B. Sector Commitment to Cybersecurity

The financial services sector is unique amongst other sectors in relation to cybersecurity. Not only do the sector's institutions provide the financial infrastructure that underpins the world economy, but it also holds, and is entrusted with, the sensitive personal, financial, account, and corporate information of its customers. Correspondingly (and unlike other sectors), the financial services sector faces threats from the full panoply of bad actors, including nation states, organized crime syndicates, politically motivated attackers, fraudsters, and other criminals. As more information has become digitized, the financial services sector has responded with greater and greater cybersecurity oversight, management, controls, and, of course, expenditure. For example, U.S. Treasury Secretary Jacob "Jack" Lew noted one financial institution's annual cybersecurity expenditure of $250 million at a conference last year,[8] a number that is expected to double by 2020.[9] Other large financial institutions spend similarly.[10]

Smaller financial institutions have evidenced a similar commitment. After conducting a "cybersecurity sweep" of approximately 500 community financial institutions, the FFIEC issued its resulting *FFIEC Cybersecurity Assessment General Observations* in November 2014. In this document, the FFIEC noted that, in terms of cybersecurity, "most" of the community financial institutions that it examined "implement preventive controls to impede unauthorized access to their systems," "have tools in place, such as anti-virus and anti-malware tools, to detect previously identified attacks," and "have a process for implementing corrective controls to address previously identified vulnerabilities by installing patches on their primary IT system."[11]

Perhaps not surprisingly, the private sector institutions of the financial services sector are credited as being among the leaders in cybersecurity. However, as a sector, these institutions have also recognized that in today's interconnected world the financial services sector is not an "island unto itself"; we need and rely on entities that provide us with power, water, telecommunications, computing, etc. Correspondingly, when in February 2013, President Obama issued *Executive Order 13636, Improving Critical Infrastructure Cybersecurity,*[12] directing that NIST develop a cross-sectoral voluntary cybersecurity framework, the financial services sector was wholly supportive. From the outset, the sector as a whole through the FSSCC was significantly involved in the development of the NIST framework, collaborated and participated

---

[8] Lew, Jacob J. "2014 Delivering Alpha Conference Hosted by CNBC and Institutional Investor." U.S. Department of Treasury, 16 July 2014. Web. <http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx>.

[9] Son, Hugh. "Dimon Sees Cyber-Security Spending Doubling After Hack." Bloomberg, 10 Oct. 2014. Web. <http://www.bloomberg.com/news/articles/2014-10-10/dimon-sees-jpmorgan-doubling-250-million-cyber-security-budget>.

[10] Shriber, Todd. "JPMorgan's War on Hackers Bodes Well for Cybersecurity ETF." ETF Trends. 19 Feb. 2015. Web. <http://www.etftrends.com/2015/02/jpmorgans-war-on-hackers-bodes-well-for-cyber-security-etf/>.

[11] Federal Financial Institutions Examination Council. *FFIEC Cybersecurity Assessment General Observations*. 3 Nov. 2014. Web. <https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf>.

[12] Obama, Barack. *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*. The White House, 12 Feb. 2013. Web. <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

in all five NIST cybersecurity workshops, and submitted responses to the Federal Register requests for information, notwithstanding the fact that our independent financial services regulators were not bound by the President's Executive Order or the resulting NIST *Cybersecurity Framework*.[13]

Regarding the NIST *Cybersecurity Framework*, almost a year and a half after its publication, it is a document that has predominantly been embraced across all the various sectors, an unprecedented feat. The reason for such an embrace is manifold, but there are potentially two principal reasons: one, the document's effectiveness; and, two, the process by which it was created. Both will be discussed later in this submission.

With the release of the FFIEC *Cybersecurity Assessment Tool* on June 30, 2015, the financial services sector again worked together to assist individual institutions more uniformly utilize the tool. Under the auspices of the FSSCC, the sector established a focused working group with the mission of making the *Assessment* more user-friendly through Excel automation for all institutions, but particularly for the smaller institutions as they review the sheer number of *Assessment* questions.[14]

Similarly, with the Federal Register publication of the PRA notice and comment solicitation concerning the FFIEC *Cybersecurity Assessment Tool*, the sector established a FSSCC working group to review the *Assessment.* This group's focus was to provide a series of positive, constructive suggestions to improve the *Assessment* and better address the *Assessment's* stated goal of helping institutions "identify their risks," "assess their cybersecurity preparedness," and "inform their risk management strategies."[15]

C. Utility of Information Collected via the FFIEC Cybersecurity Assessment Tool

Although the FFIEC is soliciting comments under the *Paperwork Reduction Act* (44 U.S.C. §§3501-3521), the sector suggests that the FFIEC treat its *Assessment* not as a finalized tool for the purposes of immediate regulatory examination (and assessing perceived cybersecurity preparedness), but as an initial version – a Version 1.0 – that will be collaboratively explored by individual sector institutions, the sector as a whole, and the FFIEC member agencies over the course of 12-18 months for the purposes of future comment, revision, and refinement. A comparable process was utilized to great effect during the development of the NIST *Cybersecurity Framework*, a framework that was developed under a similar timeframe and

[13] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0.* 12 Feb. 2014. Web. <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

[14] There are 533 *Assessment* questions: 39 questions for the Inherent Risk Profile and 494 questions to ascertain an *Assessment* Maturity Level.

[15] Federal Financial Institutions Examination Council. "FFIEC Releases Cybersecurity Assessment Tool." 30 June 2015. Web. <http://www.ffiec.gov/press/pr063015.htm>.

that is both titled and envisioned as a "Version 1.0."[16] Additionally, this seems consistent with Comptroller of the Currency Thomas Curry's letter to the Government Accountability Office discussed below.

While the *Assessment's* "User's Guide" maintains that the *Assessment* is consistent with the FFIEC Information Technology Examination Handbook and NIST Cybersecurity Framework principles, only the "Baseline" maturity level "Declarative Statements" consist of codified expectations "required by law and regulations or recommended in supervisory guidance."[17] Such expectations represent only 123 of 494 declarative statements, or controls. By contrast, the NIST *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0,* consisted of 98 subcategories, or controls. Given the 60-day notice and comment period (and the 84 days since the *Assessment's* June 30th public release), the sector has not had enough time to fully consider the utility of the *Assessment*. Indeed, banking institutions have not yet had a chance to evaluate it in the light of even one planning and budget cycle. As such, in order to provide a more considered evaluation of the *Assessment* and recommendations for positive improvement of the *Assessment* for a Version 2.0, the sector requests that the FFIEC and its member agencies refrain from using the *Assessment* as a finalized examination or comparative tool, and, rather, allow for institutions' and regulators' co-exploration of the utility and benefits of the *Assessment* over the next 12-18 months.

As part of this process, and similar to the process used during the development of the foundational *Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness* (June 26, 2000 and February 1, 2001)[18] and *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (August 12, 2003 and March 29, 2005),[19] the sector also requests that the FFIEC and its member agencies provide multiple opportunities for full comment on "all aspects" of the *Assessment*. Such opportunities helped shape those guidelines, guidelines that 10-15 years after their issuance still remain effective and relevant. The sector believes that such comment opportunities in relation to this *Assessment* will make it possible to identify topics and issues that will only surface through further exploration. In turn, the utility of the *Assessment* would be discovered and the resulting commentary would help improve the *Assessment's* next iteration so that it demonstrably assists in advancing cybersecurity and with less overall friction, the ultimate goal for both banking institutions and the regulators that oversee their safety and soundness.

---

[16] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0*.

[17] Federal Financial Institutions Examination Council. *FFIEC Cybersecurity Assessment Tool User's Guide*. P. 7. 30 June 2015. Web. < https://www.ffiec.gov/cyberassessmenttool.htm >.

[18] Later, these guidelines were named the *Interagency Guidelines Establishing Information Security Standards* upon the issuance of the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (70 FR 15736). See FN 2 above.

[19] The *Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness* Federal Register notices can be found at 65 FR 39472 and 66 FR 8616. The *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* Federal Register notices can be found at 68 FR 47954 and 70 FR 15736.

III. A Response to PRA Topic 2: "The accuracy of the Agencies' estimate of the burden of the collection of information"; and PRA Topic 5: "Estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information"

A. Collection and Capital Efforts Estimate

While the FFIEC member agencies estimated in the Federal Register PRA solicitation that the average burden per response would be 80 hours per institution, sector consensus is that that estimate understates the actual effort. Institutions emphasize that while it may only take 10's of hours to provide non-supported *'Yes/No'* answers to the 533 *Assessment* questions, in order to provide answers that are supportable during the regular examination process with documentation and the other typical evidence requested by regulators, the burden for collecting information for the *Assessment* is much larger. Indeed, absent a few outliers, small, medium, and large banking institutions have expressed that the effort required to undertake and collect the information requested in the *Assessment*, validate their own responses with subject matter experts, report out the results to their respective steering committees, and prepare for examination will be a multiple of that number. For smaller institutions, they estimate that to complete the *Assessment* it will take hundreds of hours. For medium-sized institutions, they estimate that the man-hour efforts to fully collect information for the *Assessment* may near 1000-2000 hours. For the larger institutions, their estimates are in the 1000-2000 hour range and beyond.

To address these time requirements and the recent regulatory requests to complete the voluntary *Assessment* in advance of upcoming regulatory examinations, many institutions have indicated that they will be hiring additional full-time employees or repurposing current ones to assist in completing the *Assessment* and collecting the data required to support responses (see Section IV.A for a more detailed description of concerns regarding the *Assessment's* voluntary nature).

B. Effective Boardroom Engagement

It is clear with the parallel release of the *FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors* the FFIEC member agencies are appropriately focused on effective boardroom engagement with respect to cybersecurity risk. Sector institutions, however, are reporting that their boards are having difficulty reconciling this *Assessment* with the previous NIST *Cybersecurity Framework* efforts and activities. Indeed, institutions have invested a substantial amount of energy in educating their boards on the NIST *Cybersecurity Framework*, and, where appropriate, have adjusted reports, documents and other communications to align with it. Additionally, media coverage of the NIST *Cybersecurity Framework*, its endorsement by the National Association of Corporate Directors and the proliferation of outside materials and ongoing board educational sessions hosted by third-party audit firms have created a great deal of awareness and reinforcement of the Framework and its role in cross sector cyber resilience.

The *Assessment* essentially introduces a new framework and approach that requires re-education and careful positioning in order to coexist with the NIST *Cybersecurity Framework* at the board level. Further, many board members reside or have resided in other economic sectors relevant to NIST; at a board level, the issuance of the *Assessment* could inadvertently dilute cross-sector cooperation and information exchange. Accordingly, in furtherance of the collaborative nature we promote throughout this letter, we wish to discuss this important topic of boardroom education and effective engagement.

IV. A Response to PRA Topic 3: "Ways to enhance the quality, utility, and clarity of the information to be collected"

A. General Policy Principles for Improvement

Use of the *Assessment* is described as being voluntary, and the sector contends that it should remain so for the reasons that follow. A voluntary *Assessment* will assist institutions and regulators discover and realize its utility because, if voluntary, financial institutions will be able to provide undiluted feedback and engage in open dialogue with regulators concerning its strengths, weaknesses, and areas for improvement. As mentioned, this was the process used to great effect in developing the NIST *Cybersecurity Framework*, and that voluntary effort has achieved an unprecedented level of buy-in and efficacy.

Some institutions, however, are reporting that various regulators have stated that they would like for the *Assessment* to be completed in advance of examinations in October and November and even plan to use it as a point of comparison for regulatory purposes for subsequent examinations. Moreover, as often as the FFIEC asserts that *Assessment* usage is voluntary, this message contrasts with the public statements from its individual member agencies on incorporating the *Assessment* into their regular examinations and the impending updates to the *FFIEC IT Handbook Booklets*.

The sector suggests that the regulators help clarify some of the seemingly inconsistent statements below. In addition, the sector suggest that the leadership of the FFIEC member agencies publicly express their commitment to the voluntary nature of *Assessment* usage and strongly articulate this to their examiners as well. We call your attention, specifically, to Comptroller of the Currency Thomas Curry's statement that this *Assessment* will be incorporated gradually and renew our suggestion of implementing this over a 12-18 month timeframe.

In a letter to the Government Accountability Office, Comptroller Curry stated, "[w]e expect to begin using this *Cybersecurity Assessment Tool* in selected examinations that commence during the fourth quarter of 2015."[20] On June 30, 2015, the OCC stated that it intends for OCC Examiners to "gradually incorporate the *Assessment* into Examinations of national banks, federal savings association, and federal branch and agencies (collectively,

[20] Government Accountability Office. *Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information*. GAO-15-509. July 2015. 65.

banks) of all sizes."[21] In their Spring Semiannual Risk Perspective, OCC states with regard to cyber threats: "OCC supervisory staff will review banks' programs for assessing and mitigating the evolving threat environment and cyber resilience. These reviews will include assessments of data and network protection practices, business continuity practices, risks from vendors, and compliance with any new guidance."[22]

A senior OCC official remarked that "[t]he use of the assessment tool is optional for financial institutions; however, OCC examiners will use it to supplement exam work to gain a more complete understanding of an institution's inherent risk, risk management practices, and controls related to cybersecurity. While we will never really know if these measures actually thwart a specific attack, we can be certain that more breaches will occur if we do not commit to being vigilant and continuously enhancing our ability to prevent, detect, and recover from cyber incidents."[23]

The FDIC has indicated, through Financial Institution Letter 28-2015, that "FDIC examiners will discuss the Cybersecurity Assessment Tool with institution management during examinations to ensure awareness and assist with answers to any questions."[24]

The Federal Reserve Board has explicitly stated its intent to begin using the *Assessment*, "…in late 2015 or early 2016 … as part of [the] examination process when evaluating financial institutions' cybersecurity preparedness in information technology and safety and soundness examinations and inspections."[25]

B. Recommendations for Improvement Specific to the Current *Assessment*

Based on preliminary usage of the *Assessment*, the sector has also developed a series of recommendations that could otherwise improve the current *Assessment* for future iterations. These more specific recommendations can be categorized as general recommendations to improve usage of the *Assessment* and recommendations concerning the *Assessment's* Inherent Risk Profile component and the Cybersecurity Maturity component.

---

[21] Office of the Comptroller of the Currency. *OCC Bulletin 2015-31*. Web. <http://www.occ.gov/news-issuances/bulletins/2015/bulletin-2015-31.html>. Published 30 June 2015. Accessed 21 August 2015.

[22] Office of the Comptroller of the Currency. *Semiannual Risk Perspective From the National Risk Committee. Spring 2015*. Web. <http://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2015.pdf>. Accessed 21 August 2015.

[23] Gardineer, Grovetta. "Remarks by Grovetta Gardineer, Deputy Comptroller for Compliance Operations and Policy before the 2015 Association of Military Banks of America Workshop." Leesburg, Virginia. 31 August 2015.

[24] Federal Deposit Insurance Corporation. *Cybersecurity Assessment Tool. FIL 28-2015. Web.* <https://www.fdic.gov/news/news/financial/2015/fil15028.html>. 2 July 2015

[25] Board of Governors of the Federal Reserve System. *Bank Supervision and Regulation Letters: FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors.* SR-15-9. Web. <http://www.federalreserve.gov/bankinforeg/srletters/sr1509.htm>. 2 July 2015.

a. General Recommendations

First, in terms of a general recommendation, many sector institutions suggest that the FFIEC release a companion document to the *Assessment* that describes the FFIEC assumptions and decisions that underlie the *Assessment's* "parts and processes." With such information, institutions report that they would have a greater understanding of how best to interpret and respond to the *Assessment* questions, thus streamlining information collection efforts. More specifically, institutions request interpretive guidance that provides the rationale and methodology of the Inherent Risk Profile, Cybersecurity Maturity, and their various subcomponents and questions.

Institutions also suggest that such a document include a description of the examiner expectations as to an institution's percentage of adherence to a given Inherent Risk activity or Cybersecurity Maturity declarative statement, as well as the standard of proof required to substantiate a given selection. For example, declarative statement D4.RM.Co.B.3 provides, "[c]ontracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party. (FFIEC Information Security Booklet, page 12)." Institutions question whether every single third-party's controls need to be reviewed or just those with the most "cyber risk" in order for an institution to answer '*Yes*,' and during an examination, would it be sufficient for an institution to have just "checked the box '*Yes*' or would every single contract have to be produced to substantiate the claim.

As such, the sector requests that the FFIEC issue a companion document that supplies interpretive guidance with respect to the Inherent Risk Profile, the Cybersecurity Maturity, and their subcomponents and questions, as well as guidance on degree of conformity and examiner expectation on substantiation and documentation.

Second, sector institutions suggest that they be permitted to more easily select their own risk tolerance based on their own business and security factors, such as the line of business that they are in, the business functions that they undertake, the information that they handle, and the cybersecurity program that they have in place. Under the *Assessment*, the focus is on "Inherent Risk" as determined by the FFIEC's *Assessment* categories and questions, but not on the residual risk following the selection and deployment of appropriate compensating controls. As such, in completing the Inherent Risk Profile and reading the *Assessment* statements, "[i]n general, as inherent risk rises, an institution's maturity levels should increase,"[26] and "[i]f management determines that the institution's maturity levels are not appropriate in relation to the inherent risk profile, management should consider reducing inherent risk or developing a strategy to improve the maturity levels,"[27] it indicates that examiners expect a certain inherent risk and corresponding cybersecurity maturity based on *Assessment* outputs.

A bank with an online presence, multiple branches, and internet connections at those branches would qualify as having the Most Inherent Risk. Especially in viewing the statement that "[i]f management determines that the institution's maturity levels are not appropriate in

[26] Federal Financial Institutions Examination Council. *The FFIEC Cybersecurity Assessment Tool.* Page 8. 30 June 2015. Web. <https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_with_Overview_and_Additional_Resources_June_2015_PDF1_5.pdf>.

[27] Id.

relation to the inherent risk profile, management should consider reducing inherent risk or developing a strategy to improve the maturity levels," this raises significant, but potentially distinct, issues for small-, medium-, and large-sized banking institutions. For small-sized institutions that have the desire to increase their maturity levels, examiner pressure may push such institutions toward abandoning or minimizing certain products, services, or technologies so that the Inherent Risk level decreases, rather than evaluating their ability to manage that risk. This could lead to a curtailing of valued product offerings or business growth for smaller institutions. For medium-sized banking institutions, examiners may expect a costly elevation to a new maturity level. For larger-sized banking institutions, examiners may expect not only a high maturity level, but that the institution exhibit an exceptional level of conformance to each declarative statement in those maturity levels.

Moreover, by providing a binary *'Yes/No'* response criteria for Cybersecurity Maturity declarative statements, rather than a degree (or percentage) of conformity, the *Assessment* effectively selects a risk tolerance of zero percent (0%) for the institution; if an institution makes a risk management decision whereby it then cannot answer 100 percent *'Yes'* to a statement, it must then select *'No'*. However, under the current *Assessment*, that risk management decision is not credited, thereby "flattening the risk curve." The implication is that if an institution answers *'No'* (especially to baseline statements), then the answer really should be *'Yes'*. In turn, in order to satisfy the *Assessment*, rather than actual risk, institutions might over invest in one area and under invest in others.

Accordingly, the sector suggests that an inverse model of this *Assessment* may be more appropriate. Traditionally, and by operation of law, it is the responsibility of boards of directors to review and approve the risk appetite of the institution, and then activities, products and services are built around the appetite, or abilities, of the institution to effectively manage the corresponding risk. Thus, the current *Assessment* should be modified to concentrate on residual risk, rather than inherent risk, and allow for greater board selection of risk tolerance, rather than make decisions based on binary *'Yes/No'* criteria.

Indeed, with respect to the NIST *Cybersecurity Framework*, its true value is that it helps identify an institution's capabilities and provides a roadmap for developing a corresponding "plan of action" to address residual risk. This objective-based, action-oriented Framework and corresponding taxonomy is accessible not only from the boardroom to the operations floor, but across enterprises, and across sectors. In addition, because it is applicable for all sectors and contains mapping to "informative references," it operates as a "Rosetta Stone" for various sector-specific risk management jargons and creates a common understanding amongst the sectors around various risk management terms and phrases. As a result, we have heard from member financial institutions that in terms of internal enterprise usage, Chief Information Security Officers have been using it to communicate ideas and achieve "buy-in" for various cybersecurity initiatives. Externally, institutions are using it to communicate expectations and requirements to non-sector vendors and third parties, a stated area of focus for FFIEC member agencies. In contrast, the *Assessment* measures the number of risks and processes at a given point in time, not the ability to address these risks over time or the execution on the processes themselves. In other words, it does not reveal residual risk and provide a roadmap to address it.

The sector believes that over the course of a 12-18 month collaborative, iterative process, these issues could be meaningfully addressed assuming usage is voluntary, and in the meantime, the FFIEC member agencies approach examination as a means for co-exploration of the

Assessment and not as a means to evaluate formally or compare institutions (see Section II.C for a further description of this recommended collaboration).

In addition, the FFIEC may wish to consider developing an automated tool that corresponds with the *Assessment*, provides an institution with the above-described response guidance, etc., and collects the institution's resulting responses to the *Assessment* questions. Such a tool would help banking institutions, particularly less resourced ones, complete the *Assessment* in a more rapid, consistent, and accurate manner.

b. Recommendations Specific to the Inherent Risk Profile

Within the *Assessment*, once an institution determines an Inherent Risk Level for each category's activities, services, or products, that institution would then tabulate the number of times that each respective Risk Level was selected. If, of the 39 different category activities, services or products, the "Moderate Inherent Risk" level was selected a majority of times (e.g., 20 times), then an institution could conclude that its overall inherent risk is of a "Moderate Inherent Risk" level. This overall risk level is then the level that is used as the basis of comparison against all Cybersecurity Maturity domains. It is the sector's recommendation that since there are five categories of Inherent Risk – (1) Technologies and Connection Types; (2) Delivery Channels; (3) Online/Mobile Products and Technology Services; (4) Organizational; and (5) External Threats – there should be as many points of comparison against cybersecurity maturity. Moreover, without addressing whether the five categories or five Cybersecurity Maturity domains are the optimal selections, financial institutions have suggested that the Inherent Risk categories should nonetheless align with the Cybersecurity Maturity domains so that institutions can determine residual risk that then can be "bought down" depending on an institution's risk tolerance and appetite. However, with respect to the current Inherent Risk categories and activities, for the higher level Inherent Risks (e.g., moderate, significant, most), several institutions have requested that the *Assessment* provide a gap analysis between the levels with a list of controls that might help fill those gaps.

In reviewing the current list of Inherent Risk activities, services, or products, the sector makes the following recommendation: that the current *Assessment* be modified so that there is unit consistency as one moves across the activity from the "Least" risk level to the "Most." In the current *Assessment*, there are a number of instances wherein there is lack of consistency in the unit(s) of measure as one makes this movement across an activity to select a risk level. For example, on p.11 of the *Assessment* – fourth activity– the "Minimal" risk level describes the percentage of usage for one device connection: "Only one device type available; available to <5% of employees…" However, in the "Moderate" risk level, it describes the percentage of usage for multiple device connections: "Multiple device types used; available to 10% of employees…"

As institutions and regulators engage in discussions over the next 12-18 months about the utility of the tool, we hope to collaboratively discuss and address the points above.

c. Recommendations Specific to the Cybersecurity Maturity Component

With respect to the Cybersecurity Maturity Domains, while the sector has not formed a consensus as to whether these domains are optimal measures by which to judge cybersecurity maturity, the sector suggests that they should not be viewed with equivalency or equal importance by the FFIEC, and, in turn, its member agencies' examination staff. Because the

Assessment dictates that an institution would have to answer *'Yes'* to all declarative statements in a given cybersecurity maturity level (i.e., the levels of baseline, evolving, intermediate, advanced, and innovative), for domains with more declarative answers to fulfill such as Domains 1 and 3,[28] it is much more difficult to advance in the maturity level as compared to the other domains. Accordingly, we wish to discuss a potential weighting system with the FFIEC to address any such disparities.

Regarding the declarative statements, the sector seriously suggests that the FFIEC reconsider its "all-or-nothing" approach to achieving a given maturity level. This approach does not capture an institution's true cybersecurity maturity. Activities accomplished at a higher maturity level may offset or mitigate items not being done at a lower maturity level (especially considering the number of baseline statements in the domains of Cybersecurity Controls and Cyber Incident Management and Resilience). Institutions should feel comfortable with performing activities above their *Assessment's* assessed cybersecurity maturity level if it mitigates a predecessor control.

Correspondingly, the sector is also concerned with the binary nature of the '*Yes/No*' response requirements to the declarative statements. Many institutions report that they might adhere to 99 percent of a particular declarative statement, but do not fulfill the last one percent (1%) of the statement based on its own carefully considered risk management decision, and, thus, would have to respond *'No'*. For example, D4.RM.Co.B.3 (a baseline control) provides: "Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party. (FFIEC Information Security Booklet, page 12)." It is not possible to do this for every contract, nor is it necessarily warranted. Rather, it should be a risk-based decision based on the institution's risk profile, the contracted party's risk profile, and the functions to be carried out.

In sum, for the current *Assessment* and future versions, the sector recommends revisiting the declarative statements and modifying away from an "all-or-nothing" and binary cybersecurity maturity approach.

Aside from the "all-or-nothing" or binary approach issues, the sector suggests that the *Assessment* refine the distinctions between declarative statements that repeat at the different maturity levels. In the current *Assessment*, it is not always clear what is the distinguishing feature. For example, it is unclear what the distinguishing feature is between the following declarative statements:

- D1.G.Ov.B.4: "The budgeting process includes information security related expenses and tools. (FFIEC E-Banking Booklet, page 20)";
- D1.G.Ov.E.3: "Cybersecurity tools and staff are requested through the budget process";

[28] For example, the number of declarative statements that correspond with each domain is as follows:

- Domain 1: Cyber Risk Management and Oversight = 141 declarative statements;
- Domain 2: Threat Intelligence and Collaboration = 45 declarative statements;
- Domain 3: Cybersecurity Controls = 174 declarative statements;
- Domain 4: External Dependency Management = 51 declarative statements; and,
- Domain 5: Cyber Incident Management and Resilience = 83 statements.

- D1.G.Ov.Int.8: "The budget process for requesting additional cybersecurity staff and tools is integrated into business units' budget processes"; and,
- D1.G.Ov.A.3: "The budget process for requesting additional cybersecurity staff and tools maps current resources and tools to the cybersecurity strategy".

As such, the sector suggests revising the *Assessment* to either explicitly sharpen the distinctions between repeated declarative statements or the FFIEC should consider providing a guide to explain the differing expectations in answering affirmatively to each statement.

Finally, as discussed above, in reviewing the declarative statements, they are seemingly most focused on a particular process or documentable program being in place. For example, there are nearly as many "Risk Management and Oversight" declarative statements as "Cybersecurity Controls" declarative statements, and there are approximately 60 percent more "Risk Management and Oversight" declarative statements than "Cyber Incident Management and Resilience" declarative statements. As such, the sector suggests that the *Assessment* be revised so that cybersecurity maturity is measured not only by programs and processes, but by action and execution. The existence of a policy does not necessarily "stop" an intruder or attacker. Rather, the organization has to appropriately design the policy, implement it, and effectively execute the process or procedures in order to mitigate against would-be attackers.

C. Recommendations for Specific Inherent Risk and Cybersecurity Maturity Subcomponents

Aside from our suggestions outlined above, we would also like to suggest some more specific revisions and clarifications. These are contained in an Attached Appendix B. In addition, the sector wishes to discuss other recommended revisions during an in-person meeting.

D. Other Comments (Mapping to the NIST *Cybersecurity Framework*)

Although helpful, the inclusion of an Appendix mapping the *Assessment* to the NIST *Cybersecurity Framework*, rather than incorporation of the *Assessment* itself into the NIST *Cybersecurity Framework*, will necessitate separate bodies of work or references to demonstrate the coherence of an institution's cyber program against the two frameworks on an ongoing basis. Again, the sector invites a collaborative discussion on these points.

V. A Response to PRA Topic 4: "Ways to minimize the burden of the collection on respondents, including through the use of automated collection techniques or other forms of information technology"

A. Coordination

Aside from FFIEC member agencies, certain financial sector institutions may also be subject to regulatory oversight from the Securities and Exchange Commission ("SEC"), Financial Industry Regulatory Authority ("FINRA"), U.S. Commodities Futures Trading Commission ("CFTC"), state insurance regulators, and others, each of which also have an interest in cybersecurity. In order to minimize the burden of collection, the sector strongly encourages the FFIEC and its member agencies to coordinate with these regulators and also other cybersecurity standards-setting bodies, such as NIST, SEC, etc., before, during, and after the development and release of any future version of the *Assessment*. If each of these separate agencies releases its own "Assessment," the burden on financial institutions will be immense, and, perversely, they may misallocate cybersecurity expertise from cybersecurity activities to responding to similar (but not the same) regulatory requests.

Sector cybersecurity experts are already reporting that this is occurring with their teams as they attempt to shift their cybersecurity programs' alignment from the NIST *Cybersecurity Framework* to the *Assessment* to meet regulatory agency requests and examination expectations. As indicated above, the implementation of this *Assessment* is resulting in some institutions to expend hundreds to thousands in additional resource-hours for adherence/compliance purposes (see Section III above for further discussion). Coordination is essential not only at the point of *Assessment*/Framework development in order to avoid such burdens, but also between agencies at the implementation and interpretation phases. For example, just recently, on August 5, 2015, the Farm Credit Administration ("FCA") issued an *Informational Memorandum* alert to its constituent farm credit system institutions.[29] In this alert entitled, *Cybersecurity Assessment and Expectations for System Institutions*, it stated that while the *Assessment* is not mandatory for its institutions, it should be considered as a set of "best practices" and that the FCA examination program will "incorporate[] these best practices…in [its] evaluation of institutions' cybersecurity preparedness."[30] Given that the FCA is not a FFIEC member agency, and, thus, not a part of coordinated training amongst FFIEC members, its implementation and interpretation will likely diverge.

Coordination among agencies should also occur to avoid duplicative cybersecurity compliance regimes, which could add cost and administrative burden without any perceivable

---

[29] Farm Credit Administration. *Informational Memorandum: Cybersecurity Assessment and Expectations for System Institutions.* 5 Aug. 2015. Web. <http://ww3.fca.gov/readingrm/infomemo/Lists/InformationMemorandums/Attachments/215/IM-Cybersecurity_Risk_Assessment_Tool-05Aug2015.pdf>.

[30] Id. at 2.

advance in cybersecurity. Besides the *Assessment* and the NIST *Cybersecurity Framework*, the sector is aware of the following regulator cybersecurity initiatives that should be harmonized:

- The SEC Office of Compliance Inspections and Examinations' Cybersecurity Initiative as detailed in its April 15, 2014, February 3, 2015, and September 15, 2015 *National Exam Program Risk Alerts;*[31, 32, 33]
- The National Futures Association's August 28, 2015 cybersecurity proposal for CFTC review and approval;[34]
- The Federal Trade Commission's application of cybersecurity standards in unfair, deceptive, and abusive practice (UDAP) enforcement actions post Federal Trade Commission v. Wyndham Worldwide Corporation, _____ (3d Cir. 2015);[35]
- The National Association of Insurance Commissioners' (NAIC) Cybersecurity Task Force review and update of NAIC model laws and regulations to further advance cybersecurity;[36]
- The NIST-led initiative to "pursue the development and use of international standards for cybersecurity," as detailed in the August 10, 2015 *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*[37] and required by the Cybersecurity Enhancement Act of 2014, Section 502;[38]
- The SEC's consideration of revising its rules vis-à-vis publicly traded companies' Audit Committee roles and responsibilities so as to require such committees to oversee "treatment" of "cyber risks";[39]

---

[31] Securities and Exchange Commission, Office of Compliance Inspections and Examinations. *National Exam Program Risk Alert: OCIE Cybersecurity Initiative*. Volume IV, Issue 2. SEC, 14 Apr. 2014. Web. <http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf>.

[32] Securities and Exchange Commission, Office of Compliance Inspections and Examinations. *National Exam Program Risk Alert: Cybersecurity Examination Sweep Summary*. Volume IV, Issue 4. 3 Feb. 2015. Web. <http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf>.

[33] Securities and Exchange Commission, Office of Compliance Inspections and Examinations. *National Exam Program Risk Alert: OCIE's 2015 Cybersecurity Examination Initiative.* Volume IV, Issue 8. 15 Sept. 2015. Web. <http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf>.

[34] National Futures Association. *National Futures Association: Information Systems Security Programs—Proposed Adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs*. 28 Aug. 2015. Web. <https://www.nfa.futures.org/news/.%5CPDF%5CCFTC%5CInterpNotc_CR2-9_2-36_2-49_InfoSystemsSecurityPrograms_Aug_2015.pdf>.

[35] See Federal Trade Commission v. Wyndham Worldwide Corporation, _____ (3d Cir. 2015). Filed 08/24/15, No. 14-3514. Found at: <http://www2.ca3.uscourts.gov/opinarch/143514p.pdf>.

[36] For further information, see the *NAIC Cybersecurity Task Force Meeting Notes* of August 16, 2015 at <http://www.naic.org/meetings1508/committees_ex_cybersecurity_tf_2015_summer_nm_materials.pdf>.

[37] National Institute of Standards and Technology. *NIST IR 8074: Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*. 10 Aug. 2015. Web. <http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8074>.

[38] See 15 U.S.C. 7462.

[39] See 80 FR 38995.

- The SEC Division of Investment Management's April 28, 2015 *IM Guidance Update: Cybersecurity Guidance* for investment advisors;[40]
- The Financial Industry Regulatory Authority's (FINRA) summary of cybersecurity principles and effective practices as reported in its February 3, 2015 *Report on Cybersecurity Practices;*[41]
- The New York Department of Financial Services' "expansion of its information technology examination procedures to focus more attention on cyber security";[42] and,
- The SEC's requests for more detailed cybersecurity and cyber incident related disclosures.[43, 44]

To achieve harmonization, examination simplification, and more effective management of cybersecurity, the FFIEC might consider agency coordination through the "Cybersecurity Forum for Independent and Executive Branch Agencies" ("the Forum").

Accordingly, in order to increase efficiency and *Assessment* effectiveness, increase regulatory harmonization and examination simplification, the FFIEC should consider more robust coordination with NIST and other agencies, potentially through the Forum, to align the increasingly parallel and divergent cybersecurity initiatives, standards, requirements, etc. Indeed, as mentioned, with the issuance of the *Assessment*, it could inadvertently dilute cross-sector cooperation and information exchange and usage and updating of the NIST Cybersecurity Framework.

B. Burden Reduction through Assessment Accessibility and Automated Collection Techniques

Regarding burden reduction generally, several sector institutions recommend that the FFIEC provide the current and any future *Assessment* in both MS Word and Excel formats with hyperlinks to referenced or cross-referenced texts (i.e., from the *Assessment's* Declarative Statements to the exact page and provisions in the referenced FFIEC *IT Examination Handbook Booklets*, rather than to just the FFIEC *IT Examination Handbook Booklets* themselves).

With respect to automated collection techniques, the sector suggests that while electronic collection may reduce burden, such collection and aggregation of information can

---

[40] Securities and Exchange Commission, Division of Investment Management. "IM Guidance Update: Cybersecurity Guidance." No. 2015-02. 28 Apr. 2015. Web. <http://www.sec.gov/investment/im-guidance-2015-02.pdf>.

[41] Financial Industry Regulatory Authority. "Report on Cybersecurity Practices." FINRA, 3 Feb 2015. Web. <https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf>.

[42] Lawsky, Benjamin. "Letter from the New York Department of Financial Services Superintendent to Insurers on Cyber Security." NYDFS, 26 Mar. 2015. Web. <http://www.dfs.ny.gov/about/press2015/pr150326-ltr.pdf>.

[43] White, Mary Jo. "Letter from the Securities and Exchange Commissioner to the Chairman of the U.S. Senate Committee on Commerce, Science, and Transportation." U.S. Senate, 1 May 2013. Web. <http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=7b54b6d0-e9a1-44e9-8545-ea3f90a40edf>.

[44] Temple-West, Patrick. "The SEC Won't Let Me Be." Politico Pro, 18 Aug 2015.

actually represent a sector-wide cybersecurity risk. Thus, if the FFIEC member agencies envision the usage of such collection techniques, they should first establish a highly secure repository to which bank respondents can transmit collected data voluntarily.

Appendix A

Financial Services Sector Coordinating Council Membership

The Financial Services Sector Coordinating Council (FSSCC) fosters and facilitates financial services sector-wide activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The Council was created in June 2002 by the private sector to coordinate critical infrastructure and homeland security activities in the financial services industry.

Associations	Operators	Utilities and Exchanges
American Bankers Association (ABA)	AIG	BATS Exchange
American Council of Life Insurers (ACLI)	American Express	CLS Services
American Insurance Association (AIA)	Aetna	The Clearing House
American Society for Industrial Security International (ASIS)	Bank of America	CME Group
Bank Administration Institute (BAI)	BB&T	Direct Edge
BITS/The Financial Services Roundtable	BNY Mellon	Depository Trust & Clearing Corporation (DTCC)
ChicagoFIRST	Charles Schwab	First Data
Consumer Bankers Associations (CBA)	Citi	Intercontinental Exchange (ICE) / NYSE
Credit Union National Association (CUNA)	Equifax	International Securities Exchange (ISE)
Financial Information Forum (FIF)	Fannie Mae	LCH Clearnet
Financial Services Information Sharing and Analysis Center (FS-ISAC)	Fidelity Investments	NASDAQ
Futures Industry Association (FIA)	FIS Global	National Stock Exchange
Independent Community Bankers of America (ICBA)	Freddie Mac	Omgeo
Institute of International Bankers (IIB)	GE Capital	Options Clearing Corporation
Investment Company Institute (ICI)	Goldman Sachs	
Managed Funds Association (MFA)	JPMorgan Chase	
National Automated Clearing House Association (NACHA)	Manulife Financial	
National Association of Federal Credit Unions (NAFCU)	MasterCard	
National Armored Car Association	Morgan Stanley	
National Futures Association	Navy Federal	
Property Casualty Insurers Association of America (PCI)	Northern Trust	
Securities Industry and Financial Markets Association (SIFMA)	PNC	
	RBS	
	Sallie Mae	
	State Farm	
	State Street	
	Sun Trust	
	US Bank	
	Visa	
	Wells Fargo	

Appendix B

Recommendations Specific to Inherent Risk Profile Subcomponents	
Inherent Risk Profile Category	**Recommendations**
Technologies and Connection Types	Within the "Technologies and Connection Types" Category, consider the type of connection, rather than the number of connections, in determining inherent risk. For instance, Bank A has 1 connection and Bank B has 200 connections. If Bank A's connection is a VPN that allows a third-party unlimited access, while Bank B's connections are mostly computer terminals for cleared staff to access the bank intranet and not the general Internet or other programs, Bank A's single VPN connection could be considered inherently more risky than Bank B's 200 secured and controlled connections.
Delivery Channels	Within the "Delivery Channels" Category, consider separating the "online presence" between web site presence and social media presence. For example, some banks may only offer a website with basic information, while other institutions may offer websites and a robust social media presence, but do not respond to customers via social media. Within the "moderate" level, a bank would be considered to be in this category if it communicates to customers through social media. Clarifying whether this applies to a bank that responds to customer inquiries over social media (e.g., on a Twitter exchange about whether the bank offers a particular service, without particulars as to the service or customer data) would be helpful.
N/A	Clarifying whether the number of ATMs, branches, prepaid cards, and the like affects inherent risk, or the nature of these products and services would be helpful.

Recommendations Specific to Cybersecurity Maturity Subcomponents		
Mapping Number	**Declarative Statement**	**Recommendations**
D1.RM.RA.B.3	The risk assessment is updated to address new technologies, products, services, and connections before deployment. (FFIEC Information Security Booklet, page 13)	Consider removing or reevaluating this declarative statement, because a risk assessment is at a point in time and each technology, product, service, and connection change may not have a direct effect on the environment. For example, hardware changes, such as router switching, would not necessitate a reevaluation of the risk assessment.

Recommendations Specific to Cybersecurity Maturity Subcomponents		
Mapping Number	**Declarative Statement**	**Recommendations**
D3.PC.Im.B.3	All Ports are monitored. (FFIEC Information Security Booklet, page 50) Source: IS.B.50: Institutions should consider securing PCs to workstations, locking or removing disk drives and unnecessary physical ports, and using screensaver passwords or automatic timeouts.	Clarifying this particular declarative statement would be useful, as it does not appear to be consistent with the FFIEC Information Security Booklet, which suggests monitoring all ports only on publicly accessible/open PCs, etc., within branch locations.
D4.RM.Co.B.3	Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party. (FFIEC Information Security Booklet, page 12)	Modifying this binary approach by grounding it in risk-based decision-making would be helpful.
D5.IR.Pl.E.4	Business impact analyses have been updated to include cybersecurity.	More feedback as to the degree of updating would be helpful.
D2.TI.Ti.Int.2	Protocols are implemented for collecting information from industry peers and government.	Clarifying how formal a protocol should be would be helpful. Recommend adding "where they exist" at the end of that statement so that institutions can respond more appropriately.
D2.TI.Ti.Int.3	A read-only, central repository of cyber threat intelligence is maintained.	Clarifying the definition of "read-only" would be beneficial. It is not clear whether "read-only" means that the repository is locked down to only those who need it, or that you cannot edit previous entries.

Recommendations Specific to Cybersecurity Maturity Subcomponents		
Mapping Number	**Declarative Statement**	**Recommendations**
D2.TI.Ti.A.2	Threat intelligence is automatically received from multiple sources in real time.	It would be beneficial to clarify the definition of what constitutes "real-time"; whether the "real-time" requirement applies to the threat intelligence generation or ability to transmit and share; and whether that if real-time is not applicable to generation, then it would mean the expectation is that the shared information can then be acted on almost instantly (machine to machine).
D2.MA.Ma.A.5	Threat intelligence is used to update architecture and configuration standards.	It would be beneficial to clarify whether this refers to updating architecture or architecture standards and the definition of architecture standards if the latter. Firms would be unlikely to alter the manner in which their technology architecture is arranged based on single feeds.
D2.IS.Is.E.1	A formal and secure process is in place to share threat and vulnerability information with other entities.	Recommend that the provision be amended to read, "To the extent practicable, a formal and secure process is in place to share threat and vulnerability information with other entities," given that it may not be possible to have a formal and secure program with and for every entity.
D2.IS.Is.Inn.1	A mechanism is in place for sharing cyber threat intelligence with business units in real time, including the potential financial and operational impact of inaction.	Providing a definition as to what constitutes "real-time" would be beneficial.

Recommendations Specific to Cybersecurity Maturity Subcomponents		
Mapping Number	**Declarative Statement**	**Recommendations**
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware. (FFIEC Information Security Booklet, page 21)	Clarifying what constitutes "hardware" would be beneficial. The definition of "hardware" in the FFIEC Information Security Booklet's glossary does not indicate that authentication could be applicable to that definition as it speaks to physical elements of computer systems. It is not clear whether the definition extends to routers and servers.
D1.G.IT.Int.1	Baseline configurations cannot be altered without a formal change request, documented approval, and an assessment of security implications.	Clarifying what constitutes "baseline configurations" (e.g., firewall, server, etc.) would be beneficial.
D1.G.IT.A.1	Supply chain risk is reviewed before the acquisition of mission-critical information systems, including system components.	Clarifying the types of risk that should be reviewed and providing some examples of relevant Supply Chain risks would be useful.
D1.G.IT.Inn.1	A formal change management function governs decentralized or highly distributed change requests and identifies and measures security risks that may cause increased exposure to cyber-attack.	Some examples and/or context to clarify expected governance and what is meant by decentralized or highly distributed change requests would be helpful.
D1.RM.RMP.A.5	The cyber risk data aggregation and real-time reporting capabilities support the institution's ongoing reporting needs, particularly during cyber incidents.	Some examples of risk data aggregation and real-time reporting capabilities would be helpful in providing better context.
D1.TC.Tr.A.1	Independent directors are provided with cybersecurity training that addresses how complex products, services, and lines of business affect the institution's cyber risk.	Clarifying the definition of independent directors would be helpful.
D3.PC.Im.B.4	Up-to-date antivirus and anti-malware tools are used. (FFIEC Information Security Booklet, page 78)	Clarifying the definition of "tools" and whether this refers to software updates only or virus definition updates would be helpful.

Recommendations Specific to Cybersecurity Maturity Subcomponents		
Mapping Number	**Declarative Statement**	**Recommendations**
D3.PC.Im.B.8	Programs that can override system, object, network, virtual machine, and application controls are restricted. (FFIEC Information Security Booklet, page 41)	Listing some examples of software programs having "override" capability and describing their capabilities would be helpful.
D3.PC.Im.E.8	Controls for unsupported systems are implemented and tested.	Clarifying the definition of "unsupported systems" and providing some examples of the types of controls around these would be helpful.
D3.PC.Im.Int.4	Wireless networks use strong encryption with encryption keys that are changed frequently. (*N/A if there are no wireless networks.)	Clarifying the context (e.g., if there are multiple wireless networks being used, which ones need to be more tightly controlled) would be helpful.
D3.PC.Im.A.2	Only one primary function is permitted per server to prevent functions that require different security levels from co-existing on the same server.	Clarifying the definition of "primary function" would be helpful.
D3.PC.Im.Inn.4	Public-facing servers are routinely rotated and restored to a known clean state to limit the window of time a system is exposed to potential threats.	Clarifying expectations concerning "routinely rotated and restored to a known clean state" would be helpful.
D3.PC.Am.E.3	Use of customer data in non-production environments complies with legal, regulatory, and internal policy requirements for concealing or removing of sensitive data elements.	Clarifying the definition of "sensitive" data would be helpful.
D3.PC.Am.Int.6	Multifactor authentication (e.g., tokens, digital certificates) techniques are used for employee access to high-risk systems as identified in the risk assessment(s). (*N/A if no high risk systems.)	Clarifying the definition of "high risk" would be helpful.
D3.PC.Am.Int.7	Confidential data are encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.	Clarifying the definition of "trusted zones" would be helpful.

Recommendations Specific to Cybersecurity Maturity Subcomponents		
Mapping Number	**Declarative Statement**	**Recommendations**
D3.PC.Am.Inn.1	Adaptive access controls de-provision or isolate an employee, third-party, or customer credentials to minimize potential damage if malicious behavior is suspected.	Listing some examples would be helpful.
D3.PC.Am.Inn.2	Unstructured confidential data are tracked and secured through an identity-aware, cross-platform storage system that protects against internal threats, monitors user access, and tracks changes.	Clarifying both the current technologies that perform this action and the definitions of "unstructured data" and "cross platform storage" would be helpful.
D3.PC.Am.Inn.3	Tokenization is used to substitute unique values for confidential information (e.g., virtual credit card).	Clarifying the definition of "confidential information" would be helpful.
D3.PC.Am.Inn.4	The institution is leading efforts to create new technologies and processes for managing customer, employee, and third-party authentication and access.	Clarifying the definition of "new technologies" and providing some examples would be helpful.
D3.PC.Am.Inn.5	Real-time risk mitigation is taken based on automated risk scoring of user credentials.	Clarifying the definition of "risk scoring" would be helpful.
D3.PC.De.E.1	Tools automatically block attempted access from unpatched employee and third-party devices.	Listing examples would be helpful.
D3.PC.De.E.3	The institution has controls to prevent the unauthorized addition of new connections.	Clarifying the definition of "unauthorized addition of new connections" or providing some examples would be helpful.
D3.PC.De.E.4	Controls are in place to prevent unauthorized individuals from copying confidential data to removable media.	Suggest reconsidering statement, as it appears to overlap with the first one of the previous set of questions (D3.PC.DES.B.1). Clarifying and providing examples would be helpful.
D3.DC.Th.B.2	Antivirus and anti-malware tools are used to detect attacks. (FFIEC Information Security Booklet, page 55)	Listing examples would be helpful.

Recommendations Specific to Cybersecurity Maturity Subcomponents		
Mapping Number	**Declarative Statement**	**Recommendations**
D3.DC.Th.E.3	Antivirus and anti-malware tools are updated automatically.	Clarifying the definition of "tools" would be helpful.
D3.DC.An.B.1	The institution is able to detect anomalous activities through monitoring across the environment. (FFIEC Information Security Booklet, page 32)	Clarifying the definition of monitoring and providing some examples would be helpful.
D3.CC.Re.Int.1	Remediation efforts are confirmed by conducting a follow-up vulnerability scan.	Clarifying whether the question concerns remediating identified vulnerabilities or remediation efforts would be helpful.
D4.C.Co.Int.4	Monitoring controls cover all internal network-to-network connections.	Listing examples would be helpful.
D5.IR.Pl.B.5	A formal backup and recovery plan exists for all critical business lines. (FFIEC Business Continuity Planning Booklet, page 4)	Recognizing that banks may have multiple such plans, suggest making the term "plan" plural.
D5.IR.Pl.Int.2	Plans are in place to re-route or substitute critical functions and/or services that may be affected by a successful attack on Internet-facing systems.	Clarifying whether the question is specific to technology or business and technology plans would be helpful.
D5.IR.Te.Inn.1	The institution tests the ability to shift business processes or functions between different processing centers or technology systems for cyber incidents without interruption to business or loss of productivity or data.	Clarifying the definition of "processing centers" and whether the question intends to reflect both business and technology. If so, perhaps the question could be split into two parts.