February 17, 2017

Robert deV. Frierson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, D.C. 20551
E-mail: regs.comments@federalreserve.gov

Re: Enhanced Cyber Risk Management Standards (RIN 7100-AE 61; Docket No. R-1550)

Dear Mr. Frierson:

I write on behalf of The Insurance Coalition, a group of federally supervised insurance companies and interested parties. We share a common interest in federal regulations that apply to insurance savings and loan holding companies ("insurance SLHCs") and insurers that have been designated as systemically important nonbank financial institutions ("insurance SIFIs.") In this case, we write because as insurance SLHCs or insurance SIFIs, many Insurance Coalition members would be directly affected by the enhanced cyber risk management standards supervised by the Federal Reserve Board ("the Board")[1] that are the subject of the advanced notice of proposed rulemaking ("ANPR") issued by the Board and other federal financial regulators (collectively, "the Agencies") in October of last year.

We appreciate the opportunity to comment and share your commitment to strong cybersecurity practices. As insurers whose core mission is policyholder protection, we are deeply committed to ensuring the financial sector is safe from cyber threats, especially given our mandate to protect our policyholders' critical information. We also appreciate the Agencies' deliberative approach, as evidenced by engaging in an ANPR with more than one round of public comments. We look forward to engaging on this matter as the rulemaking process moves forward.

Executive Summary

We believe that insurance SLHCs and SIFIs should be excluded from this rulemaking, as a cyber attack on such institutions would not have systemic consequences. While insurers are vulnerable to cyber-attacks (as are any actors in the economy), such attack would not create sytem-wide knock-on effects. In addition, insurers are already subject to overlapping (and

[1] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. Capital Requirements for Supervised Institutions Engaged in Insurance Activities, 81 Fed. Reg. 74315 (Oct. 26, 2016).

sometimes directly duplicative) regulatory and legal requirements around cybersecurity. Adding an additional layer of requirements would merelely serve to divert resources away from defending against cyber attacks towards demonstrating compliance with yet another standard.

If insurance SLHCs and SIFIs are not excluded, we respectfully request that the Board pursue a separate rulemaking tailored to insurers and their regulatory landscape. At a minimum, any federal cybersecurity regulations for insurers should be harmonized with existing state and federal laws and coordinated with the NAIC work regarding cybersecurity. Failure to achieve such harmonization would not serve the goal of enhancing cybersecurity of our financial system.

Additionally, we believe that the ANPR's new cyber risk governance requirements should not apply to insurers, as the Board can already effectively address any governance concerns through day-to-day examination. These new requirements would result in uncessary board and management structure changes, and in our view are overly prescriptive.

We also believe that the ANPR's cyber risk management proposal is too prescriptive, as any concerns regarding existing reporting structures addressing cyber risk can be adequately addressed through supervision. Furthermore, cyber risk to insurers is similar to other risks not subject to such prescriptive Board-imposed requirements.

Specific Comments

I. Scope of Application (ANPR Questions 1 and 3).

In promulgating enhanced cybersecurity standards, the Board seeks to mitigate risks at individual firms to minimize the risk of cyber-attacks having systemic consequences. The crux of the Agencies' concern appears to be that large, global financial institutions engaged in banking could experience cyber-attacks that, because of the particular role these institutions play in our financial system, could have wide-ranging consequences. Specifically, in providing background on the ANPR, the Agencies cite financial institutions engaging in national and international banking activities that covered entities "play an important role in U.S. payment, clearing, and settlement arrangements and provide access to credit for business and households."

We agree that cyber threats are a critical source of risk for any financial institution. We also support cybersecurity standards being applied to our member company banking operations. However, we respectfully urge that the Board exclude insurance savings and loan holding

companies and SIFIs from this rulemaking because cyber-attacks on these institutions would not have systemic consequences, and for other policy reasons described below.[2]

First and foremost, we believe that insurers do not play the type of role in the financial system that would result in contagion following a cyber-attack. To be clear, the insurance sector, like every component of the public and private sector economy, is vulnerable to cyber-attacks, and we take the threat very seriously. Insurers, like other actors in the economy, are connected to other financial and non-financial institutions, through our sales, servicing and investment activities. Thus, insurers, like all other economic actors, use third-party vendors. Such connections, if not properly addressed, can result in increased vulnerability to cyber-attack. We believe that they are generally well addressed today by the existing regulatory and legal environment and that our sector (and individual firms within it) is not so complex and interconnected such that a cyber-attack would have systemic consequences.

Notably, while insurance companies provide critical protections to policyholders across the entire sales and servicing spectrum, they do not provide payment, clearing, and settlement arrangements and access to credit in the same manner as banks. Rather, they accept policyholder premiums, invest those premiums, and pay out claims. They do not serve as a nexus or connection point between multiple different actors in the financial services system. To be clear, a cyber-attack on an insurer can have significant and devastating consequences on the institution and its policyholders. We take that threat very seriously and believe that our regulatory framework should mitigate such risk. However, insurers should not be subject to regulations aimed at reducing systemic risk following a cyber-attack, because the sector simply does not pose systemic risk caused by a cyber-attack.

Specifically, with respect to insurance SLHCs, we believe that these institutions are not sufficiently interconnected and systemically important to warrant enhanced standards of any kind, including enhanced cybersecurity standards.[3] The Board has already identified these 12 firms as not being sufficiently interconnected to pose systemic risk.[4] As a general policy matter, we believe that it is inappropriate and unnecessary to impose any enhanced prudential standards on these companies, and here the costs of added regulation on cybersecurity outweigh any benefits.

Additionally, we believe that the above arguments also apply to insurers that have been designated as SIFIs. First, as we have stated in prior comment letters, size is not an appropriate

[2] This section responds to Questions 1 and 3 of the ANPR regarding Scope of Application.
[3] As noted in prior comment letters, the Insurance Coalition takes the position that insurance companies do not pose a systemic risk.
[4] Capital Requirements for Supervised Institutions Significantly Engaged in Insurance Activities, 81, Fed. Reg. 38631, 38632 (June 14, 2016).

proxy for risk. In other words, setting aside any SIFI designation, we do not believe that insurers should be subject to enhanced cybersecurity standards by virtue of their assets under management. Second, insurance SIFIs, like insurance SLHCs, play a different role in the financial sector than large commercial banks. Insurance SIFIs do not have global banking operations. The ANPR notes that such firms "perform critical functions for the US financial system." We agree that insurers play a critical role in the economy as investors and a critical role in American households are providers of protection for families. However, insurance SIFIs do not provide payment, clearing, and settlement functions and do not provide significant access to credit for businesses. Thus, it is not appropriate to impose enhanced cybersecurity standards designed for banks on such firms.

Again, we are committed to rigorous cybersecurity measures. However, we also believe that the Board's existing supervisory tools are well equipped to address cyber risk at Board-supervised insurers. As noted in the ANPR, the Board has already incorporated information security into its supervisory review of insurers. This supervisory review is appropriately robust and also includes a review of third-party service providers. This ongoing supervisory process provides a highly effective mechanism for the Board to immediately address any perceived gaps in security at any supervised insurer. We support this existing mechanism to ensure that covered entities comply with cybersecurity requirements.

As companies that take cybersecurity extremely seriously (and indeed, in some cases, as providers of cyber insurance), we feel strongly that the appropriate focus of any regulator with respect to the adequacy of cybersecurity requirements themselves, not in the manner in which companies structure their response to requirements. In other words, the ANPR assumes that underlying cybersecurity standards are adequate, and seeks their effective enforcement through governance and other controls. We respectfully suggest that primary emphasis be placed on ensuring that a single, uniform set of controls is in place for covered entities that is robust but is flexible enough to evolve with cyber threats.

In our view, for the above reasons, the Board should exclude federally supervised insurers entirely from the cybersecurity rulemaking. Failing that, we recommend that the Board undertake a separate rulemaking for insurance SLHCs and insurance SIFIs to reflect both a greater harmonization with existing standards (see below) and the insurance business model.

II. Harmonization with Other Standards

If the Board declines to exempt insurers from enhanced cybersecurity standards, we urge the Board to pursue a separate rulemaking to address the unique aspects of insurance and the regulatory landscape. Relatedly, we respectfully request that the Board harmonize and avoid

duplication of the requirements in any new standards with existing regulation, including those under development.

As noted in the ANPR, several existing supervisory programs address cybersecurity practices. These tools include the Uniform Rating System for Information Technology ("URSIT"), the FFIEC Cybersecurity Assessment Tool, and the NIST Cybersecurity Framework. In our view, the ANPR is not adequately harmonized with these existing tools. While it is true that the ANPR would create a required regulatory standard, the standard articulated in the ANPR would not actually specifically incorporate any of the aforementioned standards. In fact, they would likely further divert resources from implementing new cybersecurity measures towards ensuing compliance with a somewhat duplicative regime. This would exacerbate, rather than ameliorate, the patchwork of standards already in place

In addition to the programs described in the ANPR, insurers are already subject to a host of cybersecurity regulations. The existing patchwork of rules has added complexity and cost and the lack of harmonization does not serve the goal of increasing cybersecurity. If not harmonized with these standards, the ANPR would likely do more harm than good.

Specifically, insurers are subject to state data security laws and oversight by state insurance commissioners. This oversight specifically includes review of insurers' cybersecurity practices. Revisions made to the Financial Condition Examiners Handbook in 2015 provide specific guidance for examiners who review an insurer's cybersecurity practices. In addition to adopting an approach to cybersecurity consistent with the NIST Cybersecurity Framework, the handbook encourages examiners to use cybersecurity experts if the insurer has significant exposure to cyber risk. Moreover, attention to cybersecurity by the state insurance regulatory community has generally increased over the past few years. Notably, in 2013 state insurance regulators established the Cybersecurity Task Force to consider issues concerning cybersecurity as they pertain to the role of state insurance regulators.[5]

In terms of federal requirements, federally supervised insurers are subject to ongoing supervision by the Board, as noted above, and many are also subject to SEC and FINRA exams, and OCC quarterly exams, all of which include cybersecurity assessments. In addition, insurers must comply with Gramm-Leach-Bliley data security requirements, enforced by state insurance commissioners. Some businesses within federally supervised insurers are also subject to the requirements of HIPAA. In addition, as noted in the ANPR, the FFIEC has done a significant

[5] NAIC, Cybersecurity (EX) Task Force, available at: http://www.naic.org/cmte_ex_cybersecurity_tf.htm.

amount of work in the privacy and data security space, including promulgating standards, regulations, and an examiners handbook.[6]

These programs are not harmonized with each other, and insurers spend an enormous amount of time and money on duplicative requirements and exams. We would support a single, comprehensive, and robust exam to fulfill all existing supervisory requirements. Such a practice would enhance cybersecurity by holding firms to a single high standard and freeing up internal resources to focus on ever-emerging threats rather than compliance with duplicative requirements.

In addition to existing programs, new cybersecurity requirements for insurers are under development, underscoring the need for harmonization with federal requirements. The Cybersecurity (EX) Task Force of the National Association of Insurance Commissioners is developing an update to its insurance data security model law that, in its current form, would be specific to the insurance sector. The model law could also be incorporated into the NAIC's accreditation standards, which would effectively ultimately mean its adoption in all 50 states.

The Insurance Coalition supports the effort to harmonize information all information security requirements. However, as with the ANPR, we believe that the model law will only advance the goal of cyber security if it provides one uniform standard. Regardless, we believe that any federal cybersecurity regulations for insurers should be harmonized with existing state laws and coordinated with the NAIC work on this topic. We note that the Financial and Banking Information Infrastructure Committee ("FBIIC") includes the Board and state insurance regulators, and would suggest that the Board develop a formal mechanism for coordination with state insurance commissioners before proceeding, to avoid creating duplicative and conflicting requirements.

In the absence of a clear federal or single state standard that other regulators defer to, the problem of the patchwork of existing requirements is likely to worsen. Without addressing the substance of the rule, we note that the New York Department of Financial Services issued an updated cybersecurity regulation, which will be effective on March 17, 2017.[7] This comprehensive regulation would apply to most federally supervised insurers (as well as banking organizations). At a minimum, we recommend that the Board delay issuance of an NPR until this rule is effective.

---

[6] *See Welcome to the Federal Financial Institutions Examination Council's (FFIEC) Web Site*, FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (last modified Aug. 30, 2016), https://www.ffiec.gov/about.htm (showing links for "IT Handbook InfoBase," "Cybersecurity Awareness" and that the FFIEC prescribes "uniform principles, standards, and reports on an array of topics).

[7] Press Release, New York Department of Financial Strategies, DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions (Dec. 28, 2016), http://www.dfs.ny.gov/about/press/pr1612281.htm.

As described above, the existing web of cybersecurity regulations has failed to produce a single robust standard that all regulators can rely on. We support such a standard, but recognize the difficulty in achieving this goal. In the meantime, we believe that federally supervised insurers are already subject to rigorous, multiple requirements at the state and federal level, and we believe that the imposition of an additional federal standard that is not harmonized with existing requirements would not serve the goal of enhancing cybersecurity of our financial system.

III. Cyber Risk Governance

The ANPR contemplates a number of new requirements regarding cyber risk governance, including:

- A written, board-approved enterprise-wide cyber risk management strategy,
- Written, board-approved, enterprise-wide cyber risk management strategy;
- Board-approved and established cyber risk tolerances;
- Board must have cyber expertise or have access to staff or resources;
- Requiring that those responsible for cyber risk be independent of business units, and have independent access to the board of directors, and fall under specific reporting relationships; and
- Senior leaders with responsibility for cyber risk oversight to be independent of business line management.[8]

We respectfully submit that these requirements are overly prescriptive and unnecessary as applied to insurers. As noted earlier, the Board can already address any governance concern at federally supervised insurers through its examination process. These new requirements could force insurance SLHCs to change their board and management structure, with the result that the board is overly involved in a firm's day-to-day management. This is more appropriately a role for senior leadership of a company, and does not diminish the benefit of ensuring full compliance with Board cybersecurity (and other regulatory) requirements. Cyber risk, while very critical, should be viewed on par with other risks to federally supervised insurers that come before boards of directors.

IV. Cyber Risk Management

The ANPR conceives cyber risk management cutting across three independent functions:

- **Business units**- would be required to access cyber risks and to adhere to policies and procedures designed to manage those risks;

[8] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74315, 74320-74321 (Oct. 26, 2016).

- **Independent risk management function**- reporting to CRO and the Board- would assess risks across the enterprise; and
- **Audit**- required to develop a full audit plan to review cyber risk management and to measure the effectiveness of the cyber risk controls, including through penetration testing and other vulnerability assessments consistent with an entity's size, complexity, scope of operations, and interconnectedness.

As with the cyber risk governance proposal, we support the goal of ensuring multiple lines of defense, but believe that the ANPR is too prescriptive. As an example, federally supervised insurers could be required to reorganize their IT and other departments, when existing structures might best serve the goals of the ANPR. Again, any Board concern regarding existing reporting structures adequately addressing cyber risk can be addressed through ongoing supervision. We also believe that cyber risk at insurers should be viewed similarly to other types of risk (underwriting risk, etc.) which are not subject to such prescriptive Board-imposed requirements.

V. Conclusion

Again, we support application of strong cybersecurity standards to financial institutions, and appreciate the thoughtful process the Agencies have undertaken. For the reasons described above, we support excluding insurance SLHCs and SIFIs from this rulemaking. If the Board declines this exemption, we support the a separate rulemaking tailored to the unique insurance and regulatory landscape, and respectfully urge the Board to harmonize existing standards and avoid duplication of current requirements in any new standards. We look forward to continued dialoug as the Board develops their subsequent Notice of Proposed Rulemaking.

Sincerely,

Bridget Hagan
Executive Director, The Insurance Coalition