***Jigar Gandhi***
*Counsel*

**Via electronic mail to** regs.comments@federalreserve.gov

February 10, 2017

Janet Yellen
Chair
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Docket No. 1550
RIN No. 7100 AE-61

Legislative and Regulatory Activities Division
Office of the Comptroller of Currency
400 7th Street SW Suite 3E-218, mail stop 9W-11
Washington, DC 20219

Docket ID OCC-2016-0016

Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

RIN No. 3064-AE45

Re: Advanced Notice of Proposed Rulemaking for Enhanced Cyber Risk Management Standards

Dear Chair Yellen:

On behalf of the American Council of Life Insurers ("ACLI")[1] and its approximately 290-member life insurance companies, we are writing in response to the request of the Board of Governors of the Federal Reserve System, Office of the Comptroller of Currency and the Federal Deposit Insurance Corporation ("Joint Agencies) for public comment on the advanced notice of proposed rulemaking on Enhanced Cyber Risk Management Standards (Cyber ANPR). As always, we welcome the opportunity to provide our

[1] American Council of Life Insurers (ACLI) is a Washington, D.C.-based trade association with approximately 290 member companies operating in the United States and abroad. ACLI advocates in state, federal, and international forums for public policy that supports the industry marketplace and the 75 million American families that rely on life insurers' products for financial and retirement security. ACLI members offer life insurance, annuities, retirement plans, long-term care and disability income insurance, and reinsurance, representing more than 94 percent of industry assets, 93 percent of life insurance premiums, and 97 percent of annuity considerations in the United States. Learn more at www.acli.com.

***American Council of Life Insurers***
*101 Constitution Avenue, NW, Washington, DC 20001-2133*
*(202) 624-2019 t (866) 953-4083 f jigargandhi@ac i.com*
***www.acli.com***

views on a regulatory proposal of significance to the life insurance industry. ACLI has several members that qualify as covered entities under the Joint Agencies' proposed scope of application.

Life insurers strongly support the underlying goal of the proposed enhanced standards to promote the security of the financial services sector and to increase its resilience to cyber events. Life insurers, regardless of size or business model, value strong cybersecurity protections and currently have in place robust policies and procedures to best avoid harm to their information technology (IT) systems and their customers' personal information. Life insurers already are subject to rigorous oversight on cyber risk, data security and other matters under state insurance laws. Therefore, we do not believe that the proposed new federal regulations on cyber risk management are currently necessary or practical for life insurers covered by the ANPR. In addition, the proposed standards the Joint Agencies lay out in the Cyber ANPR are alternatingly prescriptive or vague. We appreciate the Joint Agencies' efforts to attempt to gather additional information by asking specific, tailored questions. However, the Joint Agencies' proposed approach is overly prescriptive and not risk-based, while in other instances, the Joint Agencies lay out a general framework and requests for information that are nebulous and confusing.

We strongly recommend that the Joint Agencies collaborate on an ongoing basis with the industry to address the issues and questions raised in the Cyber ANPR. Not all covered entities under the various Joint Agencies' jurisdictions are the same. Therefore, rules that are not risk-based and flexible would impose onerous requirements on covered entities which could undercut, rather than enhance, their ability to secure their IT systems and customer information. Covered entities should be permitted to implement cybersecurity policies and practices to address the needs identified by their respective risk assessments, as appropriate to each institution. We have provided information in response to some of the Cyber ANPR's questions below; however, again we believe that the Joint Agencies should ensure an ongoing dialogue and a collaborative process with industry to consider the issues raised in the Cyber ANPR.

***Scope of Application***

As stated above, in the Cyber ANPR, the Joint Agencies are considering application of enhanced standards on an enterprise-wide basis institutions under their jurisdiction, including Savings and Loan Holding Companies with total consolidated assets of $50 billion or more. The Joint Agencies also are considering application of the standards to nonbank financial companies supervised by the Federal Reserve pursuant to Section 165 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Much of the Joint Agencies' consideration throughout the proposed standards is bank-centric. For example, in the Cyber ANPR under its discussion of Incident Response, Cyber Resilience, and Situational Awareness, the Joint Agencies state "[t]he preservation of critical records in the event of a large-scale or significant cyber event is essential to maintaining confidence in the banking system."[2] The Joint Agencies' focus on banking institutions does not consider that insurance companies have dramatically different business models, sell different products, and provide different services than banks. Further, insurance companies do not have the same level of connectivity to the payments, settlement, and clearing systems that banks do. Also, as indicated above, life insurers already have robust security policies and procedures subject to broad regulatory oversight and therefore do not believe that the proposed new standards are currently necessary or practical for life insurers covered by the ANPR.

Further, the applicability of any new security standards should be risk-based and based on a financial institution's impact on the financial system, not simply the size of its consolidated assets. To alleviate the issues described above, the Joint Agencies should engage in a collaborative process with covered

[2] Enhanced Cyber Risk Management Standards, *available at*, https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf

entities, including insurance companies. Such a process would perpetuate a risk-based approach for determining the appropriate scope of any new standards.

Further, the Joint Agencies should narrow their focus to entities over which they have direct authority. They should not attempt to exercise authority over subsidiaries or third party service providers over which they do not have direct authority.

More concerning than the broad applicability of the enhanced standards are the actual proposed standards themselves. The Joint Agencies should ensure that any standards are risk-based and flexible, allowing covered entities to respond to specific threats most effectively.

***Cyber Risk Governance***

In its Cyber ANPR, the Joint Agencies propose that covered entities "develop a written, board-approved, enterprise-wide cyber risk management strategy" that is incorporated into the overall business strategy of the covered entity.[3] The proposed standards would also require a covered entity to establish risk tolerances consistent with the firm's risk appetite and would require a covered entity to identify and assess activities that present cyber risk.[4] They would also require a covered entity to establish a management framework including policies and procedures to implement a covered entity's cyber risk management strategy and would require the Board of Directors to hold senior management accountable for implementing a framework.[5]

The Joint Agencies' proposed governance requirements would lead to several implementation challenges relevant to the requirement that a covered entity formally state its risk appetite and tolerances. The first implementation challenge relates to risk identification. There are unknown numbers of cyber risk vulnerabilities that may impact a covered entity's risk profile when risks are disclosed. Therefore, calculating and managing to a specific risk appetite and associated tolerances is subjective and based on incomplete information and largely due to the complex and dynamic nature of the threats that companies face.

The second implementation challenge relates to cyber risk evaluations and prioritizations. The pervasive nature of cyber risk entails that a single threat initially deemed low priority can potentially be exploited and impact an insurer's operations globally. Therefore, implementing a rigid process requiring identifying a risk as either low or high-risk could hamper a covered entity's ability to quickly escalate its response if an initially low-risk threat becomes high-risk.

As evidenced by recent headlines, there is a global pool of threat actors, including state actors with virtually unlimited resources, which specifically leads to the challenge of risk mitigation. These actors can make it economically unfeasible to manage cyber risks to a firm's unique risk profile and needs.

Therefore, any new governance requirements should be risk-based to ensure covered entities are taking reasonable steps, best suited to their individual needs, to identify and mitigate cyber risks. Further, any standards should place responsibility for oversight and implementation of any framework with senior management as opposed to the Board of Directors. Senior management, with inherent knowledge of a covered entity's operations, is the best positioned to implement a cyber framework.

---

[3] Enhanced Cyber Risk Management Standards, *available at*, https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf

[4] *Id.*

[5] *Id.*

***Cyber Risk Management***

In the Cyber ANPR, the Joint Agencies propose that covered entities integrate cyber risk management into the responsibilities of at least three separate business functions.[6] The Joint Agencies believe this approach would enable covered entities to appropriately hedge and protect against emerging cyber threats. In their questions, the Joint Agencies request information on the appropriateness of requiring covered entities to report on cyber vulnerabilities to the Board of Directors and seek information on whether the organizational standards they set out are appropriate.[7]

As stated above, the Joint Agencies should avoid prescriptive requirements that are not risk-based. It is generally appropriate for a covered entity's Board of Directors to receive reports on cyber risks and vulnerabilities. However, flexibility on these governance issues, that considers each covered entity's unique corporate governance structure, is essential. Covered entities may have differing Board-level committees which oversee cyber risks and vulnerabilities and may have differing Board of Directors meeting schedules. The Joint Agencies should provide a risk-based framework for covered entities to determine, on their own, how to best structure their governance models to detect and prevent cyber-attacks. As an example, the Joint Agencies should look to the Federal Trade Commission's Identity Theft Red Flag Program Guide.[8]

In its Cyber ANPR, the Joint Agencies focus on a "Three Lines of Defense" Model, where various business units and audit functions would be responsible for cyber risk management. However, again, the Joint Agencies' enumerated approach is too prescriptive and not risk-based.

The Joint Agencies envision a scattered approach to cyber risk management across a covered entity's enterprise risk management. However, this may not be the most effective approach for all covered entities. Some covered entities may effectively utilize an approach where day-to-day management of cyber risk controls are largely held within a single business unit, and where other control functions are conducted as necessary. This would allow for a level of specialization and expertise on existing and emerging cyber risks for company systems, applications, vendors, etc. Spreading oversight responsibilities for cyber risk to business units that do not have expertise in the subject-matter could cause covered entities to have less effective reporting and escalation of cyber risks and trends to senior management.

Again, a flexible, risk-based approach would best position covered entities to protect valuable information. The Joint Agencies should focus on a risk-based baseline security standard that covered entities should have in place, and allow covered entities decide how to best to organize their unique business structures.

***Internal Dependency Management***

The Cyber ANPR outlines steps intended to ensure that a covered entity can detect and manage cyber risks associated with its own internal business assets. It aims to ensure that covered entities continue to assess and improve their cyber risk management abilities. The Joint Agencies outline considerable requirements including maintaining an inventory of all business assets, prioritized based on the assets'

---

[6] *See*, Enhanced Cyber Risk Management Standards, *available at*, https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf

[7] *Id*.

[8] FTC Red Flag Program, available at, https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business

criticality and a complete list of all internal assets and business functions and mappings to other assets and other business flows.[9]

ACLI understands the concerns about cyber risks emanating from possible insider threats or legacy system issues. However, the Joint Agencies' proposed standards are overly comprehensive while also being vague. Their approach would broadly request that covered entities determine the level of criticality of their internal systems. Further, the Joint Agencies' proposed controls do not show how it would prevent issues such as insider threats or issues with legacy systems, especially with covered entities of varying sizes, business models, and system requirements.

The Joint Agencies should work with covered entities to leverage existing processes, many of which already incorporate the data security measures the Cyber ANPR is proposing.

***External Dependency Management***

In its Cyber ANPR, the Joint Agencies outline steps intended to ensure that a covered entity can detect and manage cyber risks associated with outside vendors, including suppliers, customers, and other service providers. The purpose of this section is to continually require covered entities to assess and improve their cyber risk management in relation to external parties. In addition, the Joint Agencies envision that a covered entity can monitor and manage "in real time" external dependencies and trusted connections that support sector critical systems.[10] The Cyber ANPR envisions that covered entities have "complete awareness" of all external dependencies enterprise-wide and be aware of their criticality to the business functions they support.

We have concerns with the prescriptive and overly broad nature of the Joint Agencies' proposed standards. The proposed standard would require covered entities to conduct audit testing on all their outside vendors. Further, the Joint Agencies' assumption that covered entities can be aware in "real time" with a "complete awareness" of all external dependencies does not conform with covered entities' experiences with their third-party vendors, including the level of scrutiny to which such vendors would be willing to agree. Further, testing of additional and alternative solutions for third party vendors would lead to additional and unnecessary burdens on covered entities. Instead, the Joint Agencies' objectives again may be achieved by narrowing the focus and by working through procedures which many covered entities already have in place.

In its Cyber ANPR, the Joint Agencies include cyber risks posed by customers. Customers do not pose a unique threat to systems, and therefore we recommend deletion of that provision. Again, any new requirements should provide a nonprescriptive framework to assist firms in identifying and best protecting their critical systems from external threats. The current proposed approach would require covered entities to divert significant resources away from detecting and responding to potential cyber risks and instead focus on ensuring they have met all their regulatory obligations.

***Incident Response, Cyber Resilience, and Situational Awareness***

In its Cyber ANPR, the Joint Agencies would require entities to ensure that they appropriately plan, respond, contain, and recover from disruptions related to cyber-attacks and continually assess and strengthen their cyber risk management. The Joint Agencies also envision in the Cyber ANPR that covered entities design immense incident response and situational awareness protocols. The Joint Agencies would require covered entities to develop escalation protocols and contagion containment

---

[9] See, Enhanced Cyber Risk Management Standards, *available at*, https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf

[10] *Id*.

procedures and to establish recovery time objectives (RTOs). Further, the Joint Agencies would require resilience strategies for malware and recovery strategies for critical data based on the criticality of the information affected.

The Joint Agencies' proposed standards do not account for the intricacies of the life insurance business model and are overly prescriptive and not risk-based. Specifically, again, life insurance companies do not have the same level of connectivity to the payments, settlement and clearing systems that banks do; instead, they generally access the financial system through intermediaries. Additionally, they are not faced with the same liquidity issues that confront the banking industry. Therefore, the RTO requirements, if any, should apply based on a financial company's impact on the financial system, not simply the size of its consolidated assets.

Further, the Joint Agencies' proposed standards in requiring uniform, defined data standards could potentially lead to increased risk of inherent cybersecurity failings. Since all covered entities would have substantially similar data standards, a malicious cyber-actor would only need to exploit one set of data standards to obtain considerable information. In addition, firms of different sizes would struggle to meet a strict uniform standard. Flexibility in this instance is essential for covered entities of varying nature and size.

Again, many covered entities already have robust policies and dedicated staff in place to deal with issues relating to incident response and cyber resilience. These include incident detection, response, disaster recovery, and business continuity. Further, imposing any set time limit in which to respond to and recover from incidents must be risk-based. Any standards proposed by the Joint Agencies should enable an "all-hands" approach to containment and mitigation rather than diverting important resources to regulatory responses.

Finally, any requirements regarding situational awareness should consider the substantial number of sources on which covered entities rely. These include government agencies, the Financial Services Information Sharing Analysis Center (FS-ISAC), and third party vendors to name a few. Any new standards ultimately put forward by the Joint Agencies should ensure that covered entities may protect themselves and their critical systems and customer information on those systems based on the best information they can obtain from these sources. The Joint Agencies also should ensure a flexible and risk-based standard so that covered entities can continually innovate based on the best information they receive from experts in various cyber fields.

***Conclusion***

In summary, ACLI does not believe it is necessary to subject life insurers covered by the Cyber ANPR to the proposed new enhanced cybersecurity standards, given life insurers' existing robust security policies and procedures and existing oversight of life insurers by state insurance regulators on cyber risk and data security. We also urge the agencies to clarify that life insurers are not "sector-critical" as set forth in the ANPR.

If the Joint Agencies decide to move forward with this proposal, ACLI urges the Joint Agencies to propose risk-based and flexible standards which are not overly bank-centric. We recommend the Joint Agencies consider a principle-based approach, similar to the frameworks that the Joint Agencies reference in the Cyber ANPR. This approach would best position covered entities to focus on preventing and mitigating the effects of a cyber-attack as opposed to unnecessarily diverting resources to respond to regulatory requirements.

We also strongly recommend that the Joint Agencies engage in ongoing dialogue with the industry to address the issues and questions raised in the Cyber ANPR.

We are committed to working with the Joint Agencies on this and other proposals which impact the life insurance industry. If you have any questions, please do not hesitate to contact me.

Sincerely,

Jigar Gandhi