February 17, 2017

Robert deV. Frierson
Secretary, Board of Governors
Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

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

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

Re: Enhanced Cyber Risk Management Standards (Docket No. R-1550; Docket ID OCC-2016-0016)

BSA | The Software Alliance ("BSA")[1] is grateful for the opportunity to provide preliminary feedback on the Advance Notice of Proposed Rulemaking ("ANPRM") regarding proposed Enhanced Cyber Risk Management Standards ("Enhanced

[1] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

Standards").[2] BSA is the leading advocate for the global software industry. Our members provide services across the financial services industry and thus have deep insight into the challenges of securing the industry against the threats that it faces. As global corporations, we also have a shared interest in protecting the integrity of the U.S. financial system. BSA therefore applauds the objective of increasing the operational resilience of financial services firms and will continue to stay engaged as any new potential regulations are further developed.

In issuing this ANPRM, we recognize that the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation ("FDIC"), and the Federal Reserve (collectively, the "Agencies") are seeking feedback on a proposal that is in its early stages of development, and that certain aspects remain fairly conceptual in nature. BSA therefore offers the following four high level recommendations, which we hope will inform the Agencies' efforts to further develop the Enhanced Standards:

- Ensure the Enhanced Standards are Risk-Based, Outcome-Oriented and Technology Neutral
- Align the Enhanced Standards Around the NIST Cybersecurity Framework
- Identify the Scope of Third-Party Services Subject to the Enhanced Standards
- Clarify How the Enhanced Standards Will Apply to Third-Party Services

BSA welcomes the opportunity to work with the Agencies as this proposal is further developed. BSA member companies are happy to lend their expertise and would look forward to engaging in an ongoing dialogue on this topic.

Ensure that the Enhanced Standards are Risk-Based, Outcome-Oriented and Technology Neutral

As the ANPRM notes, the intention of the Enhanced Standards will be to "[increase] the operational resilience and reduce the potential impact on the financial system in the event of a failure, cyber-attack, or the failure to implement appropriate cyber risk management."[3] For the Enhanced Standards to accomplish these objectives, covered entities must retain the flexibility to adopt technological solutions that are best suited to their organization's needs and risk profile. To that end, the Enhanced Standards should avoid overly-prescriptive requirements that could discourage covered entities from availing themselves of the security benefits offered by third-party service providers.

---

[2] Department of the Treasury, Federal Reserve System, and Federal Deposit Insurance Corporation, *Enhanced Cyber Risk Management Standards*, 81 Fed. Reg. 74315 (Oct. 26, 2016) (hereinafter "ANPRM").

[3] *Id.*at 74316.

Certainly, the Enhanced Standards should not create compliance requirements that would have the effect of discouraging the adoption of third-party technologies that could improve the security posture of a covered entity. Rather than representing operational risk, use of other third-party services can help financial services firms increase their resilience. Beyond simply replicating the security controls available in traditional IT environments, third party services can be leveraged to enhance service and network reliability, facilitate automated patching to quickly mitigate the risk of known vulnerabilities, provide redundant data storage, and offer significant resource efficiencies. As such, any new regulation should be drafted in a manner that will allow for the adoption of third-party services that enhance a covered entity's cyber resilience.

BSA members have observed that the financial services industry as a whole has been slow to embrace the efficiency and increased security benefits that can be offered by cloud and other third-party services. This hesitancy may be in part due to a regulatory environment that strongly favors maintaining data within an on-premises IT environment. In a survey conducted by the Cloud Security Alliance, 38% of companies cited regulatory concerns as a barrier to moving workloads to the cloud. Yet, in many instances, better outcomes can be achieved in partnership with cloud providers than by customers on their own. BSA's members have worked hard to develop tools that allow customers to implement the same security controls used within their enterprise within cloud installations and to achieve improved levels of transparency and monitoring. Today, companies can fully realize their security and compliance obligations in partnership with their chosen provider and do so in a way that is transparent to their regulators and other security stakeholders.

Covered entities should not be restrained in their ability to adopt technologies that will improve their security posture. Any new regulations should therefore be drafted with the objective of providing clear guidance that encourages the adoption of third-party services that offer security advantages. To this end, the Enhanced Standards must be technology neutral without creating a preference for one technology deployment model over another.

Align the Enhanced Standards Around the NIST Cybersecurity Framework

The National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF") has become a recognized best practice in the United States for enterprise risk management. Harmonizing around the NIST CSF will reduce the compliance burden placed on regulated entities allowing them to focus time and resources on risk management. Reducing the cost of compliance while achieving the same security outcomes is in the interest of all parties. For these reasons, the recent Presidential Commission on Enhancing National Cybersecurity identified regulatory

harmonization with the NIST CSF among its top recommendations for the incoming Administration.[4]

The five categories or requirements included in the ANPRM should be expressed through the functions, categories, and sub-categories of controls contained in the Cybersecurity Framework. For instance, the activities described under the Cyber Risk Governance and Cyber Risk Management categories both map directly to categories under the Identify function in the NIST CSF. Rather than introducing an artificial dividing line between internal and external dependencies, agencies should promote addressing cyber risk in a holistic manner. Under the NIST CSF, external dependencies must be identified as part of the Identify function and managed in the same manner as other information technology assets throughout the remaining functions. Creating separate standards for internal dependencies vs. external dependencies could unreasonably favor maintaining systems "on premise" even in circumstances where security and resilience advantages can be gained through use of third-party services. The NIST Cybersecurity Framework accounts for the need to manage external dependencies but does so in a way that is technology neutral and thus avoids unduly favoring traditional IT systems over cloud-based service offerings. The remaining categories of incident response, cyber resilience, and situational awareness could also be aligned with the NIST CSF. Incident Response maps directly to the Respond function in the NIST CSF; cyber resilience is both an overall goal of the NIST CSF and an outcome of the Recovery function; situational awareness is well contained in the Detect function.

Use of the NIST CSF as the basis for any new requirements will ensure that covered institutions can more easily identify and work with third-party services that are compliant with the enhanced standards. It will also simplify the work of the agencies in working with other Federal regulators and state regulators to ensure that covered entities do not become subject to multiple, overlapping, and potentially contradictory requirements. By adopting the NIST CSF as the basis for this and other regulatory actions, the Agencies will more easily be able to identify where requirements are already in place and where gaps may exist. As the mapping to the NIST CSF provided by the Federal Financial Institutions Examination Council for its

[4] Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy*, December 1 2015, *available at* https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf ("Action Item 1.4.3: Regulatory agencies should harmonize existing and future regulations with the Cybersecurity Framework to focus on risk management – reducing industry's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation.").

Cybersecurity Assessment Tool demonstrates, financial regulatory requirements can easily be expressed using the NIST CSF.[5]

Identify the Scope of Third-Party Services Subject to the Enhanced Standards

The ANPRM contemplates how the Agencies should ensure that services provided by third-party service providers to covered entities are performed in a manner that will minimize systemic risk. However, as presently drafted, the ANPRM could be read to suggest that the Enhanced Standards will apply to *all* third-party service providers, irrespective of the risk they may pose to the functioning of the financial system. BSA members are confident that this outcome is not the intent of the Agencies but seek clarity on how the scope of the requirements will be limited.

Consistent with the risk-based approach envisioned by the ANPRM, BSA recommends that the Enhanced Standards should apply only to third-party service providers whose services are essential to a covered entity's ability to deliver core banking functions. Section I of the ANPRM appears to contemplate such an approach. There the Agencies explain that points out that "[t]hird parties that provide payments processing, core banking, and other financial technology services…are vital to the financial sector." However, the Enhanced Standards themselves do not appear to be limited to third parties who are performing systemically significant functions on behalf of covered entities.

Because the objective of the ANPRM is to minimize systemic risk to the financial system, it is appropriate that the Enhanced Standards would apply in circumstances where a covered entity is using a third-party to deliver core banking functions, the interruption of which could have systemic risks to critical financial markets. However, third-party service providers who work with covered entities on matters that do not pose systemic risks to the delivery of core banking functions should not be subject to the Enhanced Standards. For instance, there is no such risk associated with providing email-as-a-service or holding human resources data (among many other non-core functions) for covered entities, while there may be for clearing transactions on a cloud-based server. The Agencies should therefore identify the categories of workloads that pose systemic risk to the financial market and extend the Enhanced Standards only to third-parties whose services are vital to a covered entity's ability to perform those specific functions.

[5] While the FFIEC should be applauded for demonstrating how its requirements can be expressed using the NIST CSF, better outcomes for all parties would be achieved by adopting the NIST CSF's lexicon and approach as the basis for any new regulatory effort.

Clarify How the Enhanced Standards Will Apply to Third-Party Services

BSA understands the interest the Agencies have in ensuring that risks are managed both within traditional IT environments and when core banking functions are carried out by third-party service providers. However, BSA members are concerned that the ANPRM lacks guidance about which of the Enhanced Standards would apply to third-party service providers and how they would be made applicable. The Agencies should clarify that only the Enhanced Standards in Category 4, which relate to "External Dependency Management," are relevant to third-party service providers. The Agencies should likewise clarify that covered entities will be responsible for passing along these requirements through contractual arrangements with their third-party service providers.

As drafted, the ANPRM outlines a highly-regimented structure for how entities subject to the regulation would need to be organized for cybersecurity. While that structure may make sense for the "largest and most interconnected" financial institutions under the Agencies' supervision, imposing a risk management structure and organizational model developed for the financial services industry would not be appropriate for the information technology industry.

It would be inappropriate for the Agencies to impose many of the specific requirements contained in Categories 1-3 and 5 of the Enhanced Standards on companies outside of the financial services sector. The risks that a financial services company must be concerned with are different than the risks that a cloud services provider must be concerned with. For instance, requiring that cloud service providers organize themselves internally so that the individuals responsible for managing cyber risk be independent of business units is incompatible with businesses who treat cybersecurity as a core function and enabler of their businesses.

The Agencies should recognize that third-party services operate as seamless extensions of internal IT operations. Covered entities should be focused on monitoring and mitigating risks, not on the internal organization of their third-party service providers. Most enterprise cloud service providers now provide customers with the real-time monitoring capabilities the Agencies envision. Other requirements envisioned by the Agencies simply make no sense for third-party technology providers, such as requirements to have "secure, immutable, off-line storage of critical records" and designation of alternate service providers.

Direct application of requirements to service providers would bring a massive new class of companies under the oversight of the Agencies. Such overreach would not result in better security outcomes. A better approach is to make covered entities responsible for managing the risk from third-parties, passing down the External Dependency Management requirements that are relevant to their vendors via contracts and working with them in a cooperative manner. In developing any new

requirements, the Agencies should recognize that many covered entities rely on the same information service providers. Any new regulatory action should seek to reduce costs of achieving compliance, allowing security spending to be focused on reducing risks. In addition, the Agencies should also be mindful that each covered entity's technology stack may include a range of service providers whose services are layered in a manner that increases overall cyber resilience. Accordingly, the Agencies should ensure that the Enhanced Standards are sufficiently flexible to allow for the continued evolution of technology delivery mechanisms.

Conclusion

We appreciate the opportunity to share our members' perspectives on these important issues. BSA and its members are strongly committed to building strong cybersecurity programs and share the interest of the Office of the Comptroller of the Currency, the Federal Reserve Board, and the FDIC in promoting the resilience of the financial sector. We welcome the opportunity to continue the dialogue on this important topic.

Sincerely,

Christian Troncoso
Director, Policy