From: **Jeremy Dalpiaz**
Date: Mon, Apr 10, 2017 at 11:43 AM
Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Lance Noggle, Jeremy Dalpiaz

Attached, please find a joint comment letter from the Intendent Community Bankers of America and the Credit Union National Association in response to the Request for Comments, "Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity." Please do not hesitate to reach out with any questions.

Thank you,

Jeremy J. Dalpiaz
Assistant Vice President
Cyber Security and Data Security Policy
Independent Community Bankers of America®
1615 L St., NW, Ste 900 | Washington, D.C. 20036 | www.icba.org

[Attachment Copied Below]

April 10, 2017

Via Electronic Submission

Mr. Edwin Games
Cybersecurity and Privacy Applications Group
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Request for Comments, "Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity"

Dear Mr. Games:

The Independent Community Bankers of America (ICBA)[1] and Credit Union National Association (CUNA)[2] appreciates the opportunity to comment on the request for comments entitled, "Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity" ("Proposal"),[3] issued by the Department of Commerce, National Institute of Standards and Technology ("NIST").

Cybersecurity is important for all sectors, including the financial services sector. Community banks and credit unions, including their boards, management and employees recognize and take seriously their responsibility to protect customer/member data and personal information. Beyond existing regulatory and statutory requirements specific to protection of customer/member data and cyber security, the community bank and credit union business models are founded on consumer trust and service. A failure to safeguard customer and member personal information, as well as to safeguard the institution as a whole, would have a significantly negative impact on any community bank or credit union. Compromised customers and members of such institutions have multiple choices in the financial marketplace. Beyond any legal or regulatory requirements, cybersecurity is a business imperative for community banks and credit unions in the digital marketplace, which community banks and credit unions take very seriously.

To provide some background, community banks and credit unions protect institutional and customer data, by employing a multitude of cybersecurity frameworks, tools and assessments based on their risk tolerance, including, but not limited to, the National Institute of

---

[1] The Independent Community Bankers of America®, the nation's voice for more than 5,800 community banks of all sizes and charter types, is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education and high-quality products and services. With 52,000 locations nationwide, community banks employ 760,000 Americans, hold $4.7 trillion in assets, $3.7 trillion in deposits, and $3.2 trillion in loans to consumers, small businesses, and the agricultural community. For more information, visit ICBA's website at www.icba.org.

[2] The Credit Union National Association represents America's credit unions and their more than 110 million members.

[3] Federal Register. 25 January 2017. Vol. 82. No. 15. 8408-8409.

Standards and Technology *Cybersecurity Framework* ("*NIST CSF"*),[4] Control Objectives for Information and Related Technology ("COBIT"), the SANS CIC Critical Security Controls, and the Federal Financial Institutions Examination Council ("FFIEC") *Cybersecurity Assessment Tool ("CAT"*). This is, of course, in addition to the guidance outlined in the *FFIEC Information Technology Examination Handbook* booklets *("IT Handbook")*,[5] the standard by which banks and credit unions are examined on information technology and security. It is not uncommon for community banks and credit unions to employ parts, or multiple parts, of various voluntary frameworks, tools and assessments to provide a tailored cybersecurity program for their institution, based on the institution's size, risk, scope and complexity.

For regulated entities, such as community banks and credit unions, the NIST CSF can serve potentially two purposes: it may serve as the cybersecurity risk policy of the institution in compliance with the IT Handbook examination requirements; or, it may serve as a compliment to another risk framework, such as SANS, COBIT or ISO. For unregulated entities, the Framework provides a baseline method for organizations to establish a cybersecurity risk policy. In this light, ICBA and CUNA support the efforts by NIST to continue to promote the Framework to all sectors, particularly those without a regulatory body to supervise and examine their cybersecurity risk policies.

The Importance of the Voluntary Nature

The voluntary use of the NIST CSF is encapsulated in both Executive Order 13636[6] and the Cybersecurity Enhancement Act of 2014.[7] Due to the voluntary nature of the NIST CSF, ICBA and CUNA support and appreciate the collaborative, iterative process used to gather feedback and the continued development and evolution of the NIST CSF. Maintaining the voluntary nature of the NIST CSF provides community banks and credit unions an option that they can use, if appropriate, based on their business model, online and mobile services, interconnectedness to third parties, technology services and other risk variables. Promoting the voluntary nature of the NIST CSF promotes the adoption of frameworks that best suit an institution based on its risk exposure, such as a small bank selecting to use an industry specific tool like CAT, or a mega, international bank using a combination of both the International Organization of Standardization (ISO 27000 series)[8] and ISACA[9] standards, for example.

The financial services sector, however, is subject to strict examination and supervision of its cybersecurity governance, risk assessment and management, mitigating or compensating controls, risk monitoring and reporting and preparedness. Federal regulators recognize that one size does not fit all when it comes to protecting against cybersecurity threats. In that light, they allow banks and credit unions of all sizes to select the risk management program that best suits their needs in relation to their risk. Therefore, it is important that the prudential banking and credit union regulators do not replace the current policy of permitting institutions to choose the

---

[4] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0*. 12 February 2014. Available at: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[5] FFIEC *IT Handbook* booklets can be found online at: http://ithandbook.ffiec.gov/.

[6] See Federal Register. 19 February 2013. Vol. 78 No. 33. 11739-11744.

[7] P.L. 113-274. 128 Stat. 2971. https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

[8] See https://www.iso.org/isoiec-27001-information-security.html.

[9] See http://www.isaca.org/about-isaca/Pages/default.aspx

framework that works best for their institution. At the same time, by adding additional, and potentially disparate tools, frameworks or requirements to the financial sector, this would not effectively address cybersecurity management preparedness of the financial sector. Requiring the use of one framework over another, for instance, may be overkill for banks with a minimal cybersecurity risk profile while it may serve a large, multi-national institution well.

For the financial services sector specifically, the Federal Financial Institutions Examination Council (FFIEC) IT Handbook, IT Security booklet outlines several frameworks or standards an institution could employ for their information security policy and for the purposes of implementing compensating controls. One of these options is, indeed the NIST CSF, while others include, but are not limited to, COBIT and ISO 27000.

It is therefore critical that any prudential financial regulator that supervises or examines financial institutions for compliance with cybersecurity risk standards not require the use of any one cybersecurity framework, assessment or tool over another, including the NIST CSF. Rather, we strongly support and encourage the continued voluntary nature of the NIST CSF, or other appropriate framework, tool or assessment, as an institution deems fit, dependent upon its risk profile in accordance with guidance issued by the FFIEC.

Harmonization

ICBA and CUNA appreciate that NIST has developed its existing framework and the draft Version 1.1 to ensure it adequately addresses new and evolving threats and can be used broadly. Its application for businesses across many different sectors allows businesses to adopt a voluntary framework with the end goal of increasing cybersecurity preparedness across the board. This is particularly helpful for businesses that are not supervised and examined on their cybersecurity programs.

ICBA and CUNA do not support new or additional cybersecurity regulatory requirements. If the prudential regulators determine that new or additional requirements are necessary, we urge the regulators not to layer additional frameworks on top of existing regulatory guidance and requirements. A better approach would be incorporating any new or additional requirements into, or harmonizing them with existing frameworks or guidance. By adding new frameworks or guidance without incorporating or harmonizing them with existing standards, the prudential regulators risk "framework fatigue" among the financial sector as resources are allocated to reconciling the different approaches rather than combating cyber threats. Moreover, any new or additional requirements would subject community banks and credit unions to new regulatory burdens without any commensurate benefit.

Supply Chain Risk Management

We appreciate the addition of supply chain risk management into the Framework. There has been an increased emphasis in the banking community, for many years, about the role that third-party vendors, and their subcontractors, play in introducing additional risk into interconnected institutions. All sectors and companies should be aware of the risk that can be introduced throughout an organization by the introduction of an additional supplier. However, in

describing the organization-wide approach to managing cyber supply chain risk, NIST suggests that this process is likely handled within a governance structure, such as a risk council. While this may hold true for many large firms, a separate risk council likely does not exist at mid-sized and small firms. We suggest including in the example "Board of Directors or other appropriate governing body".

Measuring and Demonstrating Cybersecurity

While we appreciate the addition of this new section, NIST should consider including recognition of entities that are already subject to strong supervision and examination by regulatory bodies, such as community banks and credit unions. The regulations set out by financial regulators are more specific to the financial sector than the NIST CSF and, indeed, some states require more specific requirements of their regulated banks. Reliance on these examination results should also help instill confidence in those wishing to do business with the regulated, supervised and examined entity.

Conclusion

ICBA and CUNA thank you for the continued collaborative, iterative process used to update the Cybersecurity Framework. Should you have any additional questions, please contact Jeremy Dalpiaz by email or by phone or Lance Noggle by email or by phone.

Respectfully Submitted,

/s/
Jeremy Dalpiaz
AVP, Cyber Security and
Data Security Policy
Independent Community Bankers of America

/s/
Lance Noggle
Senior Director of Advocacy and
Counsel
Credit Union National Association