January 19, 2018

Via Electronic Submission to cyberframework@nist.gov

Ms. Andrea Arbelaez
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Request for Comments, "Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, draft 2."

Dear Ms Arbelaez:

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to comment on the "Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity (a.k.a, draft 2 of the Cybersecurity Framework, version 1.1)" ("Proposal"),[2] issued by the Department of Commerce, National Institute of Standards and Technology ("NIST").

[1] **About ICBA**
The Independent Community Bankers of America®, the nation's voice for nearly 5,700 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 $4.9 trillion in assets, $3.9 trillion in deposits, and $3.3 trillion in loans to consumers, small businesses, and the agricultural community. For more information, visit ICBA's website at www.icba.org.

[2] "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Draft 2." National Institute of Standards and Technology. Revised December 5, 2017. See: https://www.nist.gov/cybersecurity-framework/cybersecurity-framework-draft-version-11.

The Importance of the Voluntary Nature of the NIST Cybersecurity Framework

ICBA appreciates the continued voluntary nature of the NIST Cybersecurity Framework ("Framework").[3] As regulated financial institutions, community banks are subject to a variety of security and privacy requirements, including the implementation of appropriate risk-based controls for managing cybersecurity threats and vulnerabilities.[4] The Federal Financial Institutions Examination Council ("FFIEC") *IT Handbook* ("IT Handbook"), for example, lists the NIST 800 series of publications as one reference that financial institutions can use for this purpose.[5] Others include the Control Objectives for Information and Related Technology ("COBIT"), the IT Infrastructure Library ("ITIL"), International Organization for Standardization ("ISO") 27000 series, industry publications and sources and vendor-provided publications, bulletin boards, and user groups. Community banks employ a multitude of cybersecurity frameworks, tools and assessments based on their risk tolerance, including, but not limited to, the technology frameworks and industry standards listed above. It is not uncommon for community banks 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.

Expansion of the Framework's Applicability Beyond Critical Infrastructure

The creation of the Framework arose from Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."[6]

The Proposal expands the applicability of the Framework beyond critical infrastructure, *to wit*, "[w]hile this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community."[7]

For regulated entities such as community banks, the Framework 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 COBIT or ISO. For unregulated entities, the Framework provides a baseline method for organizations to establish a cybersecurity risk policy. In this light, ICBA supports the efforts by NIST to continue to promote the

---

[3] For ICBA's past letter, please see: http://www.icba.org/docs/default-source/icba/advocacy-documents/letters-to-regulators/2017/cl041017.pdf?sfvrsn=0.

[4] FFIEC IT Handbook, *Information Security* booklet, Section II.C.4. "Control Implementation." https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic4-control-implementation.aspx. September 2016.

[5] Ibid, 13.

[6] Federal Register. Vol 78., No. 33. "Executive Order 13636-Improving Critical Infrastructure Cybersecurity." https://www.gsa.gov/cdnstatic/ATTCH_1_-_CyberEO-FedReg.pdf. February 19, 2013.

[7] "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Draft 2" National Institute of Standards and Technology. Revised December 5, 2017. Page 2. https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_with-markup.pdf.

Framework to all sectors beyond critical infrastructure, particularly those not supervised and examined on their cybersecurity risk policies and practices.

Addition of Two Subcategories

The Proposal includes the addition of two subcategories to the Framework's Core – a subcategory under the "Protect" function, "Identity Management and Authentication and Access Control," which recommends authentication methods commensurate with a given transaction's risk (PR.AC-7);[8] and, a subcategory under the "Analysis" category of the "Respond" function that recommends the establishment of a process to receive, analyze and respond to disclosed vulnerabilities (RS.AN-5).[9] The additions read as follows:

> PR.AC-7: Users, devices, and other assets are authenticated (e.g. single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
>
> RS-AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

Most community banks comply with both standards. First, the use of single- or multi-factor authentication is dependent upon the risk of the transaction. The IT Handbook, both in the *E-Banking* booklet[10] and *Retail Payments* booklet,[11] demonstrate instances when multi-factor authentication would be of benefit over single-factor authentication. With the expansion of the Framework's audience beyond critical infrastructure to "any sector or community,"[12] such modifications will assist those not required to apply this standard in achieving a better security posture of protecting sensitive information. Additionally, community banks regularly engage in information sharing as it pertains to vulnerabilities. They both receive and report out such vulnerabilities to a variety of entities including, but not limited to, the Financial Services-Information Sharing and Analysis Center ("FS-ISAC") and United States Computer Emergency Readiness Team ("US-CERT"), among others.

Financial Services Sector Specific Profile/Harmonization

Finally, it is 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, or

---

[8] "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Draft 2" National Institute of Standards and Technology. Revised December 5, 2017. Page 31. https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf.

[9] Ibid, page 43.

[10] FFIEC IT Handbook, *E-Banking* booklet. https://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/information-security-program/authenticating-e-banking-customers.aspx. August 2003.

[11] FFIEC IT Handbook, *Retail Payment Systems.* https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-e-mobile-financial-services.aspx. April 2016.

[12] Page 2 of Draft 2, Version 1.1 of the Framework.

add to the myriad of tools and frameworks currently in place. This includes the creation of a new, additional "Financial Services Sector Specific Profile," which is currently being discussed between the prudential financial services regulatory agencies, large banks and their trade associations.

If it is determined that a new framework or tool is necessary, it should be voluntary and not a regulatory examination tool. Additionally, it should be consistent with existing frameworks and guidance (such as the FFIEC IT Handbook). A consistent regulatory framework avoids the risk of framework fatigue among community banks, which distracts from their primary business of serving customers. As an example, different requirements throughout the country will create a burden on small institutions. Moreover, requiring differing standards may serve to do little by way of cybersecurity preparedness.

ICBA strongly supports and encourages the prudential banking regulators to continue to view the Framework as voluntary and as one of several methods by which a financial institution may use for its cybersecurity risk purposes.

ICBA thanks you for the continued, collaborative, and iterative process used to update the Framework. Should have any additional questions, please contact me by email at Jeremy.Dalpiaz@icba.org or by phone at 800-422-8439.

Respectfully submitted,

/s/
Jeremy Dalpiaz, Assistant Vice President
Cyber Security and Data Security Policy