National Association
of Federal Credit Unions
3138 10th Street North
Arlington, VA 22201-2149
NAFCU | Your Direct Connection to Advocacy, Education & Compliance

September 9, 2016

Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

Dear Ms. Grayson,

**Re: Comments on Current and Future States of Cybersecurity in the Digital Economy**

On behalf of the National Association of Federal Credit Unions (NAFCU), the only national trade association focusing exclusively on federal issues affecting the nation's federally insured credit unions, I am writing to you regarding the request for information on "Current and Future States of Cybersecurity in the Digital Economy." See 81 Fed. Reg. 52827 (Aug. 10, 2016).

NAFCU supports the ongoing efforts of the Presidential Cyber Commission (the Commission) and the National Institute of Standards and Technology (NIST) to coordinate cross-sector harmonization of the Framework for Improving Critical Infrastructure Cybersecurity (the Framework). NAFCU is optimistic that the Framework's collaborative development, which has so far involved both small and large stakeholders, will continue to improve agency understanding of financial sector capabilities and best practices. NAFCU offers several recommendations that it believes will enhance the effectiveness of the public-private partnership between NIST, stakeholders, and financial regulators.

## Executive Summary

- Cybersecurity Insurance
  - Reducing third-party risk by holding retailers accountable for their data security practices is necessary to lower cybersecurity insurance costs.
- Information Sharing
  - A federal hub for information sharing would enhance analysis of vulnerability information and streamline cross-sector participation.
- Federal Governance
  - NAFCU backs the *Data Security Act*, H.R 2205, because a statutorily authorized framework is necessary to fairly allocate cybersecurity burdens across sectors.

- Cybersecurity Research and Development
    - NAFCU supports efforts to promote multifactor authentication (MFA) in the private sector and believes that requiring retailers to formally adopt MFA would improve overall sector security.

**Cybersecurity Insurance**

Currently, cybersecurity insurance remains expensive for many small credit unions. NAFCU believes that lowering premiums for comprehensive cybersecurity insurance depends on reducing exposure to third-party risk. Credit unions already comply with numerous privacy laws and regulations, but retailers and other merchants are neither subject to similarly comprehensive oversight nor exposed to the risk of severe, regulatory penalties for disclosure of confidential consumer information. NAFCU believes that holding retailers accountable for data security under terms similar to the *Graham-Leach Bliley Act* (1999) would facilitate merchant adoption of best practices, mitigate third party risk, and lower the cost of cybersecurity insurance.

Given the highly interconnected relationship between credit unions and merchants, the current division of data security responsibilities lacks justification. Furthermore, merchants are not subject to periodic examinations to assess their cybersecurity capability—a state of affairs that has allowed retailers like Target and Home Depot to become the weak links in financial sector security. Both NIST and the Federal Financial Institutions Examination Council (FFIEC) warn that exposure to third party vulnerabilities, such as point of sale attacks, has a major impact on cybersecurity risk. Accordingly, the Commission should determine what incentives exist to compel retailers to upgrade their cybersecurity capabilities. NAFCU believes that requiring retailers to purchase cybersecurity insurance would be one method for ensuring that merchants follow the Framework and implement best practices.

The difficulty associated with modeling cybersecurity threats also impacts the availability of affordable cybersecurity insurance. For reasons discussed below, NAFCU believes that centralized information collection would facilitate research of vulnerabilities and improve underwriting standards for cybersecurity insurance providers.

**Information Sharing**

Effective data security requires financial institutions to participate in information sharing and analysis. To date, the FFIEC has encouraged regulated entities to participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC) to develop threat assessments and mitigate cybersecurity risk. The FFIEC's recommendation should be applauded; however, the Commission should explore the benefits of maintaining a hub for information sharing and analysis organizations (ISAOs) to enhance research and collection of vulnerability information.

NAFCU believes that centralized collection of vulnerability information under the direction of a single agency would improve current threat modeling capabilities. The Protected Critical Infrastructure Information (PCII) Program could serve as a blueprint for such consolidation. In fact, the *Cybersecurity Information Sharing Act of 2015*, S.754, already envisions an information sharing hub operated by the Department of Homeland Security for federal entities. The

Commission should determine whether a similar hub for private entities who wish to voluntarily share vulnerability information would be feasible.

Currently there are too many platforms for sharing cyber incident data and coordinating research activities: NIST's National Vulnerability Database, the Department of Homeland Security's National Cybersecurity and Communications Integration Center, the Treasury's Financial Crimes Enforcement Network—just to name a few. While ISAOs such as the Retail Cyber Intelligence Sharing Center (R-CISC) and FS-ISAC have generally been responsive to the need for increased coordination, NAFCU believes that a single platform would lead to faster development of threat responses and provide better awareness of cross-sector vulnerabilities.

**Federal Governance**

*a. A formal process for soliciting small entity participation is desirable.*

NAFCU believes that collaboration between agencies and stakeholders represents the best model for developing the Framework and keeping it up to date. Since the Framework was released in 2014, the coordinated efforts of FS-ISAC, NIST and other information sharing and analysis centers (ISACs) has demonstrated that the financial sector is capable of voluntarily implementing best practices. However, this public-private partnership can be improved. In particular, NAFCU would like the Commission to consider the benefits of a formal process for soliciting input from credit unions and other small financial entities to better inform regulators' understanding of the financial sector's overall "maturity."

Credit unions do not necessarily use the same threat-assessment and monitoring systems available at larger banks due to their inherent risk profile—an umbrella term used by the FFIEC to refer to factors such as institutional size, sophistication, and exposure to third party risk. Credit union input is essential for contextualizing capability information across the financial sector and for developing scalable benchmarks that recognize inherent risk.

Without proper contextualization, regulators may overestimate the financial sector's overall state of maturity, which could reorient the goals of cybersecurity towards exam compliance rather than threat prevention. NAFCU believes that financial regulators should be required to consult with small businesses before identifying particular cybersecurity practices as best practices. As the Financial Services Sector Coordinating Council (FSSCC) has emphasized in previous correspondences with NIST, the "fundamentals of cybersecurity are weakened when…cybersecurity activities are compliance oriented, rather than security oriented."

Additionally, while NAFCU supports current efforts to map cybersecurity capabilities to the Framework, it does not want identification of "best practices" to translate into de-facto regulation. The Treasury's Office of Financial Research has remarked that the Framework is "emerging as a de facto standard for firms seeking guidance in their efforts to counter cyber threats." NAFCU supports the idea of a voluntary framework, but believes that legislation should describe agency authority for memorializing best practices as cybersecurity regulations, and that agencies should also issue their own guidance to clarify how evolving capabilities will be incorporated into examination procedures.

*b. The core strength of the Framework will be impaired if financial regulators are invited to promulgate duplicative or unnecessary standards.*

The root cause behind the recent data breaches at Target, Experian and Home Depot, has been the failure of retailers to manage third party risk. Unfortunately, the Financial Stability Oversight Council (FSOC) has seized upon these high profile breaches to conflate retail sector risk with the need to intensify financial sector regulation. In particular, FSOC has advocated for empowering the National Credit Union Administration (NCUA) to directly supervise credit union vendors such as Fiserv and Jack Henry, who are likely among the least vulnerable sector entities. FSOC's recommendation is counterproductive and unnecessary. Accordingly, NAFCU urges the Commission to clarify how the Framework operates as a collaborative model that promotes self-governance.

Clarification in this area would be particularly useful because FSOC regards the Framework as merely a lexicon of shared terms and not "designed to serve as a regulatory standard." While it is true that the Framework requires agency-specific guidance to operate effectively, downplaying its value as a collaborative tool for voluntary regulation conflicts with guidance in Executive Order 13636. E.O. 13636 clearly states that the Framework will "identify areas for improvement that should be addressed through future collaboration with particular sectors and standards developing organizations." NAFCU believes that characterizing the Framework as an invitation to create novel or duplicative regulations undermines the goal of cross-sector harmonization. The Commission should seek to correct this misapprehension.

NAFCU is also concerned that any plan to grant the NCUA regulatory authority over credit union vendors would contribute to a compliance-oriented cybersecurity environment and frustrate effective risk-prevention. Inviting the NCUA to develop a parallel interpretation of the Framework, on top of what the FFIEC has already developed, would strain its subject matter expertise and potentially cause confusion. NAFCU asks that the Commission encourage NCUA to focus on updating its Examiner's Guide to account for major IT developments in the last 14 years.

Additionally, the costs associated with comprehensive supervision of vendors such as Fiserv would be high and place a significant burden on the National Credit Union Share Insurance Fund. NCUA already has access to the FFIEC's reviews of third-party vendors that serve both banks and credit unions. Subjecting vendors to duplicative standards and further compartmentalizing financial sector cybersecurity is counterproductive; NCUA should rely on the findings of the FFIEC without burdening the data security market with yet another set of standards.

*c. National standards that hold retailers accountable for poor data security are necessary to promote best practices and protect customers.*

NAFCU believes that clearly defined, national standards for cybersecurity are essential to preventing future data breaches and ensuring the safety of confidential consumer information.

NAFCU backs the recently proposed *Data Security Act*, H.R 2205, because a statutorily authorized framework is long overdue. NAFCU also urges the Commission to consider ways to distribute data security burdens more equitably across sectors, such as formally adopting Payment Card Industry Data Security Standards (PCI DSS) as best practices and enforcing retailer compliance through data privacy regulation.

NAFCU also recommends that retailers disclose their data security policies to consumers at the point of sale, report data breaches within a defined timeframe, and identify incidents involving unauthorized exposure of consumer PPI to affected external partners.

*d. The Vulnerabilities Equities Process requires greater transparency.*

NAFCU urges the Commission to develop formal, sector-specific guidance to clarify the scope of the Vulnerabilities Equities Process (VEP) and how it impacts financial regulation. NAFCU believes that more transparent procedures for determining when the government will publicly announce flaws it discovers in financial sector infrastructure would greatly improve consumer confidence in the safety of both banks and credit unions.[1]

Due to the lack of publicly available information, the VEP is poorly understood. Accordingly, guidance is needed to describe the extent to which information sharing and research capabilities will be impacted by the government's decision to keep zero-day vulnerabilities secret. NAFCU is particularly concerned that the usefulness of the Framework, as well as the effectiveness of NIST's collaboration with stakeholders, will be undermined by a poor understanding of how the VEP works.

Additionally, declassified documents describing the VEP do not address when, if ever, previously withheld vulnerability information will be made public, or whether the government intends to retroactively acknowledge that certain information was not shared with FS-ISAC or other ISAOs. Lack of clarity in this area raises a host of problems related to credit union examinations, liability for data breaches caused by undisclosed vulnerabilities, and the safety of consumer information. NAFCU urges that the Commission recommend greater disclosure of the VEP and issue guidance regarding its regulatory impact.

**Cybersecurity Research and Development**

NAFCU supports efforts by the National Strategy for Trusted Identities in Cyberspace to promote adoption of multifactor authentication (MFA) standards in the private sector. Two-factor authentication is currently required for federal agencies pursuant to FISMA and FedRAMP, and NIST has advocated for non-federal entities to continuously improve their e-

[1] *See* National Security Agency, Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process, National Security Agency (Feb. 16, 2010), 2. Obtained under the Freedom of Information Act from National Security Agency and the Office of the Director of National Intelligence; requested as "Vulnerabilities Equities Process" July 1, 2014; received January 14, 2016, available at https://www.eff.org/cases/eff-v-nsa-odni-vulnerabilities-foia

authentication systems.[2] The Commission should explore ways to incentivize merchant adoption of MFA in light of recent data breaches at large retailers.

NAFCU is aware that the National Cybersecurity Center of Excellence (NCCoE) has already proposed a MFA solution for e-Commerce platforms, and would like to see NCCoE's architecture translated into regulation that holds retailers accountable for their data security practices. NAFCU supports current efforts undertaken by the President's National Cybersecurity Awareness Campaign to promote consumer awareness of the benefits MFA, but would prefer that merchants follow binding standards.

**Conclusion**

NAFCU appreciates the opportunity to share our thoughts on the current and future states of cybersecurity. We look forward to continuing to work with the Commission and NIST to identify emerging concerns and best practices. Should you have any questions or would like to discuss these issues further, please feel free to contact me, or Andrew Morris, NAFCU's Regulatory Affairs Counsel at (703) 842-2266 or amorris@nafcu.org.

Sincerely,

Alexander Monterrubio
Director of Regulatory Affairs

[2] *See* NIST-SP-800-63-2, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf