National Association
of Federal Credit Unions
3138 10th Street North
Arlington, VA 22201-2149

NAFCU | Your Direct Connection to Education, Advocacy & Advancement

February 3, 2016

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930,
Gaithersburg, MD 20899

RE: NIST Notice and Request for Information on views on the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

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 write to you regarding the National Institute of Standards and Technology's (NIST) request for information to update its framework to reduce cybersecurity risk against critical infrastructure (Framework). *See* 80 FR 76934 (Dec. 11, 2015). NAFCU appreciates NIST's current voluntary approach to a cybersecurity framework, which has proven to be flexible enough to address circumstances within credit unions of varying size and complexity. We hope that any updates made to the Framework as a result of this comment process will maintain the voluntary structure, while also remaining scalable and flexible in its application to financial institutions of all sizes and structures.

General Comments

Since the release of the NIST Cybersecurity Framework in 2014, credit unions have evaluated their existing cybersecurity programs, internal and external network connections, and risk management programs in order to conform to the Framework and industry best practices. NAFCU supports the current Framework Implementation Tiers that provide a method for credit unions to contextualize and understand different approaches for managing cybersecurity risk. In particular, the Framework Tiers account for varying degrees of processes in place and levels of integration into overall risk management plans. In revising the current framework, we strongly encourage NIST to take into account credit unions of all sizes, in particular small to mid-sized credit unions, with varying levels of technical expertise and cyber risk. As financial regulatory agencies begin to develop their own cybersecurity frameworks and regulatory expectations, NAFCU urges NIST to continue to provide leadership and insight to ensure that the regulators follow the NIST Cybersecurity Framework in a manner that is feasible to implement and adaptive to evolving risks.

FFIEC Cybersecurity Self-Assessment Tool

NAFCU members strive to ensure the security of their systems and sensitive consumer data as the cyber threat landscape continues to evolve. In 2015, the FFIEC released a Cybersecurity Assessment Tool (Assessment), which was developed using the NIST Framework as the core cybersecurity-related principles. NAFCU applauded the collaboration of the FFIEC regulators to release the Assessment, which can be utilized by individual credit unions of all asset sizes to identify their individual risks and assess their cybersecurity preparedness. This voluntary self-assessment tool will be helpful for credit unions of all asset sizes to measure and assess their individual cybersecurity maturity and determine what changes should be implemented based on their internal risk appetite.

NAFCU recommends that NIST carefully study the framework adopted in the Assessment and ensure that the revised NIST framework follow a similar approach, especially since the National Credit Union Administration (NCUA) and other FFIEC regulators will be incorporating this Assessment into the supervisory and examination process for financial institutions. In general, the Assessment has two specific parts, Inherent Risk Profile and Cybersecurity Maturity, which are designed to be completed periodically by credit unions as significant operational and technological changes occur in order to be an effective risk management tool. The Inherent Risk Profile Assessment identifies a credit union's inherent risk, by considering the type, volume, and complexity of a credit union's operations. Second, the Cybersecurity Maturity Assessment determines a credit union's current state of cybersecurity preparedness by analyzing a credit union's behaviors, practices, and processes that impact cybersecurity preparedness within five main domain areas. Once running both parts of the Assessment, a credit union's management can decide what actions are needed either to change the credit union's inherent risk profile or to achieve a desired state of maturity.

Since FFIEC announced the creation of the Cybersecurity and Critical Infrastructure Working Group in June 2013, NAFCU and our members have supported the efforts of this group to enhance communication among the FFIEC member agencies and build on existing efforts to strengthen the cybersecurity activities of other interagency and private sector groups. NAFCU is hopeful that this effort by FFIEC agencies to share cyber threat information will improve the cyber preparedness of the entire financial sector. We are confident that the Assessment tool is the first step toward achieving an industry-wide threat analysis and data.

Legislative Action Needed

NAFCU would like to express our appreciation to NIST for taking a leadership role on cybersecurity. However, NAFCU believes that full cyber and data security for consumers and the financial services industry cannot be achieved without comprehensive legislative measures that promote information sharing and protect against cyber-attacks. Americans' sensitive financial and personally identifiable information will only be as safe as the weakest link in the security chain. While financial institutions, including credit unions, have been subject to federal standards on data security since the passage of the *Gramm-Leach-Bliley Act* (GLBA), retailers and many

other entities that handle sensitive personal financial data are not subject to these same standards. Consequently, they have become the vulnerable targets of choice for cybercriminals.

In 2015, bipartisan legislation was introduced in both the House and Senate – the Data Security Act of 2015 (H.R. 2205/S. 961), that would create a national standard of protection for retailers data breaches. NAFCU has been working with others in the financial services sector to educate lawmakers on the need for these common sense legislative reforms to create a safer environment and hold retailers accountable for data breaches. While NAFCU will continue to advocate for these important legislative measures, we urge NIST to use its expertise to educate lawmakers and regulators about the emerging cybersecurity threats and the need for real-time multi-sector collaboration to prevent consumer data breaches.

Conclusion

While NAFCU and members strongly support efforts to ensure the safety and security of the financial system from cyber threats, the regulatory pendulum post-crisis has swung too far towards an environment of overregulation that threatens to stifle economic growth and financial innovation. Cybersecurity poses a unique threat to individual institutions since it requires management discretion about the credit union's risk appetite and cyber maturity. As such, cybersecurity is not an issue that can be solved with more regulatory red tape. Instead, emerging cyber risks must be addressed by adopting solutions that are scalable and nimble enough to be used both on an institution-level and industry- wide basis to identify and respond to the ever-changing threat landscape.

We look forward to continuing to work with NIST and the FFIEC regulators in order to address how to best secure credit unions and their members against the evolving threats in the cybersecurity space. Should you have any questions or would like to discuss these issues further, please feel free to contact me at ksubramanian@nafcu.org or (703) 842-2212.

Sincerely,

Kavitha Subramanian
Regulatory Affairs Counsel