CUNA
Credit Union National Association

601 Pennsylvania Ave., NW
South Building, Suite 600
Washington D.C 200004-2601

Phone: 202-638-5777
Fax: 202-638-7734

Via Electronic Submission to cyberframework@nist.gov

February 9, 2016

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

RE: Views on the Framework for Improving Critical Infrastructure Security

Dear Ms. Honeycutt:

The Credit Union National Association (CUNA) appreciates the opportunity to provide comments in response to the notice and request for information published in the Federal Register, Vol. 80, No. 238, on December 11, 2015, by the National Institute of Standards and Technology ("NIST") regarding views on the "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0" (the "Cybersecurity Framework"). CUNA represents America's credit unions and their more than 100 million members.

CUNA supports NIST's goals to collect information about the use of the Cybersecurity Framework and the possible need for update. The Cybersecurity Framework should continue to recognize existing, robust data security requirements and standards that apply to financial institutions. Credit unions and other financial institutions should not be subject to additional prescriptive requirements, as they are already subject to a risk-based approach to manage cyber threats. We also urge additional coordination between the public and private sectors on cybersecurity.

CUNA is submitting this comment letter in addition to working with The Financial Services Sector Coordinating Council ("the FSSCC"), which CUNA is a participating member, in developing a comment letter that addresses the request for information more broadly.

In addition to the thoughts represented in the FSSCC letter, we have the following comments to the request for information.

I. What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cyber security Enhancement Act of 2014?

Credit unions are subject to diverse regulations and standards, including those required by the Sarbanes-Oxley Act, Payment Card Industry Data Security Standard (PCI DSS), the Federal

Financial Institutions Examination Council (FFIEC), the Graham Leach Bliley Act, the Fair and Accurate Credit Transactions Act and many separate privacy rules and local government rules depending on the operating environment of the credit union being examined or audited. To meet these diverse requirements, credit unions often must use many different vendors to conduct risk assessments to ensure compliance.

Meeting the requirements of the various regulations is costly and there is often conflict between the different rules and requirements, which leaves a credit union in the undesired position of being forced to choose which conflicting regulation, requirement or standard to comply with. A task force to review each of these regulations and their stated purposes with respect to the NIST CORE requirements would be helpful to reconcile conflicting regulations and requirements with prioritization of these in a manner that states clearly not only the desired outcome of the practice but the risk factors of not adhering to the practice. This would greatly reduce the number of risk assessments that are performed by the credit union, reduce confusion and result in stronger security.

II. What steps could the U.S. government take to increase sharing of best practices?

Cyber security is a moving target, particularly in the financial services industry. Increasingly, the threats related to the financial industry are not only criminal but are also state sponsored. The Federal Bureau of Investigation (FBI) has sponsored an association called InfraGard that is dedicated to sharing information and intelligence to prevent hostile acts. This program is the only known outlet for credit unions to determine global financial threats with information supplied by the United States. The U.S. government should take a stronger position to inform the private sector, particularly financial institutions, of known state sponsored threats. This would especially be useful for smaller institutions which many times lack either the technical talent or resources to keep up with the changing landscape of the threats. If more information could be shared, as well as remedies from other larger financial institutions, this would enable the smaller institutions to work together to implement similar solutions. It is just a matter of time until the state sponsored actors turn their attention to easier targets with fewer resources. NIST should include regular updates to the CORE that are specific to the types of threats that are being watched by the U.S. government and include remedies and opportunities for shared resources with the government to protect the members of credit unions from cyber terrorism.

III. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

Yes. However, the type of organization will be important. The organization should be a standards-based organization with no examination or auditing authority so that prudential regulators that know credit unions best retain examination authority. The type of organization is of crucial importance to credit unions that have great variability in size and operations. An entity would need to understand credit unions and have the ability to factor this understanding into the framework.

IV. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cyber security standards, guidelines, and practices within the United States and globally?

The following factors should be considered:

1. The entity should be standards-based with experience in keeping a standard up to date and facilities and infrastructure to collect feedback in real time on the standards and deliver real time updates.
2. The entity should have a global footprint so it can factor in foreign attacks and translate and disseminate information for the U.S. as well as share our best practices with our global allies.
3. The entity should have access to FBI InfraGard, the Department of Homeland Security, the National Security Agency and other government entities who have access to information to improve the framework against changing global attack vectors.
4. The entity should have background in financial security as well as general infrastructure security.
5. Continued development of tools should be available to the private sector to promote the framework. The entity should foster this within the security community.
6. The entity should also evolve into a source of data that is required to be implemented by organizations deemed critical to the U.S. infrastructure. This would include but not be limited to:
    a. A federated internet protocol (IP) black list
    b. A federated attack vector signature list
    c. Any direct threats to credit unions that are discovered by the U.S. regardless of how credible the threat is.
7. The entity should be able to cross-reference global infrastructure attacks and provide predictions on known criminal or state sponsored activity.
8. The entity should work with security vendors to improve the position of the framework and core by holding workshops for the vendors and including them in discussions of changes to the framework.
9. The entity should improve audit guidelines and provide certification for audit firms to guarantee consistency of audits across the country as it relates to implementing the framework. This can serve as a means of income for the entity.
10. The entity should work with the major data centers and carriers to help monitor threats and help coordinate defenses in terms of updating regulation in light of either past attacks or pending attacks.

Thank you for the opportunity to comment on this request for information. If you have any question concerning this letter, please feel free to contact me.

Sincerely,

Lance Noggle,
Senior Director of Advocacy and Counsel