3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

January 19, 2018

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

RE: Comments on the Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Dear Mr. Games:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only national trade association focusing exclusively on federal issues affecting the nation's federally-insured credit unions, I would like to share with you NAFCU's thoughts on Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity (the Framework) published by the National Institute of Standards and Technology (NIST). NAFCU supports NIST's efforts to update the Framework and has determined that the changes in revised Version 1.1 (Draft Two) are effective at clarifying key cybersecurity concepts.

General Comments

As highly regulated financial institutions, credit unions must satisfy rigorous data security standards prescribed by the *Gramm-Leach-Bliley Act of 1999*. The National Credit Union Administration (NCUA) regularly examines credit unions to ensure compliance with these standards and has relied on NIST's guidance to develop its IT examination procedures. Many NAFCU members have benefited from NIST's promulgation of the Framework by using its concepts and terminology to approach data and cybersecurity problems through a common vernacular.

In addition, NIST's Framework has aided in the development of the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT), which has served as an informative benchmark for credit unions and other financial institutions. The NCUA indicated in its 2018 Supervisory Priorities that its future cybersecurity examination procedures will substantially mirror the CAT's structure, which is itself a reflection of the Framework. NCUA plans to adopt the "Automated Cybersecurity Examination Tool" (ACET) this year to establish a baseline maturity level for the largest and most complex credit unions.

NAFCU also believes that continuous refinement of the Framework over time will help non-regulated entities achieve the high standards set by financial institutions and ensure that regulatory expectations are aligned with objective, risk-based principles.

Draft Two Comments

NAFCU believes that NIST's clarifications regarding the relationship between tiers and maturity level are necessary to inform users and regulatory agencies adopting the Framework that an organization's desired maturity level should be risk-based and aligned with cost benefit analysis. This distinction is essential given that there is no one-size-fits-all approach to cybersecurity. NIST should seek to advise agencies adopting the Framework that the declarative statements in each Tier are not intended to designate discrete maturity levels. In addition, NAFCU encourages NIST to describe how different industry environments influence the cost-benefit analysis that informs an organization's Target Profile. NAFCU believes that illustrative examples of industry exposure to regulatory and legal factors would elucidate how Tier selection depends on business context.

NAFCU supports revisions to Section 4.0 that replace discussion of metrics and measures with a more holistic view of how organizations employ measurements as part of the Framework process. NAFCU agrees that leading measurements will typically be more important for the purpose of accomplishing future reduction in risk. Likewise, NAFCU concurs that a disproportionate emphasis on lagging measurements—which may be prevalent in a compliance-oriented environment—will be less useful and possibly detrimental. For example, introducing too many regulator-specific measurements to document maturity level could increase operational expenses without a corresponding improvement in measurement accuracy or risk reduction. To offset the cost of an ever expanding list of measurements examined by regulators, NAFCU agrees with NIST that any measurement system should be designed with business requirements and operating expenses in mind.

NAFCU also asks that NIST discourage agencies from adopting binary, declarative statements to assess cybersecurity maturity. As evidenced by the CAT's compensating controls option, simple yes or no answers to declarative statements do not adequately reflect the risk-based nature of the Framework and may incentivize institutions to adopt controls that are poorly aligned with cost-effective risk reduction strategies. Accordingly, NAFCU urges NIST to include discussion of how the use of yes/no declarative statements for assessing cybersecurity maturity may be less than beneficial or possibly misleading. Such discussion could also clarify NIST's advice regarding avoidance of "artificial indicators" to evaluate cybersecurity risk management.

Lastly, NAFCU supports the new draft language which emphasizes the utility of information sharing to improve threat intelligence and better understand the impact of cybersecurity events. However, NAFCU would caution against formalizing these requirements in a way that suggests organizations have a duty to share information externally.

Conclusion

NAFCU recognizes that the Framework has proven influential in harmonizing government cybersecurity standards and encourages NIST to continue to update the Framework as necessary—bearing in mind that the successful adoption of the Framework is largely attributable to its outcome-based approach and voluntary nature. NAFCU believes that NIST should also work with other regulators and industry stakeholders to ensure that that the Framework retains its risk-based focus. As noted in the Framework itself, there is no one-size-fits-all approach to cybersecurity. Accordingly, NAFCU asks that NIST play a role informing regulators of the perils of adopting cybersecurity "best practices" as de-facto regulation before there is sufficient time to comment on whether such practices are necessary or beneficial in all contexts.

NAFCU appreciates the chance to submit comments regarding NIST's proposed update to the Framework. Should you have any questions or concerns, please do not hesitate to contact me at amorris@nafcu.org or (703) 842-2266.

Sincerely,

Andrew Morris
Regulatory Affairs Counsel