From: **Andrew Morris**
Date: Fri, Apr 7, 2017 at 3:08 PM
Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

NAFCU's Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity.

Organization Name: National Association of Federally-Insured Credit Unions

Submitter Name: Andrew Morris

Andrew Morris
Regulatory Affairs Counsel
National Association of Federally-Insured Credit Unions
3138 10th Street North, Arlington, Virginia 22201
www.nafcu.org

[Attachment Copied Below]

April 7, 2017

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

RE: Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity

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 the proposed update to the Framework for Improving Critical Infrastructure Cybersecurity (the Framework) published by the National Institute of Standards and Technology (NIST). NAFCU fully supports NIST's efforts to revise the Framework and finds that Version 1.1 offers both improved utility and better explanations for key cybersecurity concepts.

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. NAFCU 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.

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. NIST's Framework's has also 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 also indicated in a September 2016 Board Meeting that its future cybersecurity examination procedures may substantially mirror the CAT's structure, which is itself a reflection of the Framework.

NAFCU believes that NIST's clarifications regarding supply chain risk management and the use of the Framework's implementation tiers will help credit unions understand risks relative to other financial sector stakeholders. Additionally, the proposed use of "metrics" and "measures" is commendable for its forward-looking emphasis; specifically, the stressed importance of correlating cybersecurity policies with business results. NAFCU agrees that the cause and effect relationship between cybersecurity and business outcomes is an important data measure; however, quantifying this relationship should be an activity undertaken voluntarily by organizations that use the Framework. NAFCU does not believe that the metrics and measures portion of the Framework is well-suited for compliance-oriented credit union examinations. For example, introducing too many regulator-specific metrics could increase operational expenses without a corresponding improvement in measurement accuracy or organizational resilience. To offset the risk of an ever expanding list of

metrics examined by regulators, NAFCU agrees with NIST that any measurement system should be designed with business requirements and operating expenses in mind.

NAFCU recognizes that the Framework has proven influential in harmonizing government cybersecurity standards and encourages NIST to continue to update the Framework "core" 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 continue to work with other regulators and industry stakeholders to clarify how the Framework should be used or adopted, and emphasize that there is no one-size-fits-all approach to cybersecurity.

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.

Sincerely,

Andrew Morris
Regulatory Affairs Counsel