



Credit Union National Association

cuna.org

601 Pennsylvania Ave., NW | South Building, Suite 600 | Washington, DC 20004-2601 | **PHONE:** 202-638-5777 | **FAX:** 202-638-7734

Submitted via email: csfcomments@nist.gov

December 13, 2013

Information Technology Laboratory
Attn: Adam Sedgewick
National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick:

This comment letter represents the views of the Credit Union National Association (CUNA) regarding the National Institute of Standards and Technology's (NIST's) request for comment on its preliminary "critical infrastructure" cybersecurity framework. By way of background, CUNA is the largest credit union advocacy organization in this country, representing state and federal credit unions, which serve about 99 million members. This letter supplements our letter on April 8, 2013 to NIST regarding the previous information request on the framework. CUNA, along with the Financial Services Sector Coordinating Council (FSSCC), also appreciates the meeting with our group in August with you, NIST Director Patrick Gallagher, and other senior staff to discuss the framework.

CUNA supports NIST's goals to develop a "critical infrastructure" cybersecurity framework. The framework should recognize existing, robust data security requirements and standards that apply to financial institutions. As NIST proceeds with finalizing and implementing the framework, we urge NIST to coordinate closely with all financial regulators, including the National Credit Union Administration (NCUA), to ensure the framework is consistent with, and does not expand the scope of, existing rules and regulations. We also urge additional coordination between the public and private sectors on cybersecurity.

Credit unions and other financial institutions are already subject to a risk-based approach to manage cyber threats, and should not be subject to additional prescriptive requirements. The existing cybersecurity framework for the financial services sector is risk-based and dynamic. It was designed to address a wide range of existing and emerging



OFFICES: | WASHINGTON, D.C. | MADISON, WISCONSIN

cybersecurity risks, often in a collaborative way. Examples of effective collaboration within the financial sector include information sharing during Hurricane Sandy and other storms, recent Distributed-Denial of Service (DDoS) and internet threats, and on Y2K and business continuity issues. While a limited number of financial institutions, including credit unions, have been the target of data breaches and cyber attacks, the financial services sector and its systems continue to evolve and adopt defensive measures to mitigate such these risks.

As NIST continues to coordinate with private and public stakeholders, it should focus on maximizing the ability of the federal government to address communications and other gaps that undermine the ability of sectors such as financial institutions to protect themselves.

NIST Should Coordinate Closely with Financial Regulators to Ensure Framework is Consistent With, and Does Not Expand Scope of, Existing Rules and Regulations

CUNA continues to urge NIST to coordinate closely with all financial regulators, including the NCUA and the Federal Financial Institutions Examination Council (FFIEC), to ensure the framework is consistent with existing rules and regulations.

We agree with NIST that the framework should “be designed for compatibility with existing regulatory authorities and regulations,” which will promote “technical innovation and account for organizational differences” and “not prescribe particular technological solutions or specifications.”

NIST should make it a priority to ensure that its framework is consistent with existing legal authorities and does not impose any new requirements on financial institutions, which are already overwhelmed by current compliance burdens. The White House Executive Order (EO) and Presidential Policy Directive on cybersecurity issued in February 2013 is consistent with existing, applicable law and does not provide new legal authority for federal agencies on “critical infrastructure” cybersecurity other than that which is provided under existing law.

Further, under the EO, the Department of Homeland Security (DHS) Secretary in coordination with sector-specific agencies, will establish a voluntary program to support the adoption of the cybersecurity framework by “critical infrastructure” entities, as well as other interested entities. NIST should coordinate with regulators and stakeholders to ensure that any voluntary “critical infrastructure” initiatives remain voluntary, and do not result in additional requirements on entities such as credit unions.

Privacy Rights and Civil Liberties Should Be in Context of “Critical Infrastructure” Cybersecurity

While we agree the NIST framework should provide appropriate protections on individual privacy and civil liberties, as well as business confidentiality, in the context of “critical infrastructure” cybersecurity, we share similar concerns with the financial services sector that the preliminary framework lists a very detailed and potentially prescriptive set of steps regarding privacy and civil liberties.

The framework should not expand the scope of privacy and civil liberties beyond “critical infrastructure” cybersecurity activities, which could cause potential conflicts with existing laws, regulations, and other rules that currently apply to financial institutions. Also, we share concerns that an expansion of privacy and civil liberties within the framework would also impede the broader adoption of the framework.

NIST should limit the scope of the proposed steps associated with business confidentiality, individual privacy, and civil liberties to be applicable only within the context of “critical infrastructure” cybersecurity. In addition, NIST should ensure the framework is fully consistent with existing rules that apply to financial institutions for these areas.

Credit Unions and Financial Institutions Are Already Subject to Robust Cybersecurity Requirements

Credit unions and other financial institutions are already subject to very robust cybersecurity and data security requirements. This includes the Gramm-Leach-Bliley Act (GLBA) and other applicable data security laws, regulations, and standards from the FFIEC and NCUA. The FFIEC is a formal interagency body of financial regulators, including NCUA, which prescribes uniform principles, standards, and report forms for the federal examination of financial institutions, including credit unions. We have included a more detailed discussion on data security requirements for credit unions in our April 8, 2013 letter.

The FFIEC already sets risk-based standards for financial institutions, including credit unions, regarding their information systems and minimum control requirements, as well as a layered approach to managing information risks. A risk-based approach provides the financial sector with effective, flexible methods to manage existing and novel cyber threats, and supports NIST’s goals for a prioritized, flexible, and cost-effective approach. In addition, a risk-based approach should account for the entity’s complexity, size, and data use.

Further, for other entities outside of the financial sector, which do not currently fall under the framework, we also encourage NIST to assess fully the extent to which new or revised standards are needed for such entities.

NIST Should Continue to Coordinate with Public and Private Stakeholders

CUNA appreciates that NIST has coordinated with public and private stakeholders on the cyber framework, including: releasing several drafts of the framework for public comment; meeting with stakeholders, including the financial services sector; and holding a series of workshops for relevant stakeholders.

We encourage NIST to continue to coordinate on framework developments and potential updates in partnership with public and private stakeholders. By working with the Department of Homeland Security (DHS) and national intelligence agencies, sector-specific agencies, including the U.S. Treasury, NCUA, and other regulators; the FSSCC and other sector-coordinating councils; and CUNA and other trade associations, NIST will be better able to identify, refine, and guide the many interrelated cybersecurity considerations from all key sectors. More coordination is also needed between national enforcement and intelligence-gathering agencies to help identify potential threats.

Finally, NIST and other government entities should focus on cybersecurity education and providing access to timely information, so public and private stakeholders are informed on cyber threats and can take steps to protect their interests.

Thank you for the opportunity to comment on the NIST preliminary cyber framework. If you have any questions concerning our letter, please feel free to contact CUNA SVP and Deputy General Counsel Mary Dunn or me at (202) 508-6733.

Sincerely,

A handwritten signature in blue ink that reads "Dennis Tsang". The signature is fluid and cursive, with the first name "Dennis" and last name "Tsang" clearly legible.

Dennis Tsang
CUNA Assistant General Counsel