CUNA
Credit Union National Association
601 Pennsylvania Ave., NW | South Building, Suite 600 | Washington, DC 20004-2601 | PHONE: 202-638-5777 | FAX: 202-638-7734
cuna.org

Submitted via email: cyberframework@nist.gov

April 8, 2013

Diane Honeycutt
National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Developing a Framework to Improve "Critical Infrastructure" Cybersecurity

Dear Ms. Honeycutt:

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 information on developing a framework to improve "critical infrastructure" cybersecurity. By way of background, CUNA is the largest credit union advocacy organization in this country, representing approximately 90% of our nation's 7,000 state and federal credit unions, which serve about 96 million members.

CUNA supports NIST's goals to develop a framework to improve "critical infrastructure" cybersecurity. The cybersecurity framework should 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.

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 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.

This is not to mask, however, the fact that a limited number of financial institutions, including credit unions, have been the target of data breaches

and cyber attacks. These problems do not mean that more regulation in this area is required for financial institutions. On the contrary, financial institution systems have been tested like few others, and are probably ahead of some other sectors in the evolution and adoption of defensive measures. Experience does tend to confirm that more coordination is needed between national enforcement and intelligence-gathering agencies to help identify potential threats. As NIST works with these agencies and coordinates 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. We also encourage NIST to assess fully the extent to which new or revised standards are needed for other entities outside of the financial sector, which do not currently fall under our framework.

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 Federal Financial Institutions Examination Council (FFIEC) and the National Credit Union Administration (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 agree with NIST that the framework should "be compatible with existing regulatory authorities and regulations," which will promote innovation, and "not prescribe particular technological solutions or specifications." As NIST Undersecretary Dr. Patrick D. Gallagher noted in his written testimony for the March 2013 Senate hearing on cybersecurity, private entities are already supporting critical infrastructure and "should not be diverted from those efforts through new requirements."

The FFIEC sets risk-based standards for financial institution information systems, regarding 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.

The Government Accountability Office (GAO) has also outlined the robust cybersecurity of the financial services sector. As noted in the December 2011 GAO Report on critical infrastructure cybersecurity, the financial

sector's regulations, guidance, and examination standards are substantially similar to the NIST Special Publication 800-53, mapping to all applicable recommended controls for federal information systems.[1] Another recent GAO report in February 2013 showed that that depository institutions in the banking and finance sector are already required to meet mandatory cybersecurity standards established by federal regulations and as a sector, banking and finance was only one of seven sectors that listed cybersecurity guidance in its sector-specific critical infrastructure plan issued by the Department of Homeland Security (DHS) and the U.S. Treasury.[2]

NIST Should Coordinate "Critical Infrastructure" Cybersecurity with Public and Private Stakeholders

This request for information provides a positive, initial step on the coordination of a framework to implement the White House Executive Order (EO) and Presidential Policy Directive on cybersecurity issued in February 2013, but NIST should coordinate "critical Infrastructure" cybersecurity initiatives in partnership with public and private stakeholders going forward.

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 Financial Services Sector Coordinating Council (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.

The FSSCC plays an important role in coordinating the financial sector's critical infrastructure efforts. Members of the FSSCC include CUNA and over 50 financial service entities and associations. The FSSCC works closely with the Financial and Banking Information Infrastructure Committee (FBIIC), which coordinates the government's critical infrastructure efforts, and includes the U.S. Treasury, NCUA, and others.

The cybersecurity framework should also provide protections on business confidentiality, individual privacy and civil liberties. NIST should coordinate with stakeholders on these important issues, in addition to data and information security goals.

---

[1] GAO, Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use, GAO-12-92 (Washington, D.C.: December 9, 2011).

[2] GAO, National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, GAO-13-187 (Washington, D.C.: February 14, 2013).

Further, 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.

Cybersecurity Framework Should Be Consistent with Existing Law

The EO 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. NIST should make it a priority to ensure that its framework is consistent with existing legal authorities and does not impose any new legal requirements on financial institutions, which are already overwhelmed by current compliance burdens.

Voluntary Critical Infrastructure Program Should Be Voluntary

Under the EO, the 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 stakeholders to ensure that any voluntary "critical infrastructure" initiatives remain voluntary, and do not result in additional requirements on entities such as credit unions.

Further Discussion on Data Security for Credit Unions

NCUA regulates and implements data security requirements and standards for credit unions, as do the banking regulators of the FFIEC for banks. These data security requirements and standards include the federal laws of GLBA, FCRA, and Right to Financial Privacy Act (RFPA), as well as state laws and other rules. Other standards apply to financial institutions, such as the Payment Card Industry Data Security Standards (PCI-DSS) on payments card data security. Also, NCUA has published agency Letters to Credit Unions, Regulatory Alerts, Legal Opinion Letters, and other guidance in response to data security, cybersecurity, and consumer protection laws.

Credit unions are subject to data security requirements under § 501(b) of the GLBA and part 748 of the NCUA's regulations. NCUA requires credit unions to establish a comprehensive data security program addressing the safeguards for member and customer records and information. These safeguards are intended to ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against any unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer. Credit unions are also required to develop and implement risk-based response

programs to address instances of unauthorized access to member information. Regarding reporting on data breaches, credit unions have to file a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network (FinCEN) in the event of an attack that accesses consumer data or critical institutional data.

In addition, under part 716 of NCUA's regulations on the use of customer and member non-public personal information, credit unions must comply with requirements on prohibitions on sharing of account numbers, privacy notices to members and customers, and when applicable, a conspicuous notice that explains the right to "opt out" of sharing non-public personal information with certain nonaffiliated parties. Other provisions include a prohibition on sharing account numbers with third parties for marketing purposes, and limitations on the re-disclosure, and reuse of information with nonaffiliated third-parties.

Further guidance on developing cyber threats is applicable to credit unions. As a recent example, in February 2013, NCUA issued guidance on Distributed-Denial of Service (DDoS) attacks to identify appropriate policies and procedures for credit unions. Credit unions should: perform risk assessments to identify risks associated with DDoS attacks; ensure incident response programs include a such attacks; and perform ongoing third-party due diligence to identify and manage risks. Financial institutions should also follow regulations on internet and data security, as well as FFIEC guidance on internet authentication.

NCUA and federal banking regulators have developed and published additional information security requirements which cover specific threats and mitigation of identified cyber risks. The FFIEC has issued specialized IT handbooks on cybersecurity for depository institutions, including credit unions. These 11 separate booklets are very similar to the cybersecurity guidance for federal agencies, and cover areas such as : 1) audits, 2) business continuity, 3) development and acquisitions, 4) electronic banking, 5) information security, 6) management, 7) operations, 8) outsourcing technology, 9) retail payment systems, 10) supervision of technology providers, and 11) wholesale payment systems. These booklets are incorporated into NCUA's examination practices for credit unions.

The methodologies that NCUA and federal banking regulators use to provide oversight and supervision include periodic examinations, self-reporting, and other administrative and legal supervisory actions to enforce compliance. Enforcement under the GLBA and NCUA's regulations are through NCUA's supervision and enforcement actions for federal credit unions, or the state supervisory agencies for federally-insured state-chartered credit unions. Additionally, the Federal Trade Commission has enforcement authority for compliance with these

requirements for other state-chartered credit unions. NCUA's examiners use Automated Integrated Regulatory Examination Software (AIRES) consisting of multiple information technology (IT) examination questionnaires to assist with reviewing a credit union's IT systems.

Thank you for the opportunity to comment on this request for information. 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,

Dennis Tsang
CUNA Assistant General Counsel