March 7, 2013

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

Executive Summary

- The National Institute for Standards and Technology (NIST) has issued a request for information on the coordination of a "critical infrastructure" cybersecurity standards framework (framework), as one of the initial steps of the White House Executive Order (EO) and Presidential Policy Directive (PPD) on cybersecurity. The framework will consist of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks for the U.S.
- Specifically, this request for information will help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop the U.S. cybersecurity framework.
- NIST intends to gather information from all diverse sectors of the U.S. economy, including the 16 "critical infrastructure" sectors identified by the PPD, such as dams, healthcare, food, financial services, water, and IT.
- The goals of the framework development process will be to:
    1. Identify existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable;
    2. Specify high-priority gaps for which new or revised standards are needed; and
    3. Collaboratively develop action plans by which these gaps can be addressed.
- Credit unions should continue to follow current data security and cybersecurity rules, such as rules from the National Credit Union Administration (NCUA) and Federal Financial Institution Examination Council (FFIEC), and the Gramm-Leach-Bliley Act.
- CUNA continues to assess the impact of the "critical infrastructure" cybersecurity framework; we are interested in your feedback if you have any concerns with potential effects on credit unions.
- Comments for the request for information are due to NIST by April 8, 2013; **please submit your comments to CUNA by March 25, 2013.**
- Please e-mail your comments to CUNA Assistant General Counsel for Regulatory Research Dennis Tsang at dtsang@cuna.com and CUNA SVP and Deputy General Counsel Mary Dunn at mdunn@cuna.com.

- CUNA continues to work with regulators, the Financial Services Sector Coordinating Council (FSSCC), BITS, and others to emphasize that the cybersecurity framework should recognize existing, robust data security standards that are applicable to financial institutions, including credit unions, and that credit unions should not be unduly impacted from the cybersecurity framework.
- For further details, please visit the Federal Register notice on the request for information.

Background and White House Executive Order on Cybersecurity

On February 16, 2013, the White House released an Executive Order (EO) on "critical infrastructure cybersecurity" in the U.S., and a related Presidential Policy Directive (PPD). The EO includes a broad, general framework intended to improve "critical infrastructure" cybersecurity coordination and information sharing among government agencies and the private sector, as well as a process for a voluntary cybersecurity program for critical infrastructure entities. The EO is consistent with existing, applicable law and does not provide new legal authority.

The Department of Homeland Security will coordinate with sector-specific agencies, such as the U.S. Treasury for the financial services sector, which will coordinate with financial regulators, including NCUA.

Under the EO, "critical infrastructure" is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The scope of what is considered "critical infrastructure" is not specifically defined, and could potentially include the power grid, financial market exchanges, and telecommunications networks.

As part of the new cybersecurity framework, NIST will coordinate a cybersecurity standards framework. This request for information will help NIST with the coordination.

Goals of New Cybersecurity Framework

NIST believes the U.S. cybersecurity framework should have a number of general properties or characteristics. The framework should include flexible, extensible, scalable, and technology independent standards, guidelines, and best practices, that provide:

- A consultative process to assess the cybersecurity-related risks to organizational missions and business functions;
- A menu of management, operational, and technical security controls, including policies and processes, available to address a range of threats and protect privacy and civil liberties;
- A consultative process to identify the security controls that would adequately address risks that have been assessed and to protect data and information being processed, stored, and transmitted by organizational information systems;

- Metrics, methods, and procedures that can be used to assess and monitor, on an ongoing or continuous basis, the effectiveness of security controls that are selected and deployed in organizational information systems and environments in which those systems operate and available processes that can be used to facilitate continuous improvement in such controls;
- A comprehensive risk management approach that provides the ability to assess, respond to, and monitor information security-related risks and provide senior leaders/executives with the kinds of necessary information sets that help them to make ongoing risk-based decisions; and
- A menu of privacy controls necessary to protect privacy and civil liberties.

Questions to Consider Regarding the Request for Information – For the full list of 30 questions from NIST, please refer to the Federal Register request for information.

1. Current Risk Management Practices - NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity.
    - As a credit union, what do you see as the greatest challenges in improving "critical infrastructure" cybersecurity?

      _____
    - How does your senior management oversee your cybersecurity policies / procedures?

      _____
    - To what extent is cybersecurity incorporated into your enterprise risk management?

      _____
    - What existing standards, guidelines, best practices, and tools are credit unions using to understand, measure, and manage risk?

      _____
    - What performance goals have you adopted to ensure you can provide essential services to your members while managing cybersecurity risks?

      _____
2. Use of Existing Frameworks, Standards, Guidelines, and Best Practices - NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including from government regulators, industry associations, and others.
    - Are there limitations on current security standards that expose or increase cybersecurity risks?

      _____
    - What modifications could make these standards more useful?

      _____

3. Specific Industry Practices – NIST believes specific financial services industry practices include: separation of business from operational systems; use of encryption and key management; identification and authorization of users; asset identification and management; monitoring and incident detection tools and capabilities; incident handling policies and procedures; mission/system resiliency practices; security engineering practices; and privacy and civil liberties protection.
    - Which current practices are most important for "critical infrastructure" purposes?
      _____
    - Which of these practices are the most difficult to implement?
      _____
    - Do you have a formal escalation process to address cybersecurity risks that suddenly increase in severity?
      _____
4. Regarding privacy and civil liberties, do you have any comments on how cybersecurity practices affect these rights?
   _____
5. Does your credit union have any general comments on these NIST questions?
   _____
6. Any other comments or suggestions on this topic?
   _____

   Thank you for your comments.