HUNTON & WILLIAMS

Client Alert

February 2013

NIST Issues RFI for Framework for Reducing Cyber Risks

On February 26, 2013, the National Institute of Standards and Technology ("NIST") issued a Request for Information ("RFI") to gather comments regarding the development of a framework to reduce cybersecurity risks to critical infrastructure. As we previously reported, the Obama Administration's executive order, Improving Critical Infrastructure Cybersecurity (the "Executive Order"), released on February 12, 2013, directs NIST to coordinate development of this framework. Under the Executive Order, NIST is charged with collaborating with industry partners and identifying existing international standards and practices that have proven effective.

The development process for the framework aims to (1) identify existing cybersecurity standards applicable to critical infrastructure; (2) identify security gaps where new or revised standards should be implemented; and (3) develop action plans to address these gaps. According to NIST, the finalized framework will consist of standards, guidelines and best practices to promote the protection of information and information systems supporting critical infrastructure operations. The framework will help critical infrastructure owners and operators manage cybersecurity risk while protecting business confidentiality, individual privacy and civil liberties.

NIST's RFI specifies that the standards, guidelines and best practices in the framework should provide the following:

- A consultative process to assess cybersecurity risks;
- management, operational and technical security controls that address security threats and protect privacy and civil liberties;
- a consultative process to identify security controls that would address risks and to protect processed, stored and transmitted data;
- metrics, methods and procedures that can be used to assess and monitor the effectiveness of security controls;
- a comprehensive risk management approach that provides the ability to assess, respond to and monitor information security risks and that provides senior leaders with the necessary information to help them make risk-based decisions; and
- a menu of privacy controls necessary to protect privacy and civil liberties.

The RFI solicits ideas, recommendations and other input on three topics:

1. Current risk management practices: The RFI seeks information on how organizations assess and manage risk and cybersecurity risk in particular.

    - How organizations define and assess cybersecurity risk
    - Policies and procedures that govern cybersecurity risk
    - The standards and guidelines used to measure and manage risk
    - The greatest challenges to improving cybersecurity practices

2. Use of frameworks, standards, guidelines and best practices: The RFI seeks information on whether existing standards and guidelines are applicable to address cybersecurity needs.

- How organizations use these approaches
- How these approaches take into account sector-specific needs
- Whether these approaches have limitations and how these approaches can be modified to be more useful

3. Specific industry practices: The RFI seeks information on how organizations use key cybersecurity practices, such as: (1) separation of business from operational systems, (2) encryption and key management, (3) identification and authorization of users, (4) asset identification and management, (5) monitoring and incident detection tools, and (6) incident handling policies and procedures. Specifically, the RFI requests information on:

    - Whether these cybersecurity practices are widely used
    - Which practices are most important for critical infrastructure security
    - Which practices would be most challenging to implement
    - The risks to privacy and civil liberties posed by these practices

Responses to the RFI may be submitted until April 8, 2013, and will be posted publicly to encourage review and discussion. NIST directs commenters not to include information they do not wish to be posted, including personal or confidential business information. Throughout the framework development process, NIST will host interactive workshops and outreach events to invite input from critical infrastructure owners and operators, agencies, state and local governments and other interested parties. The first such meeting will be held on April 3, 2013, at the NIST headquarters in Gaithersburg, Maryland. NIST intends to publish a draft framework for additional comment within eight months.

Contacts

Lisa J. Sotto
lsotto@hunton.com

Evan D. Wolff
ewolff@hunton.com

Lawrence J. Bracken II
lbracken@hunton.com

John J. Delionado
jdelionado@hunton.com

Frederick R. Eames
feames@hunton.com

Maida O. Lerner
mlerner@hunton.com

Mark W. Menezes
mmenezes@hunton.com

Aaron P. Simpson
asimpson@hunton.com