[redacted]

February 13, 2014 1:56 PM

NIST Cybersecurity Framework Released: FYI

1 Attachment, 323 KB

I am happy to take questions on this on our next legislative call (March 3, at 4:00 pm), or by email before then.

**Document: Attached.**

**Press Release: http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.**

To help organizations charged with providing the nation's financial, energy, health care and other critical systems better protect their information and physical assets from cyber attack, the Commerce Department's National Institute of Standards and Technology (NIST) today released a Framework for Improving Critical Infrastructure Cybersecurity. The framework provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs.

In February 2013, President Obama issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity. The order calls for the development of a voluntary, risk-based Cybersecurity Framework—a set of existing standards, guidelines and practices to help organizations manage cyber risks. The resulting framework, created through public-private collaboration, provides a common language to address and manage cyber risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses.

"The framework provides a consensus description of what's needed for a comprehensive cybersecurity program," said Under Secretary of Commerce for Standards and Technology and NIST Director Patrick D. Gallagher. "It reflects the efforts of a broad range of industries that see the value of and need for improving cybersecurity and lowering risk. It will help companies prove to themselves and their stakeholders that good cybersecurity is good business."

The framework allows organizations—regardless of size, degree of cyber risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.
Organizations can use the framework to determine their current level of cybersecurity, set goals for cybersecurity that are in sync with their business environment, and establish a plan for improving or maintaining their cybersecurity. It also offers a methodology to protect privacy and civil liberties to help organizations incorporate those protections into a comprehensive cybersecurity program.

While today's framework is the culmination of a year-long effort that brought together thousands of individuals and organizations from industry, academia and government, it is expected to be a first step in a continuous process to improve the nation's cybersecurity.

***The framework document is labeled "Version 1.0" and is described as a "living" document that will need to be updated to keep pace with changes in technology, threats and other factors, and to incorporate lessons learned from its use. According to the document, these updates will ensure the framework meets the needs of critical infrastructure owners and operators in a dynamic and challenging environment.***

The three main elements described in the document are the framework core, tiers and profiles.

- The core presents five functions—identify, protect, detect, respond and recover—that taken together allow any organization to understand and shape its cybersecurity program.
- The tiers describe the degree to which an organization's cybersecurity risk management meets goals set out in the framework and "range from informal, reactive responses to agile and risk-informed."
- The profiles help organizations progress from a current level of cybersecurity sophistication to a target improved state that meets business needs.

"The development of this framework has jumpstarted a vital conversation between critical infrastructure sectors and their stakeholders," said Gallagher. "They can now work to understand the cybersecurity issues they have in common and how those issues can be addressed in a cost-effective way without reinventing the wheel."

NIST also released today a "Roadmap" document to accompany the framework. It lays out a path toward future framework versions and ways to identify and address key areas for cybersecurity development, alignment and collaboration. It says NIST will continue to serve as a convener and coordinator to work with industry and other government agencies to help organizations understand, use and improve the framework. This will include leading discussions of models for future governance of the framework, such as potential transfer to a non-government organization.

**News Stories / Commentary:**

- http://www.lawfareblog.com/2014/02/nist-cybersecurity-framework-issued/#.Uv0Tgt8o5D8
- http://healthitsecurity.com/2014/02/13/nist-releases-final-voluntary-cybersecurity-framework/
- http://www.broadcastingcable.com/news/washington/nist-releases-cybersecurity-framework/129156
- https://www.cdt.org/pr_statement/cybersecurity-framework-useful-falls-short-privacy

+ + +

Best regards,

Reed

NIST–cybers…pdf (323 KB)