ei
the magazine of the electro*industry*
Published by the National Electrical Manufacturers Association | www.NEMA.org | June 2014 | Vol. 19 No. 6
2014 Hermes Award Winner

Think about it—

How Smart is Your Grid?

- Information and Operation Technologies
- Transactive Energy
- Microgrids and Energy Storage
- NERC Compliance
- Cybersecurity
- Smart Grid Interoperability Panel
- High-Voltage/Temperature Materials
- Energy-Water Nexus

NEMA

NIST Cybersecurity Framework Addresses Risks to Critical Infrastructure

Victoria Yan Pillitteri, CISSP, Advisor for Information System Security, Computer Security Division, Information Technology Laboratory, NIST

According to President Obama, cyber threats "pose one of the gravest national security dangers that the United States faces."

In a statement on February 12, 2014, which coincided with the publication by the National Institute of Standards and Technology (NIST) of *Framework for Improving Critical Infrastructure Cybersecurity,* the president said, "To better defend our nation against this systemic challenge, one year ago I signed an executive order directing the administration to take steps to improve information sharing with the private sector, raise the level of cybersecurity across our critical infrastructure, and enhance privacy and civil liberties."

That executive order—EO 13636 *Improving Critical Infrastructure Cybersecurity*—directed NIST to develop a voluntary risk-based cybersecurity framework based on existing industry standards and best practices to help organizations manage cybersecurity risk. The resulting framework was created through a yearlong collaboration between government and industry.

Connecting Shareholders and Technology

The critical infrastructure community includes public and private owners, operators, and other entities with a role in securing the nation's infrastructure. Members of each critical infrastructure sector perform functions that are supported by information technology (IT) and industrial control systems (ICS). This reliance on technology, communication, and the interconnectivity of IT and ICS has changed and expanded potential vulnerabilities and increased potential risk to operations.

For example, as ICS and the data produced in ICS operations are increasingly used to deliver critical services and support business decisions, the potential impacts of a cybersecurity incident on an organization's business, assets, health and safety of individuals, and the environment must be considered. To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of IT and ICS is required.

In developing the framework, it was clear early on that the use of common language would help organizations address and manage cybersecurity risk in a cost-effective way without introducing additional regulatory requirements. Using business drivers to guide cybersecurity activities helps clarify that cybersecurity risk can affect an organization's bottom line by reducing revenue, hindering innovation, and impacting the ability to gain and maintain customers.

The framework consists of three parts: Framework Core, Framework Profile, and Framework Implementation Tiers. Figure 1 provides a high-level summary of each component.

While the intended outcomes identified in Framework Core are the same for IT and ICS, the operational environments and considerations differ, leading to different implementations of security technologies and solutions. ICS have a direct effect on the physical world including potential risks to the health and safety of individuals and environmental impacts. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.

Protecting Privacy and Civil Liberties

The framework includes a methodology to protect individual privacy and civil liberties as critical infrastructure organizations conduct cybersecurity activities. The methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time. Organizations may address these considerations and processes with a range of technical implementations. However, not all activities may give rise to these considerations.

The framework is applicable to organizations of all sizes, with differing risks and levels of sophistication. It does not provide a one-size-fits-all approach. Rather, it can be leveraged as a tool across the 16 critical infrastructure sectors,[1] recognizing that each sector has unique threats, vulnerabilities, risk tolerances, and operational constraints.

Ensuring that there are products available to support the owners and operators of critical infrastructure are key and a continued focus moving forward. Industry-led efforts, such as the January 2014 "Statement of Cybersecurity Principles" by the NEMA Industrial Automation Control Products and Systems Section, are already underway to invest in the development, coordination, and ongoing refinement of relevant cybersecurity standards for the critical infrastructure and the vendors that provide services and solutions for them.

Similarly, other critical infrastructure sectors are working together through their respective sector-coordinating councils, sector-specific agencies, and trade groups to develop sector-specific framework implementation guidance.

In addition to the framework, NIST also released the *Roadmap for Improving Critical Infrastructure Cybersecurity*, a companion document that discusses NIST's next steps with the framework and identifies key areas of development, alignment, and collaboration. These next steps are based on input and feedback received from stakeholders throughout the framework development processes, specifically on the "Areas for Improvement" section of the preliminary framework, which has been moved to this document.

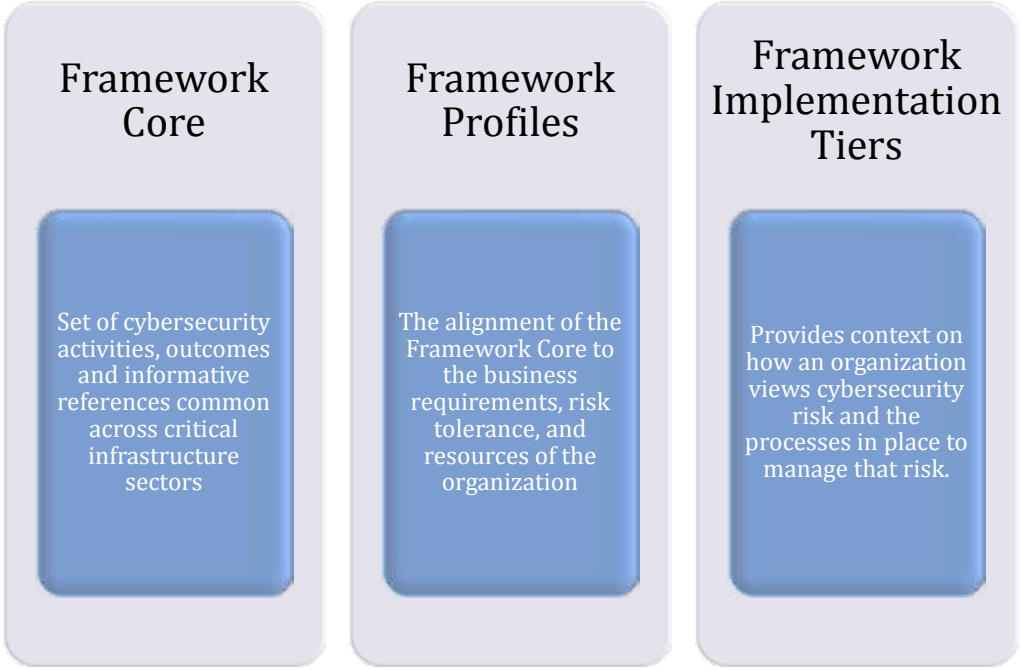
NIST will host future workshops around specific roadmap areas and get feedback on the framework to inform future versions. It also will build on existing relationships and expand its outreach in partnership with the Department of Homeland Security's Critical Infrastructure Cyber Community C³ Voluntary Program.[2]

The framework will continue to be updated and improved as industry provides feedback on implementation and lessons learned. As has been the case throughout its development process, organizations are encouraged to contribute observations, suggestions, and lessons learned to *cyberframework@nist.gov.*

Ms. Pillitteri is part of the NIST team that worked on EO 13636, chairs the Smart Grid Interoperability Panel Cybersecurity Committee, and is the NIST co-chair of the Cyber-Physical Systems Cybersecurity public-private working group.

[1] Chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; water and wastewater systems

[2] C³ (C cubed) encourages use of the NIST framework to strengthen critical infrastructure cybersecurity and to help critical infrastructure owners and operators improve their cyber risk management processes.
For more information, visit *www.dhs.gov/about-critical-infrastructure-cyber-community-c³-voluntary-program* or contact *ccubedvp@hq.dhs.gov.*



The *Framework for Improving Critical Infrastructure Cybersecurity*, the *Roadmap for Improving Critical Infrastructure Cybersecurity*, and related news and information are available at *www.nist.gov/cyberframework*

Figure 1. NIST cybersecurity framework encompasses a core, profile, and Implementation tiers.