Framework for Improving Critical Infrastructure Cybersecurity

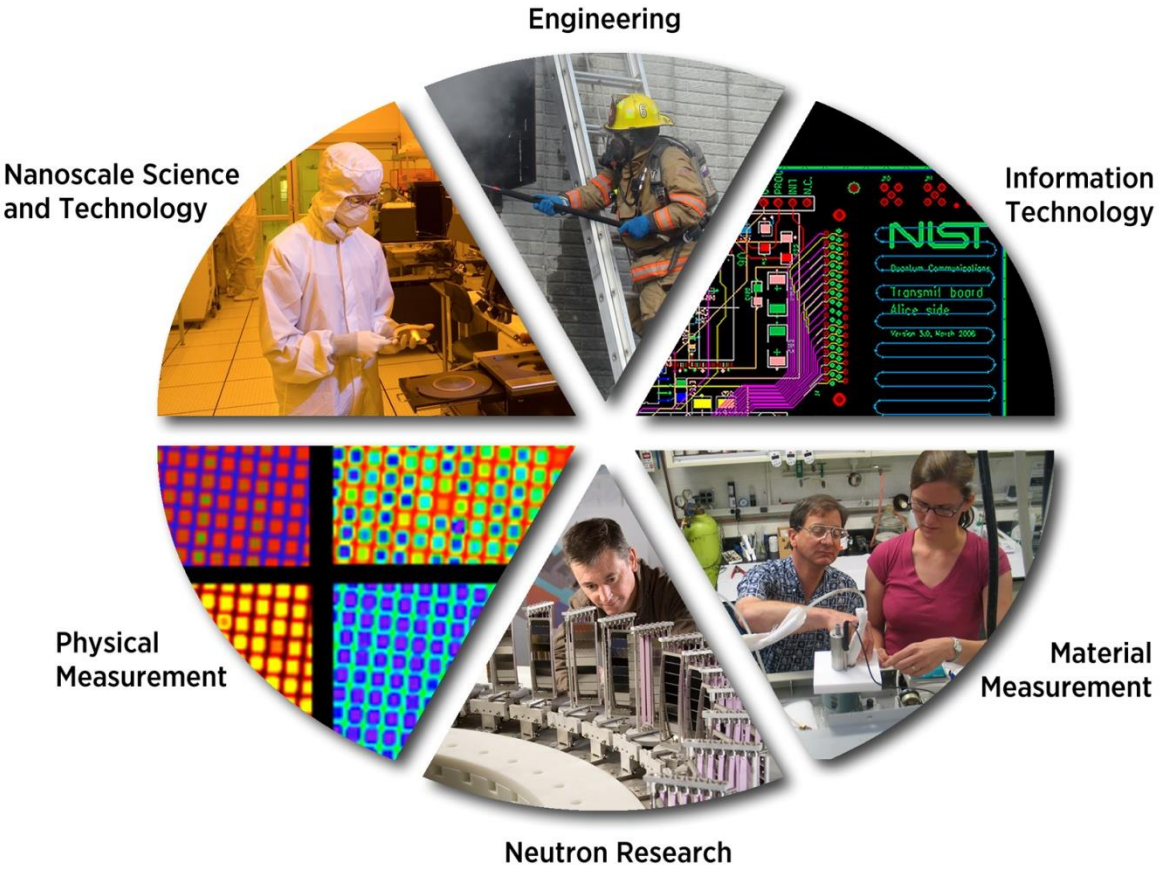
Overview and Status

Executive Order 13636
“Improving Critical Infrastructure Cybersecurity”

Kevin Stine
National Institute of Standards and Technology

National Institute of Standards and Technology

Promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.



Executive Order: Improving Critical Infrastructure Cybersecurity

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

President Barack Obama

Executive Order 13636, *Feb. 12, 2013*

- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work

As Directed in the EO, the Cybersecurity Framework ...

- Includes a set of existing standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks

- Provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk

- Identifies areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations

Framework Components

Framework Core

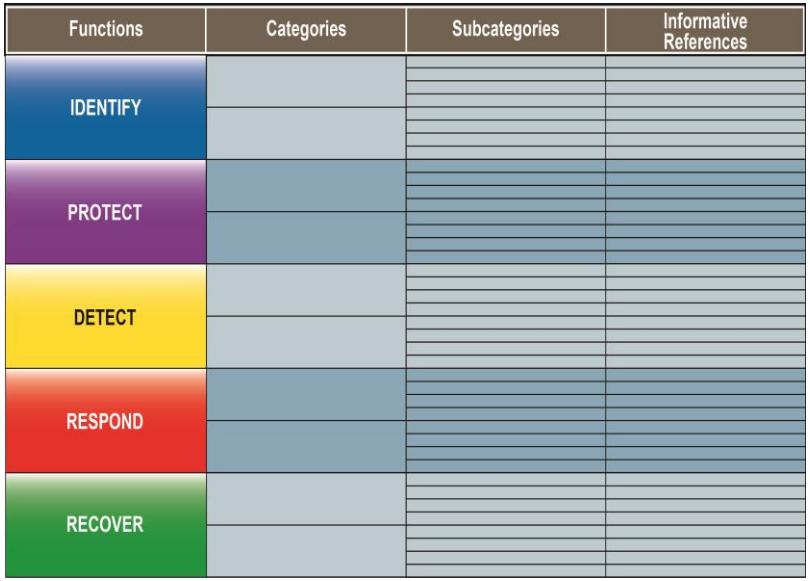
- Cybersecurity activities and informative references common across critical infrastructure sectors and organized around particular outcomes

Framework Profile

- Aligns industry standards and best practices to the framework Core in a particular implementation scenario

Framework Implementation Tiers

- Describes how cybersecurity risk is managed by an organization



Key Points about the Framework

- It's a framework, not a prescription.
- The framework is a flexible, highly adaptable tool.
- It's a demonstration of a strong public-private partnership
- The framework is a living document.

What's Next for the Framework

- Organizations should use the framework, and provide feedback to NIST
- Industry groups, associations, and standards organizations can play key roles in assisting their members to understand and use the framework
- Focus on high-priority areas for development, alignment, and collaboration:

Authentication
Automated Indicator Sharing
Conformity Assessment
Cybersecurity Workforce
Data Analytics
Technical Privacy Standards
International Alignment
Supply Chain Risk Management
Federal Agency Cybersecurity Alignment

http://nist.gov/cyberframework/upload/roadmap-021214.pdf

Where to Learn More and Engage…

- *Framework for Improving Critical Infrastructure Cybersecurity*, available at www.nist.gov/cyberframework
  - Share your framework experiences at cyberframework@nist.gov
- Participate in our cybersecurity workshops and comment on our standards and guidelines
- Participate through the National Cybersecurity Center of Excellence (NCCoE)
- Follow our cybersecurity activities at http://csrc.nist.gov