Framework for Improving Critical Infrastructure Cybersecurity

Overview and Status

Executive Order 13636
“Improving Critical Infrastructure Cybersecurity”

Kevin Stine
National Institute of Standards and Technology

Executive Order 13636: 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

The Cybersecurity Framework...

- Includes a set of 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

The Cybersecurity Framework…

- Provides a structure organizations can use to create, guide, assess or improve comprehensive cybersecurity programs based on risks
- Offers 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
- 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
- Helps companies prove to themselves and their stakeholders that good cybersecurity is good business
- Builds on global and other standards, guidelines, and best practices
- Provides a means of expressing cybersecurity requirements to business partners and customers
- Assists organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program

Framework Components

Framework Core

- Cybersecurity activities and informative references common across critical infrastructure sectors and organized around particular outcomes
- Enables communication of cyber risk across an organization

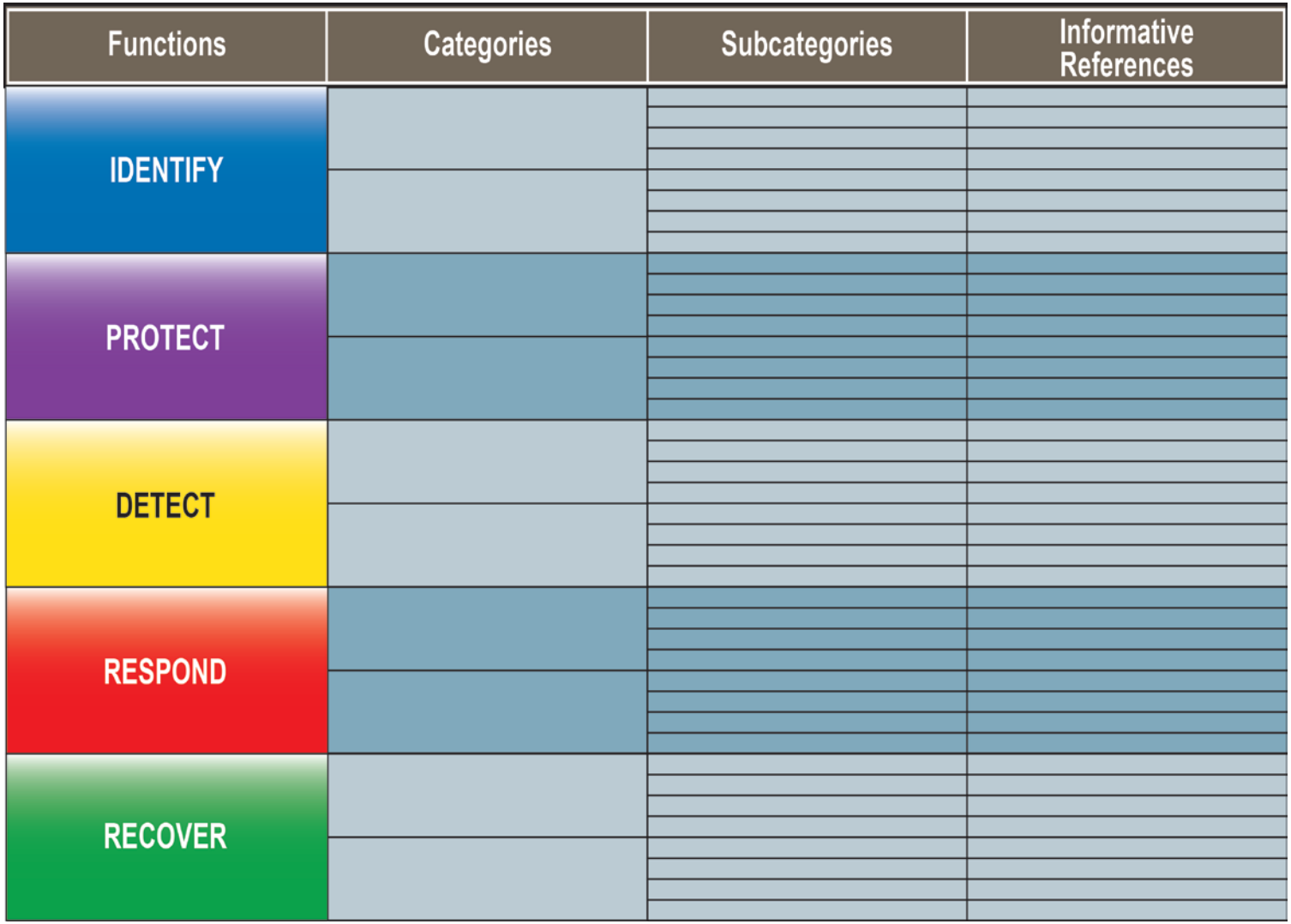
Framework Profile

- Aligns industry standards and best practices to the framework Core in a particular implementation scenario
- Supports prioritization and measurement of progress toward the Target Profile, while factoring in other business needs— including cost-effectiveness and innovation

Framework Implementation Tiers

- Describes how cybersecurity risk is managed by an organization
- Describes degree to which an organization's cybersecurity risk management practices exhibit the key characteristics (e.g., risk and threat aware, repeatable, and adaptive)

Framework Core



What's Next: Using the Cybersecurity Framework

- Organizations—led by their senior executives—should use the framework now, and provide feedback to NIST
- Industry groups, associations, and non-profits can play key roles in assisting their members to understand and use the framework by:
  - Building or mapping their sector's specific standards, guidelines, and best practices to the framework
  - Developing and sharing examples of how organizations are using the framework
- NIST is committed to helping organizations understand and use the framework
  - NIST is expanding its outreach and will work with the Department of Homeland Security on its "C^3" Voluntary Program (http://www.dhs.gov/about-critical-infrastructure-cyber-community-c^3-voluntary-program)

What's Next: Areas for Development, Alignment, and Collaboration

- The Executive Order calls for the framework to "identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations"
- High-priority areas for development, alignment, and collaboration were identified based on stakeholder input:
  - Authentication
  - Automated Indicator Sharing
  - Conformity Assessment
  - Cybersecurity Workforce
  - Data Analytics
  - Federal Agency Cybersecurity Alignment
  - International Aspects, Impacts, and Alignment
  - Supply Chain Risk Management
  - Technical Privacy Standards

Cybersecurity Workforce: Training and Preparing

- A skilled cybersecurity workforce is needed to meet the unique cybersecurity needs of critical infrastructure.
  - Adapt to continuously improve the necessary cybersecurity practices.
- Organizations must understand their current and future cybersecurity workforce needs.
  - Develop training awareness, training, and education resources to raise the level of technical competence.
- Promote existing and future cybersecurity workforce development activities to expand and fill the cybersecurity workforce pipeline.

What's Next: Roadmap for the Framework

- NIST will work with stakeholders to further understand these areas for development, alignment and collaboration and to develop or identify new or revised standards
- For specifics, see the companion Roadmap to the framework that also was issued Feb. 12, 2014 :

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

- Areas for development, alignment, and collaboration are covered in greater detail
- Strengthening private sector involvement in long-term governance of the framework is also discussed

Where to Learn More and Stay Current

The *Framework for Improving Critical Infrastructure Cybersecurity*, the *Roadmap*, and related news and information are available at:

http://www.nist.gov/cyberframework