Cybersecurity Framework: Current Status and Next Steps

Implementation of Executive Order 13636

November 24, 2014

Adam Sedgewick
Senior IT Policy Advisor
Adam.Sedgewick@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

National Institute of Standards and Technology (NIST)

About NIST

- Part of the U.S. Department of Commerce
- NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
  - 3,000 employees
  - 2,700 guest researchers
  - 1,300 field staff in partner organizations
  - Two main locations: Gaithersburg, Md and Boulder, Co

NIST Priority Research Areas


Advanced Manufacturing


IT and Cybersecurity


Healthcare


Forensic Science


Disaster Resilience


Cyber-physical Systems


Advanced Communications

The Role of NIST

- The National Institute of Standards and Technology's mission is to stimulate innovation, foster industrial competitiveness, and improve the quality of life.

- Role in cybersecurity began in 1972 with the development of the Data Encryption Standard – began when commercial sector also has a legitimate need for cryptography, including in ATMs.

- Using widely-accepted standards helps create competitive markets around market need through combinations of price, quality, performance, and value to consumers. It then promotes faster diffusion of these technologies throughout industry.

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

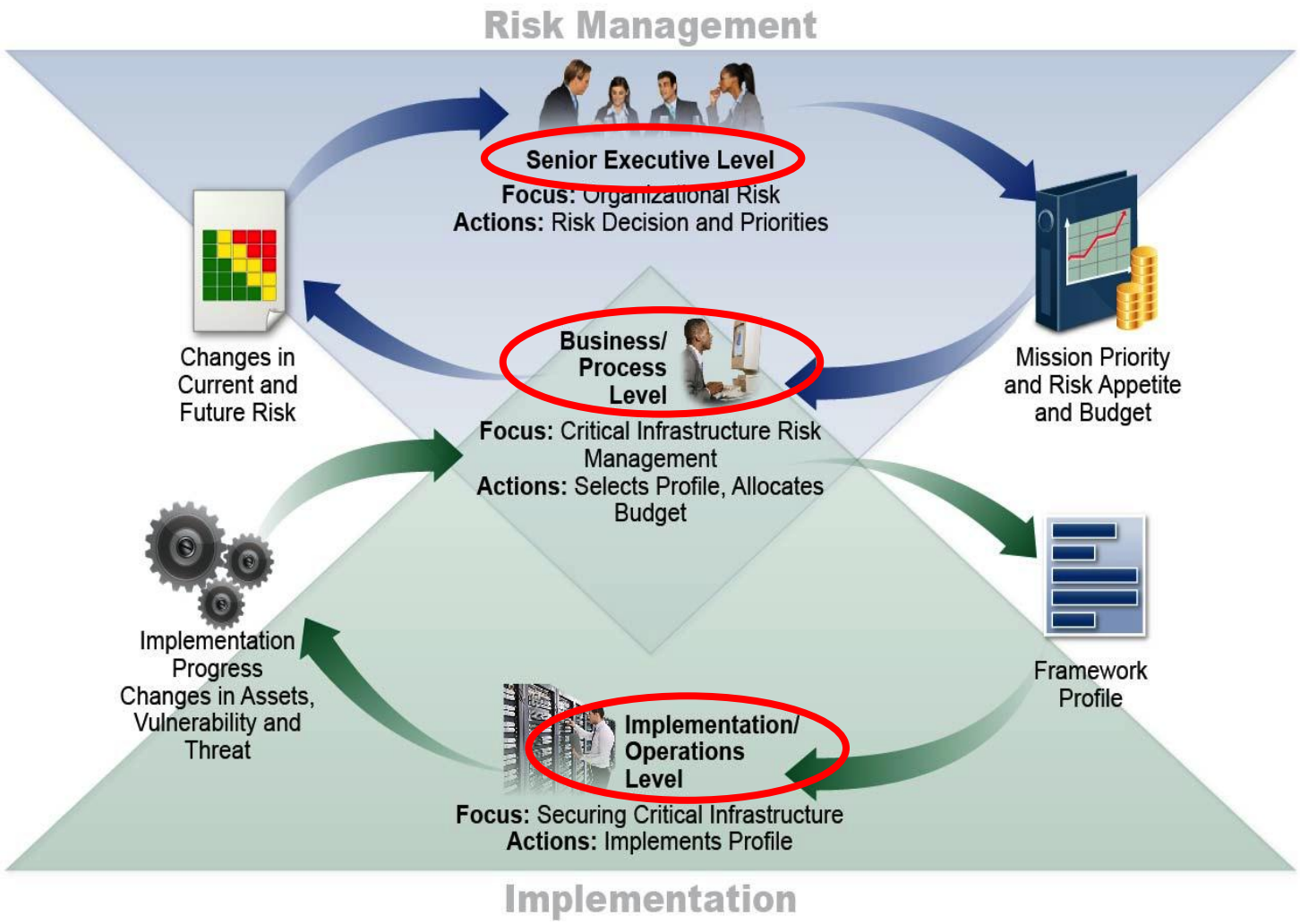
Based on the Executive Order, the Cybersecurity Framework Must...

- Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks
- Provide 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
- Identify areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations
- Be consistent with voluntary international standards

The Cybersecurity Framework Is for Organizations…

- Of any size, in any sector in the critical infrastructure
- That already have a mature cyber risk management and cybersecurity program
- That don't yet have a cyber risk management or cybersecurity program
- With a mission of helping keep up-to-date on managing risk and facing business or societal threats

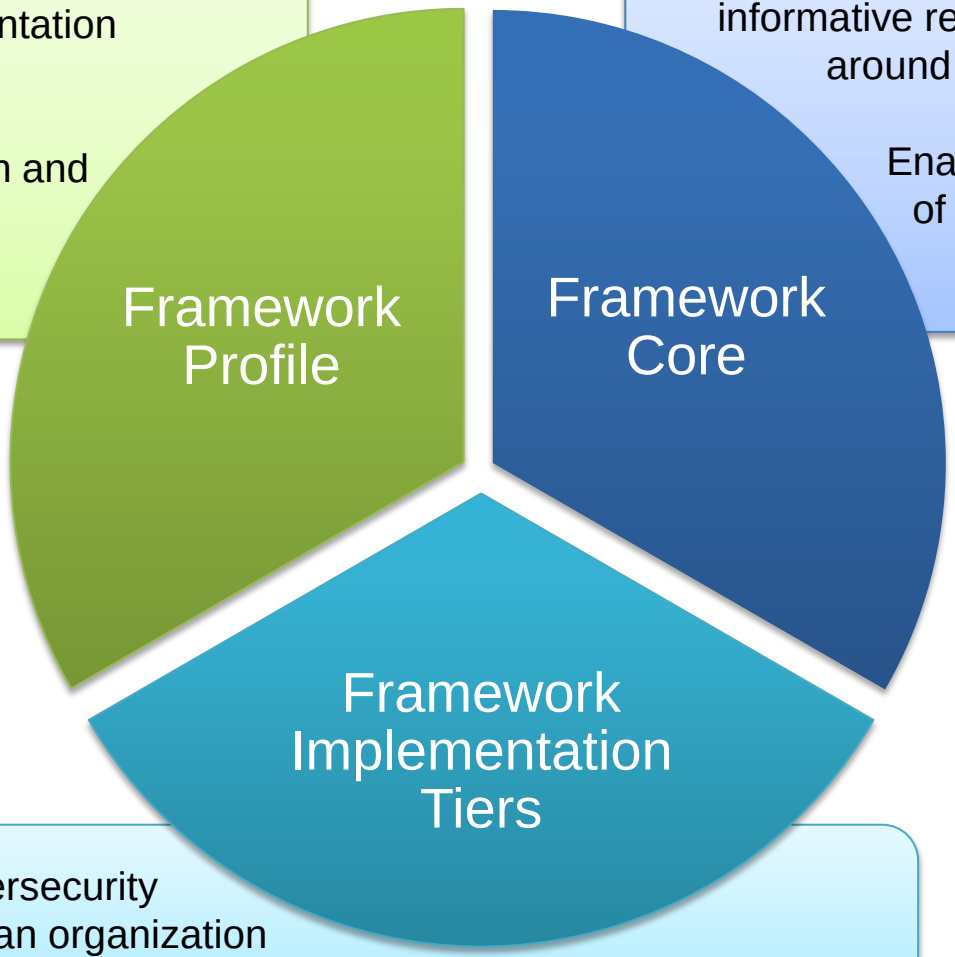
Must apply from Executives to Operations



Framework Components

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

Supports prioritization and measurement while factoring in business needs



Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Framework Core

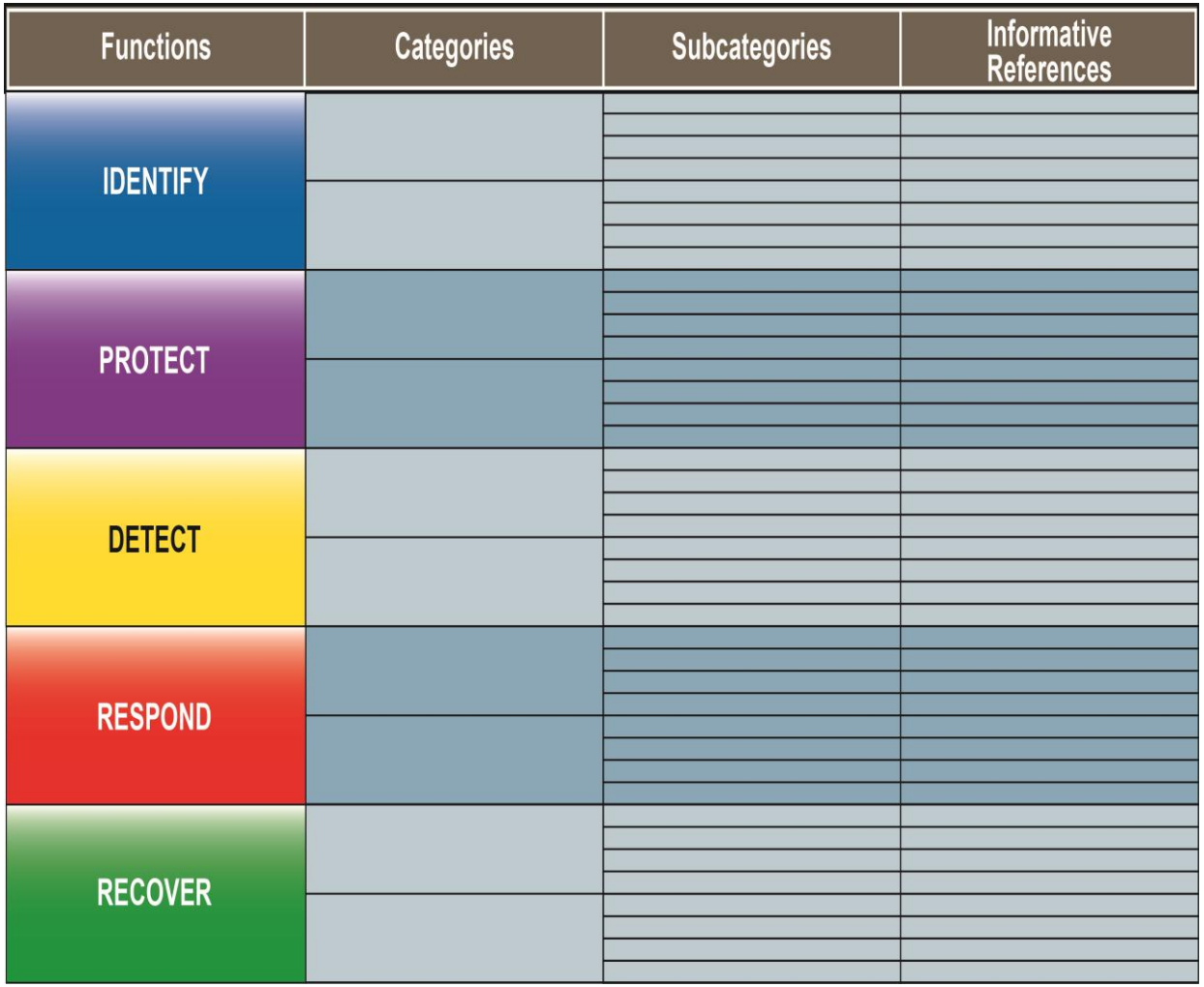
What assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?



Framework Profile

- Alignment of Functions, Categories, and Subcategories with business requirements, risk tolerance, and resources of the organization

- Enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities

- Can be used to describe current state or desired target state of cybersecurity activities

Framework Implementation Tiers

- Feedback indicated the need for the Framework to allow for flexibility in implementation and bring in concepts of maturity models.

- Responding to feedback, Framework Implementation Tiers were proposed to reflect how an organization implements the Framework Core functions and manages its risk.

- The Tiers are progressive, ranging from Partial (Tier 1) to Adaptive (Tier 4), with each Tier building on the previous Tier.

- The Tier characteristics are defined at the organizational level and are applied to the Framework Core to determine how a category is implemented.

How to Use the Cybersecurity Framework

The Framework is designed to complement existing business and cybersecurity operations, and can be used to:

- Understand security status
- Establish / Improve a cybersecurity program
- Communicate cybersecurity requirements with stakeholders, including partners and suppliers
- Identify opportunities for new or revised standards
- Identify tools and technologies to help organizations use the Framework
- Integrate privacy and civil liberties considerations into a cybersecurity 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

International Aspects, Impacts, and Alignment

- Because the Framework references globally accepted standards, guidelines and practices, organizations inside and outside of the United States can use the Framework to efficiently operate globally and manage new and evolving risks.

- “Cybersecurity risks and threats are a global problem, and the more the Framework can be socialized globally, especially among governments and those agencies that deal with cyber issues, the better.” - ISACA

- We are working with standards developing organizations, industry, and sectors to ensure the Cybersecurity Framework remains aligned and compatible with those existing and developing standards and practices.

What's Next: Using the Cybersecurity Framework

"A model of public-private cooperation, this Framework will help industry and Government strengthen the security and resiliency of our critical infrastructure." – President Obama, September 30, 2014

- Organizations—led by their senior executives—are using the framework to improve their cybersecurity programs
- Industry groups, associations, and non-profits are playing 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.
- The U.S. Government is committed to helping organizations understand and use the framework, getting feedback on initial use.

Key Points about the Framework

- **It's a framework, not a prescription**
  - It provides a common language and systematic methodology for managing cyber risk
  - It does not tell a company *how* much cyber risk is tolerable, nor does it claim to provide "the one and only" formula for cybersecurity
  - Having a common lexicon to enable action across a very diverse set of stakeholders will enable the best practices of elite companies to become standard practices for everyone
- **The framework is a living document**
  - It is intended to be updated over time as stakeholders learn from implementation, and as technology and risks change
  - That's one reason why the framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, and standards will change over time—principals will not

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

Email: cyberframework@nist.gov