

# Cybersecurity Framework: Current Status and Next Steps

Federal Advisory Committee on Insurance

November 6, 2014

Adam Sedgewick  
Senior IT Policy Advisor  
[Adam.Sedgewick@nist.gov](mailto: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

# 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

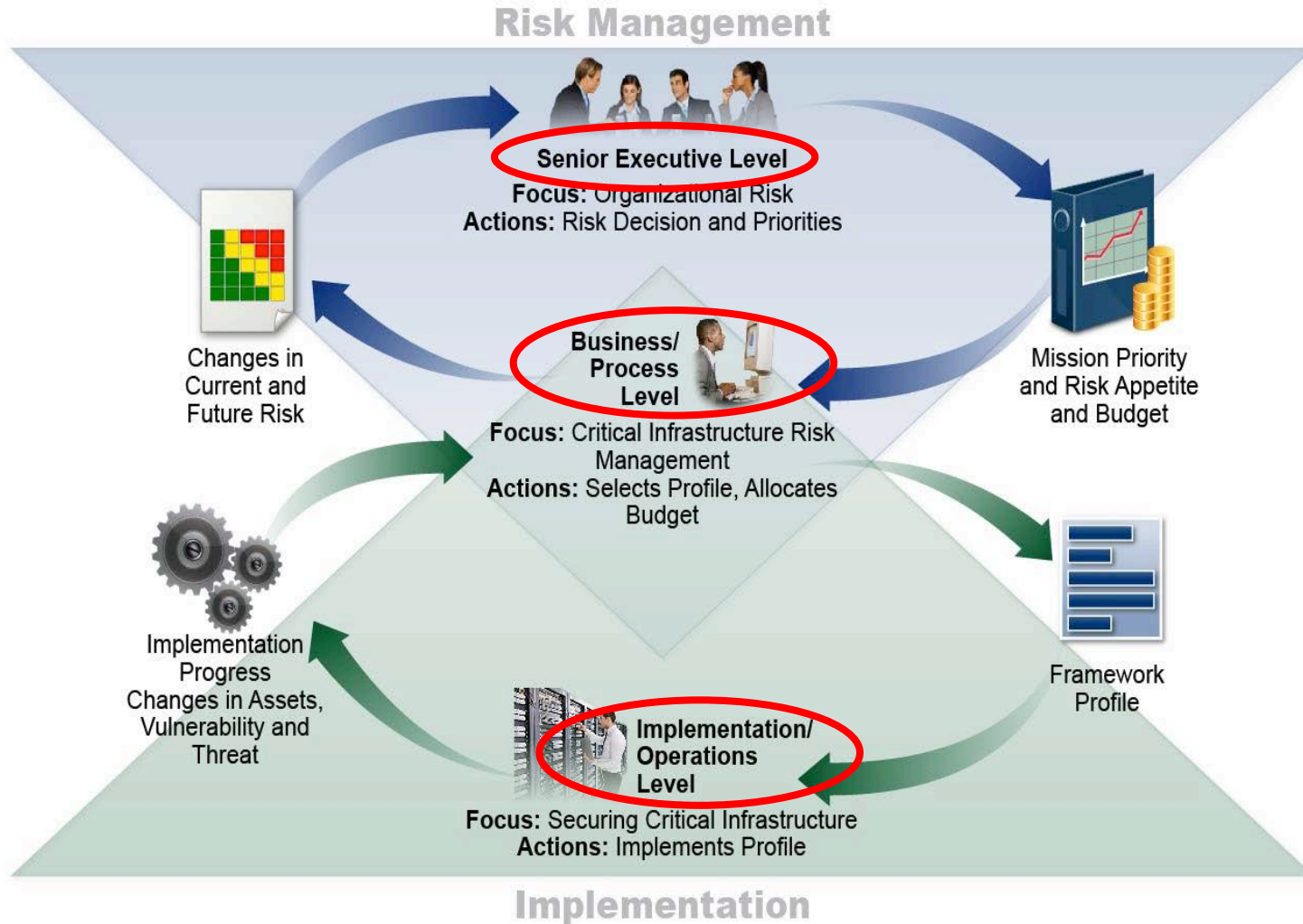
# The Cybersecurity Framework Is for Organizations...



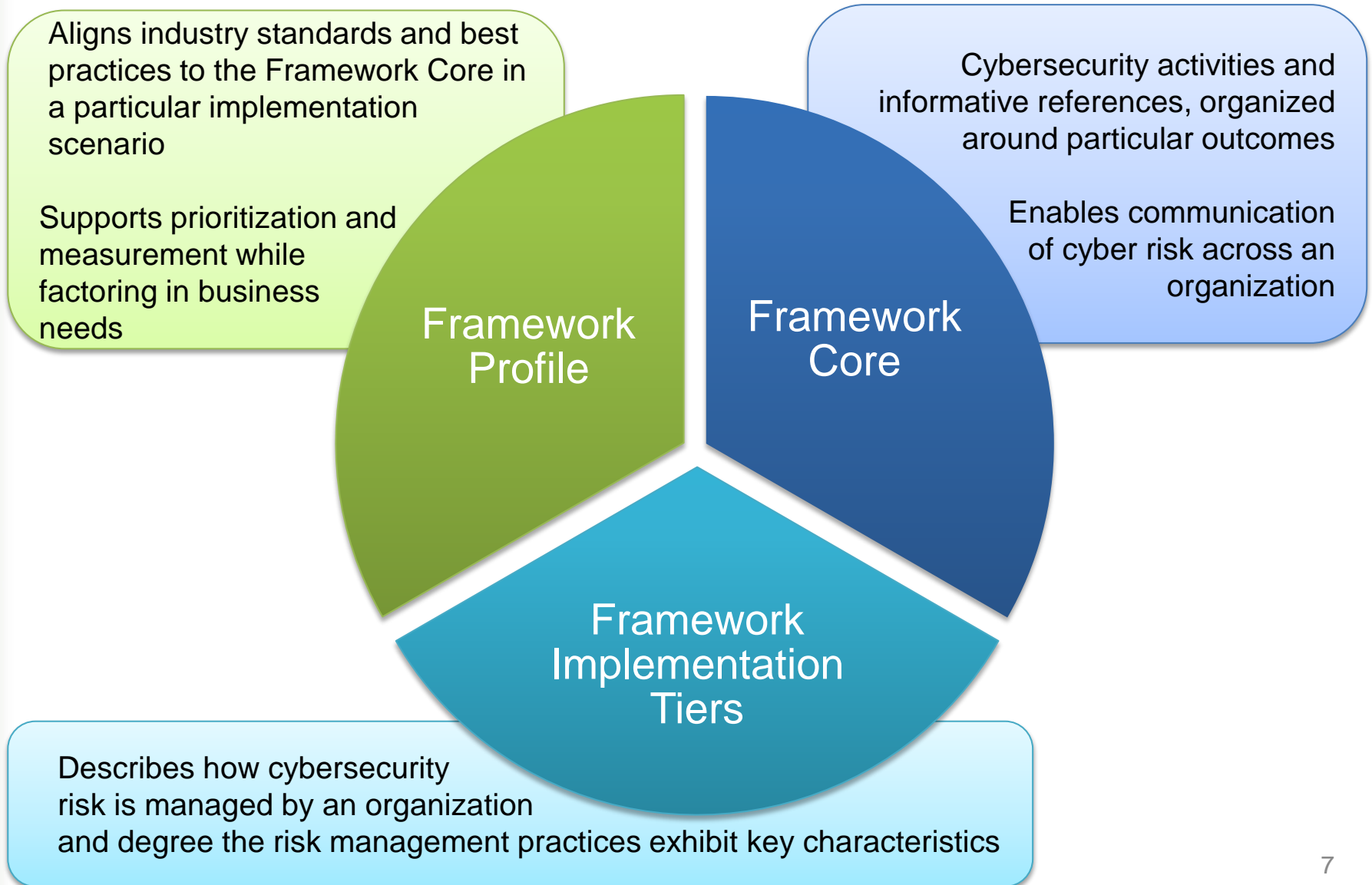
- Of **any size**, in **any sector** in the critical infrastructure
- That already have a **mature** cyber risk management and cybersecurity program
- That **don't yet** have a cyber risk management or cybersecurity program
- With a mission of **helping keep up-to-date** on managing risk and facing business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



# Must apply from Executives to Operations



# Framework Components



# Framework Core

Functions	Categories	Subcategories	Informative References
What assets need protection?	IDENTIFY		
What safeguards are available?	PROTECT		
What techniques can identify incidents?	DETECT		
What techniques can contain impacts of incidents?	RESPOND		
What techniques can restore capabilities?	RECOVER		



# 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



# 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 practice, organizations domiciled inside and outside of the United States can use the Framework to efficiently operate globally and manage new and evolving risks.
- Feedback from Stakeholders (ISACA): “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.”
- We are exchanging information and working with standards developing organizations, industry, and sectors to ensure the Cybersecurity Framework remains aligned and compatible with existing and developing standards and practices.



# What's Next: Using the Cybersecurity Framework

---

- Organizations—led by their senior executives—are **using the framework now**
- **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 of how organizations are using the framework
- NIST is committed to helping organizations understand and use the framework, getting feedback on initial use.
- Workshop was held on October 29th and 30th in Tampa, FL.

## 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](mailto:cyberframework@nist.gov)