Framework for Improving Critical Infrastructure Cybersecurity

Implementation of Executive Order 13636

10 April 2015

cyberframework@nist.gov

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

Agenda

- Mission of NIST
- Cybersecurity at NIST
- Cybersecurity Framework
  - The Executive Order
  - Our Development Approach
  - Basic Framework Components
  - Roadmap Items
- Observations about Framework Use in Industry
- Applying Framework
  - Getting Started
  - Assessing New Technologies
- Future Plans
- Discussion & Question-Answer

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

- 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.
- Charter for both public and private sectors
- Non-regulatory
- 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.
  - Ensure timely availability of standards, and associated testing, that address identified NIST IT Laboratory priorities, including national priorities established in statute or administration policy;
  - Achieve cost-efficient, timely and effective solutions to legitimate regulatory, procurement and policy objectives;
  - Promote standards and standardization systems that enable innovation and foster US competitiveness; and
  - Facilitate international trade and avoid the creation of unnecessary obstacles to trade.

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

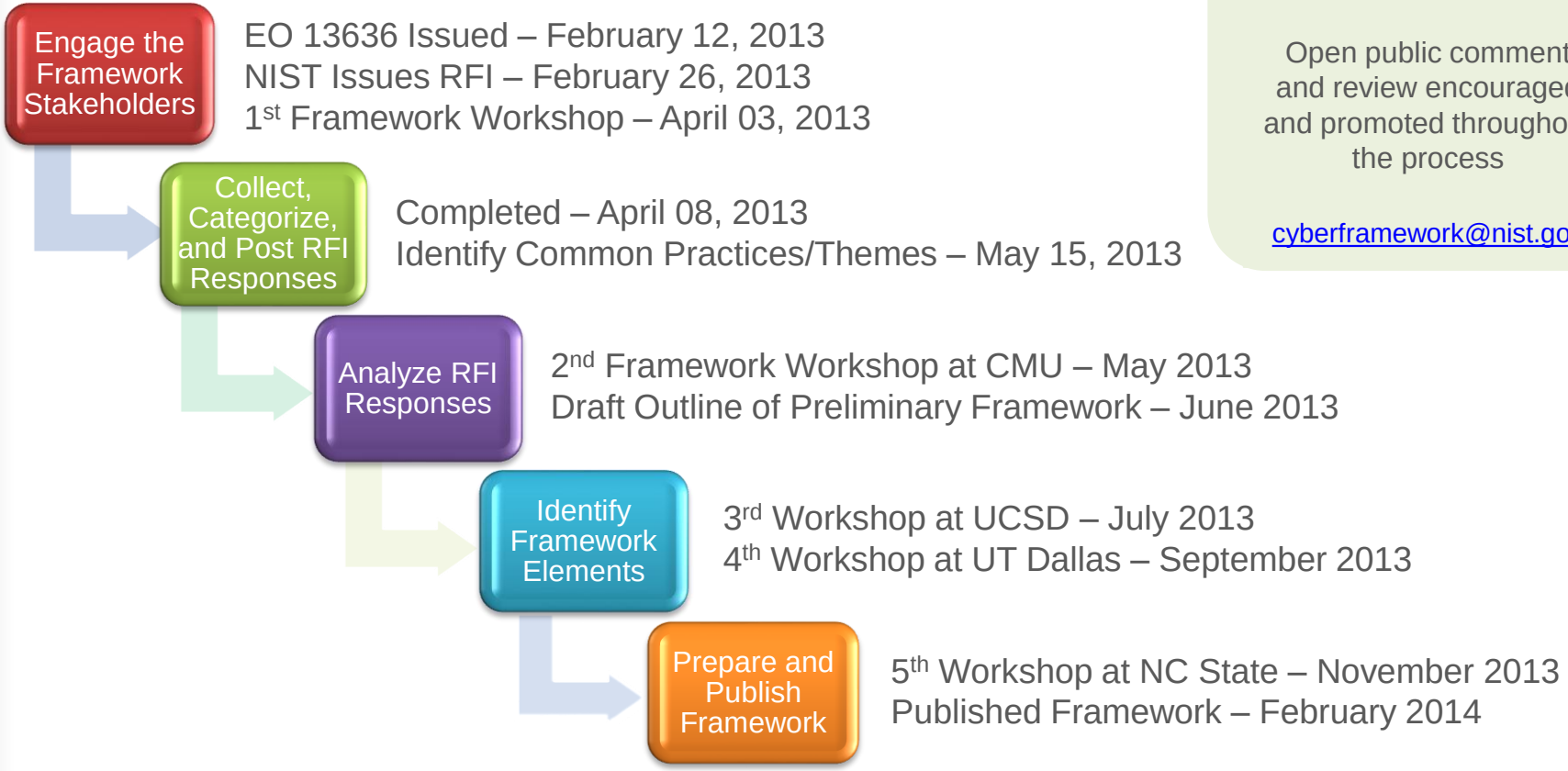
Executive Order 13636, *Feb. 12, 2013*

- 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

Development of the Framework

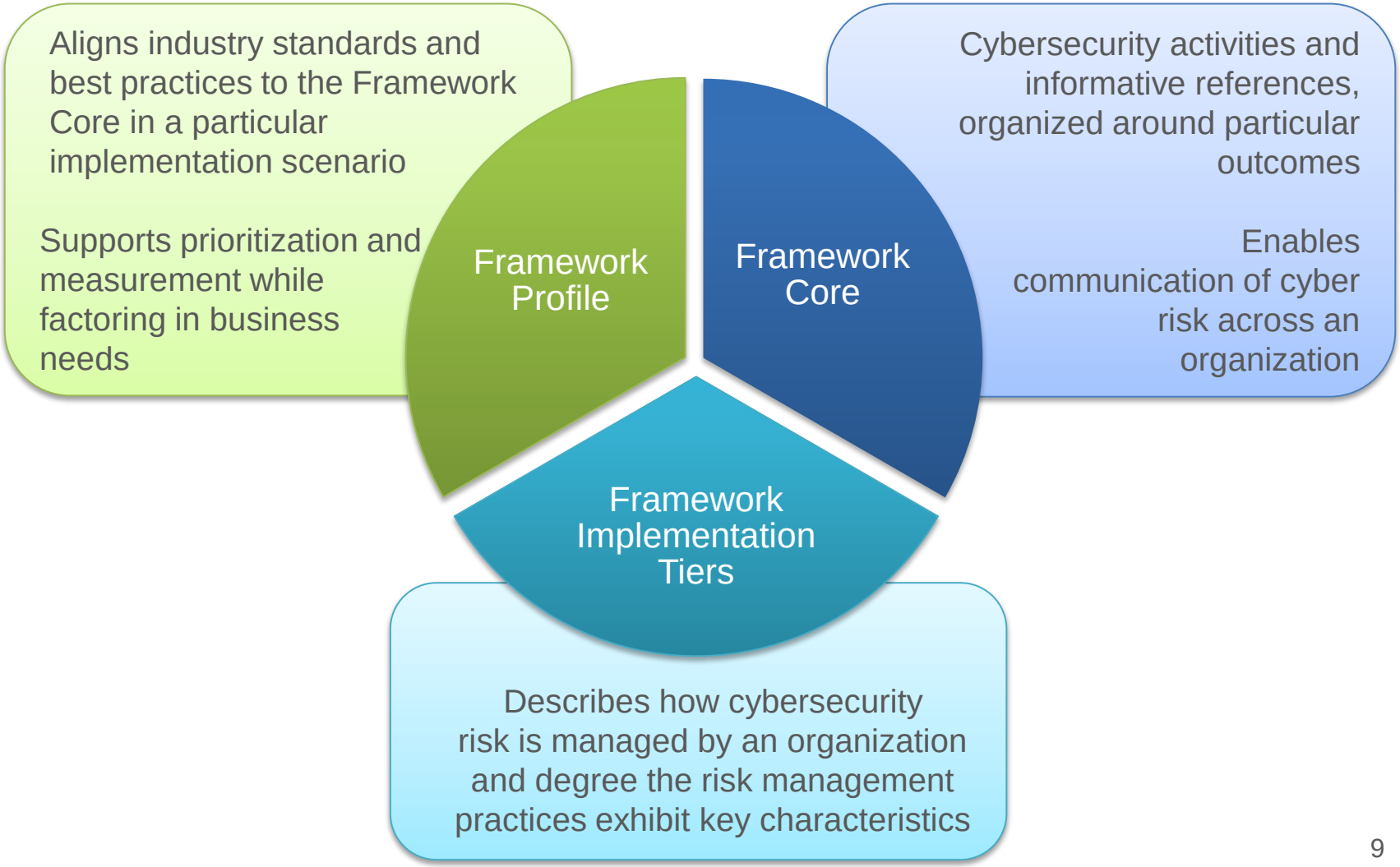


Ongoing Engagement:

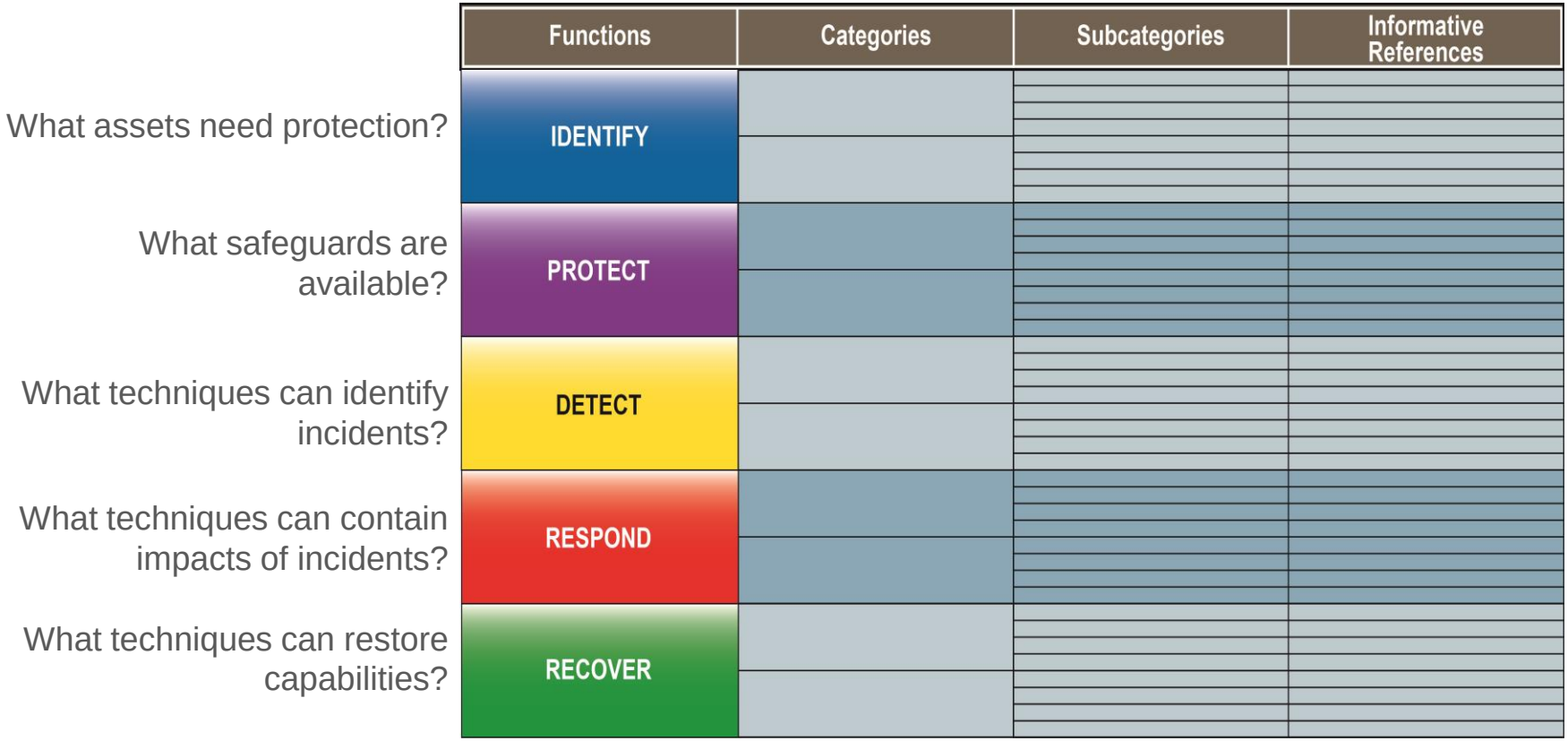
Open public comment and review encouraged and promoted throughout the process

cyberframework@nist.gov

Framework Components



Framework Core



Framework Core Excerpt

PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1

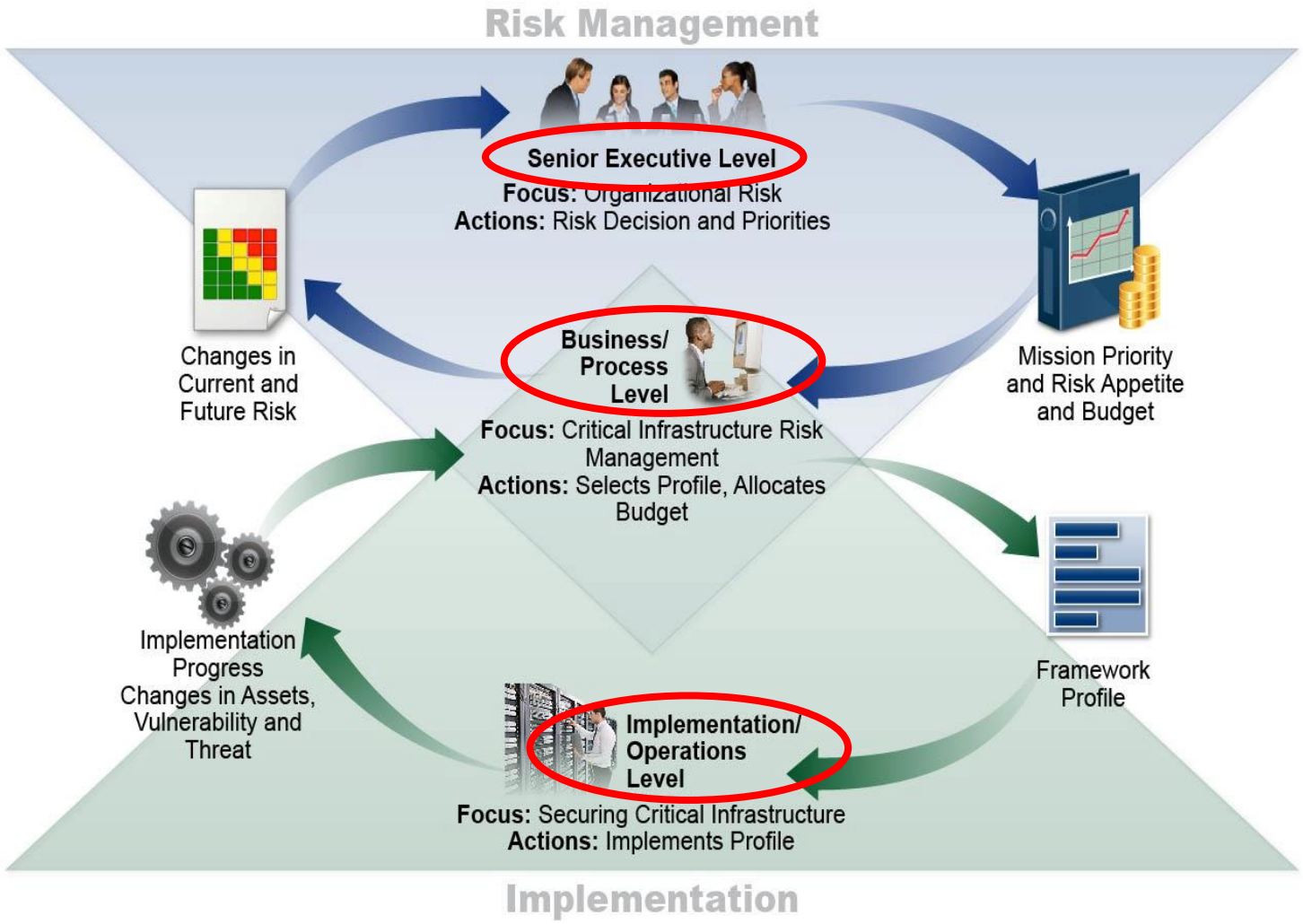
Framework Profile

- 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 from Executives to Operations



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.

Uses of 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

Business Value of Cybersecurity Framework

Benefits	Features
• Reduces time and expense of starting an information security program • Reduces risk within current information security programs by identifying areas for improvement • Increases efficiencies and reduce the possibility of miscommunication within your information security program and with other organizations such as partners, suppliers, regulators, and auditors	• Organizes reconciliation and de-confliction of legislation, regulation, policy, and industry best practice (Core) • Guides organization and management of and information security program (Core) • Measures current state and expresses desired state (Profile) • Enables investment decisions to address gaps in current state (Profile) • Communicates cybersecurity requirements with stakeholders, including partners and suppliers (Profile) • Enables informed trade-off analysis of expenditure versus risk (Tiers)

Key Points about the Cybersecurity 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

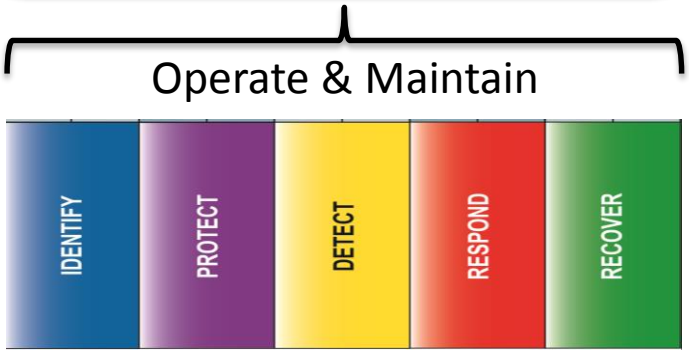
- **The framework is a living document**
  - It is intended to be updated over time as stakeholders learn from implementation, and as technology and risks change
  - That's one reason why the framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, and standards will change over time—principals will not

Where Should I Start?

(1) Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

(2a) Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk

(2b) Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.



Framework Version 1.0, Section 3.2, Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

Key Questions for New Technologies

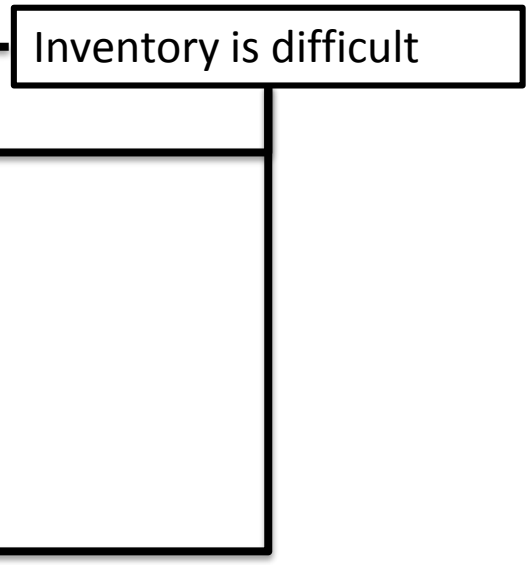
Overarching Question	Question	Who	Decision Materials
Proceed?	Will implementing the technology help me fulfill mission priorities?	Mission	ID.BE-3
	Will implementing the technology adversely affect the mission function of my current systems?	Technology	ID.AM-5
	Will implementing the technology introduce untenable risk?	Cyber Security	ID.RM-2/Profile *Inherent risks*
Proceed now?	Is it possible to implement this technology given my current infrastructure?	Technology	ID.AM-1, 2, & 3
	How can I minimize risk associated with this new technology: • in a way that supports my organization's requirements, and • within my finite budget?	Cyber Security	ID.RM-2/Profile *Inherent risks*
	How much security is 'enough' to implement this new technology?	Cyber Security	ID.RM-2/Profile
Hand-off to operations	What do I need to do to ensure on-going risk management of this new technology?	Cyber Security	*Remaining Categories*

Inherent Risks of Mobile Devices & Bring Your Own Device

- Inventory is difficult
  - Organization-supplied, personnel-supplied, hybrid
- Administrative diligence may be unknown or minimal
  - Patching, software baseline, security configuration management
- Mobile technologies bring increased possibility of malicious code to the enterprise due to increased attack surface and networks
  - Devices tend to connect to a large number of networks, the majority of which are not managed by the organization
  - Lots of spectrum per device (e.g., LTE, WiFi, GPS, Near Field Communication, Blue Tooth)
- Possibility of loosing control of organizational information as it is transported via mobile device
- Risk assessment before ‘go live’ is impossible and impractical
- Strong potential for personal data to traverse organizational networks

Assessing and Minimizing Inherent Risks

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications



Assessing and Minimizing Inherent Risks

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

ID.GV-3

ID.GV-1

Personal and organizational data is co-mingled

ID.GV-1: Organizational information security policy is established

ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners

ID.GV-3: Legal and regulatory requirements regarding cybersecurity,

Framework Roadmap Items

- 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

Since the 12 February 2014 Release of Framework 1.0

Request for Information: Experience with the Cybersecurity Framework
Questions focused on: awareness, experiences, and roadmap areas

August 26, 2014

6th Cybersecurity Framework Workshop
Goal: Raise awareness, encourage use as a tool, highlight examples of sector-specific efforts, implementation efforts, gather feedback

Oct. 29-30, 2014 Florida Center for Cybersecurity

Update on the Cybersecurity Framework
Summary posted that includes analysis of RFI responses, feedback from the 6th workshop, an update on Roadmap areas, and next steps

December 5, 2014

February 13, 2015
White House Releases Fact Sheet on Cybersecurity and Consumer Protection

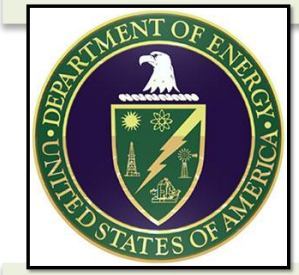
1 Year Anniversary of the Release
NIST Cybersecurity Framework site update to include: FAQs, Upcoming Events, and Industry Resources. Ongoing, targeted outreach continues

February 12, 2015

Examples of Framework Industry Resources

[The Cybersecurity Framework in Action: An Intel Use Case]

[Cybersecurity Guidance for Small Firms]



[Energy Sector Cybersecurity Framework Implementation Guidance]

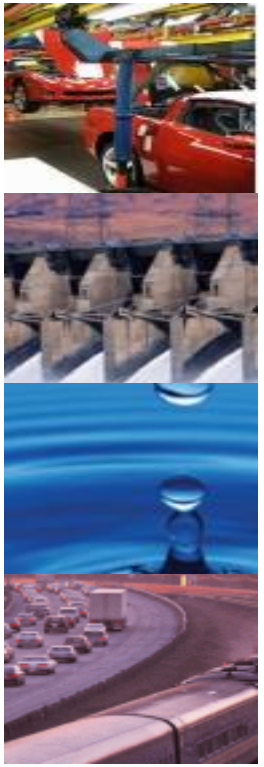
[Process Control System Security Guidance for the Water Sector]

[CFORUM] and other online communities of interest

Near Term Framework Activities

In summary, “Collect, Reflect, and Connect” – understand where industry is having success, help others understand those successes, and facilitate relationships that support understanding and use

- Continue education efforts, including creation of self-help and re-use materials for those who are new to the Framework
- Continue awareness and outreach with an eye toward industry communities who are still working toward basal Framework knowledge and implementation
- Educate on the relationship between Framework and the larger risk management process, including how organizations can use Tiers
- To allow for adoption, Framework version 2.0 is not planned for the near term



Resources

Where to Learn More and Stay Current

The National Institute of Standards and Technology Web site is available at http://www.nist.gov

NIST Computer Security Division Computer Security Resource Center is available at http://csrc.nist.gov/

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

For additional Framework info and help cyberframework@nist.gov