Cybersecurity Framework Development Overview

NIST's Role in Implementing Executive Order 13636
"Improving Critical Infrastructure Cybersecurity"

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

Executive Order 13636: Improving Critical Infrastructure Cybersecurity - February 12, 2013

“The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.”

“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”

Executive Order 13636

- Introduces efforts focused on:
  - Sharing of cybersecurity threat information
  - Building a set of current, successful approaches—a framework—for reducing risks to critical infrastructure

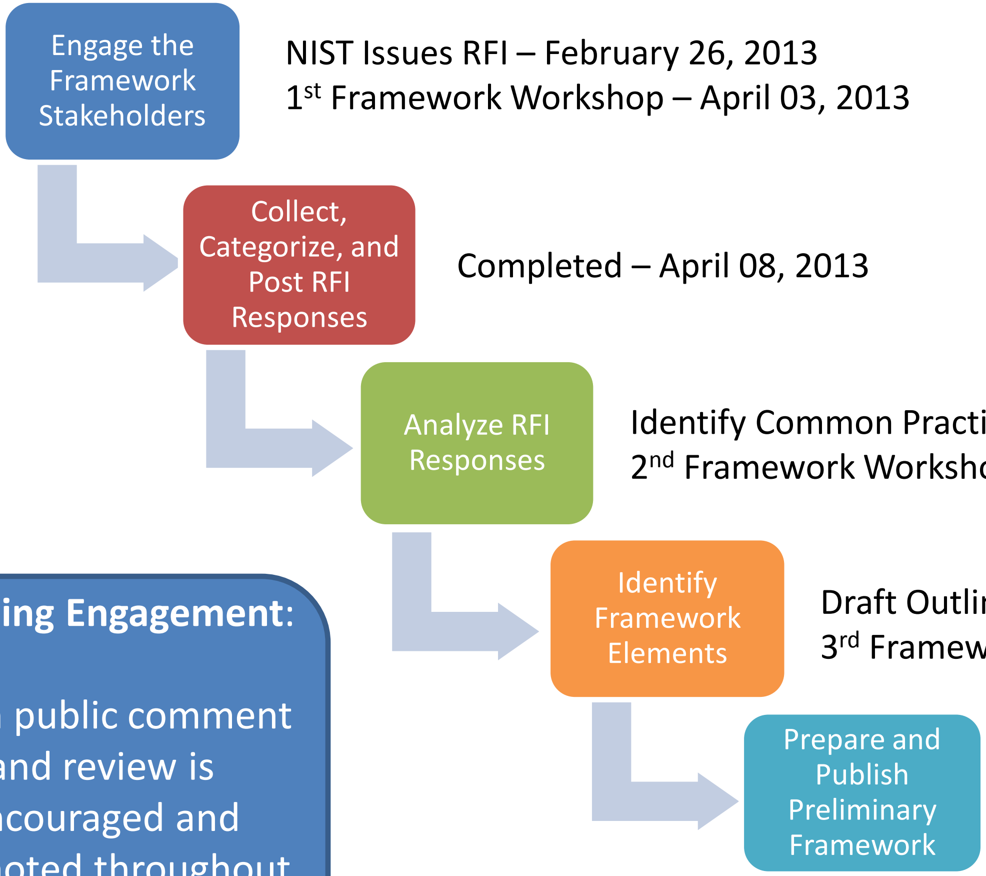
- The National Institute of Standards and Technology (NIST) is tasked with leading the development of a “Cybersecurity Framework” – a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

The Framework

To Structure the Framework to Meet The Requirements of the Executive Order, it 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 that should be addressed through future collaboration with particular sectors and standards-developing organizations to enable technical innovation and account for organizational differences, including guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

How Is the Framework being developed?



Engage the Framework Stakeholders

NIST Issues RFI – February 26, 2013
1st Framework Workshop – April 03, 2013

Collect, Categorize, and Post RFI Responses

Completed – April 08, 2013

Analyze RFI Responses

Identify Common Practices/Themes – May 15, 2013
2nd Framework Workshop at CMU – May 29-31, 2013

Identify Framework Elements

Draft Outline of Preliminary Framework – June 2013
3rd Framework Workshop at UCSD – July 10-12, 2013

Prepare and Publish Preliminary Framework

4th Framework Workshop – September 2013
Publish Preliminary Framework – October 2013

Ongoing Engagement:

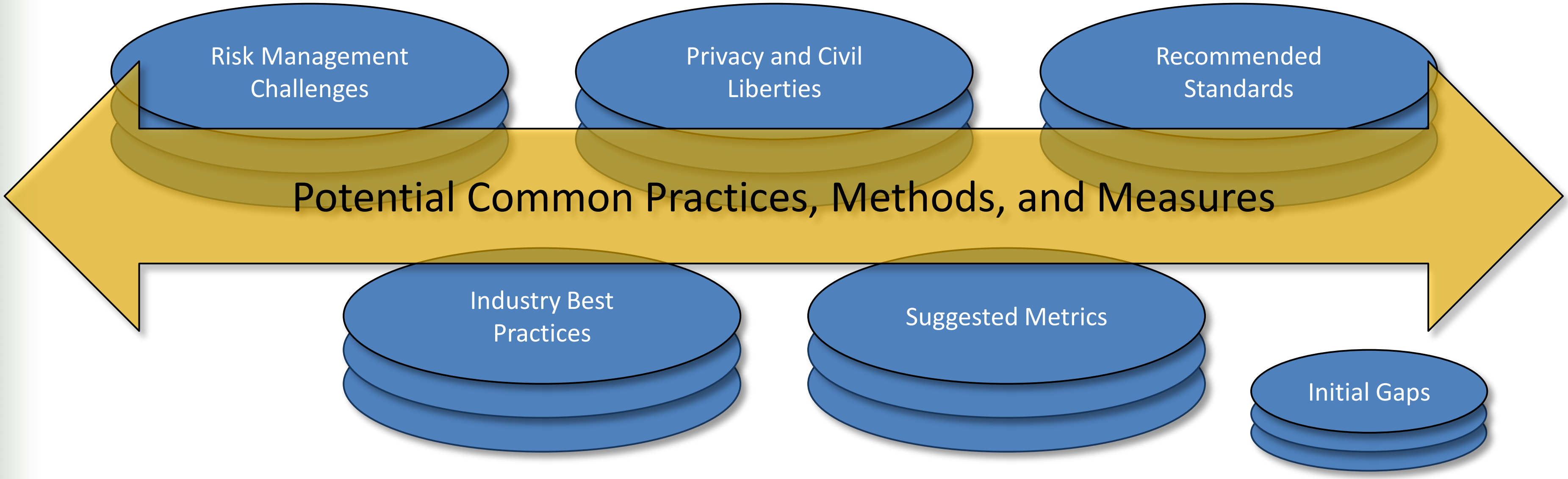
Open public comment and review is encouraged and promoted throughout the process

The NIST Framework Process

Analyze RFI Responses

Grouping of the RFI comments helped to:

- Identify repositories, content, and key points
- Identify gaps (e.g., lack of standards or input related to a topic)



Risk Management Challenges
Privacy and Civil Liberties
Recommended Standards
Potential Common Practices, Methods, and Measures
Industry Best Practices
Suggested Metrics
Initial Gaps

Cybersecurity Framework Principles, Common Themes, and Initial Gaps

Framework Principles	Common Themes	Initial Gaps
• Flexibility • Impact on Global Operations • Risk Management Approaches • Leverage Existing Approaches, Standards, and Best Practices	• Senior Management Engagement • Understanding Threat Environment • Business Risk / Risk Assessment • Separation of Business and Operational Systems • Models / Levels of Maturity • Incident Response • Cybersecurity Workforce	• Metrics • Privacy / Civil Liberties • Tools • Dependencies • Industry Best Practices • Resiliency • Critical Infrastructure Cybersecurity Nomenclature

The NIST Framework Process

Based on the responses to the RFI, conclusions from the workshops, and NIST analysis, the Preliminary Framework outline is designed to incorporate:

- Effective existing practices to inform an organization's risk management decisions
- A modular and flexible approach that supports business needs for organizations of different sizes and levels of maturity
- Organizational risk management processes that
  - Engage senior leadership in cybersecurity and
  - Integrate threat and vulnerability information with an understanding of potential impact to business needs
- A means for organizations to express the maturity of their cybersecurity risk management practices
- The expression of workforce awareness and training requirements
- The management of various types of dependencies

Draft Outline of Preliminary Framework

Identify Framework Elements

The draft outline of the Preliminary Framework includes the following:

- Executive Overview and Summary
- How To Use The Framework
- Framework's Risk Management Approach
  - Functions, Categories, Subcategories, and Informative References
  - Implementation Levels; Overarching Characteristics by both Role and Function, Categories, and Subcategories
- Compendium of Informative References (Standards, Guidelines, Practices)
- Glossary

What do we expect to accomplish at this workshop?

This workshop is focused on:

- Discussing and refining the draft Outline
- Generating content for the Preliminary Framework
- Specific topics that inform the Preliminary Framework

The Draft Preliminary Framework…

- Provides an Executive Overview for senior leadership
- Describes the Framework Development Process
- Discusses and describes how to use the Framework
- Describes the Framework’s Risk Management Approach
- Provides illustrative Framework examples
- Defines Terms and Acronyms

The Cybersecurity Framework Elements

- Functions
- Categories
- Subcategories
- Compendium of Informative References
- Framework Implementation Levels
- Roles

The Framework Core

Function	Category	Sub-Category	Informative Reference(s)	FIL1	FIL2	FIL3	Role
Function …				FIL 1 Chars	FIL 2 Chars	FIL 3 Chars	Senior Executive
	Category …			FIL 1 Chars	FIL 2 Chars	FIL 3 Chars	Business Process Manager
		Subcat 1	Ref 1 Ref …	FIL 1 Chars	FIL 2 Chars	FIL 3 Chars	Operations Manager
		Subcat 2	Ref 1 Ref …	FIL 1 Chars	FIL 2Chars	FIL 3 Chars	
		Subcat …	Ref 1 Ref …	FIL 1 Chars	FIL 2 Chars	FIL 3 Chars	

Functions

Know – Gaining the institutional understanding to identify what systems need to be protected, assess priority in light of organizational mission, and manage processes to achieve cost effective risk management goals

Prevent – Categories of management, technical, and operational activities that enable the organization to decide on the appropriate outcome-based actions to ensure adequate protection against threats to business systems that support critical infrastructure components.

Detect – Activities that identify (through ongoing monitoring or other means of observation) the presence of undesirable cyber risk events, and the processes to assess the potential impact of those events.

Respond – Specific risk management decisions and activities enacted based upon previously implemented planning (from the Prevent function) relative to estimated impact.

Recover – Categories of management, technical, and operational activities that restore services that have previously been impaired through an undesirable cybersecurity risk event.

Categories, Subcategories, and Informative References

- **Categories**
  - Logical subdivision of a function; one or more categories comprise a function.
  - Examples may include “Know the enterprise assets and systems”, “Implement access control”, “Implement risk monitoring & detection”, “Perform incident response”, and “Perform system recovery”.

- **Subcategories**
  - Logical subdivision of a category; one or more subcategories comprise a category.
  - Examples may include “Inventory hardware assets”, “Restrict and protect remote access”, and “Perform incident handling activities as described in the incident handling plan”.

- **Informative References**
  - Existing cybersecurity-related standards, guidelines, and practices.

The Compendium of Informative References

- A listing of submitted Informative References (e.g., standards, guidelines, and best practices)
  - Issuing Organization
  - Title
  - Type
  - Source
  - Description
  - Sector-Specific or General
  - Sector(s) Referenced in RFIs / Cross Sector Application
  - RFI Sources

- Informative and illustrative resource
  - Not an endorsement of any included

Roles and Framework Implementation Levels (FIL)

Function	Category	Sub-Category	Informative Reference(s)	FIL1	FIL2	FIL3	Role
Function …				FIL 1 Chars	FIL 2 Chars	FIL 3 Chars	Senior Executive
	Category …			FIL 1 Chars	FIL 2 Chars	FIL 3 Chars	Business Process Manager
		Subcat 1	Ref 1 Ref …	FIL 1 Chars	FIL 2 Chars	FIL 3 Chars	Operations Manager
		Subcat 2	Ref 1 Ref …	FIL 1 Chars	FIL 2Chars	FIL 3 Chars	
		Subcat …	Ref 1 Ref …	FIL 1 Chars	FIL 2 Chars	FIL 3 Chars	

Framework Implementation Levels (FILs)

- Express, by role, the characteristics of the level of maturity of an organization for each function, category, and subcategory
- Reflect the organizational cybersecurity maturity by implementing the Framework
- Allow the organization to assess their cybersecurity risk and readiness
- Provide an indicator and measure of an organization’s performance that can be assessed in terms of managing risk
- Guidance for measuring the performance of an entity in implementing the Cybersecurity Framework

Framework Implementation Level – Senior Executive

Function	FIL1	FIL2	FIL3	Role
KNOW	I understand the organizational components that need to be protected. I have provided resources to support corporate knowledge of risk management components such as vulnerabilities, threats, and risk assessment.	I understand the organizational components that need to be protected, their value, their threats, the impact of cyber risk events, and the likelihood of those events.	I understand the organizational components that need to be protected and the true impact of cybersecurity events on them. I have integrated cybersecurity risk management into the enterprise risk management model.	Senior Executive

Framework Implementation Level – Business Process Manager

Function	Category	FIL1	FIL2	FIL3	Role
KNOW	Asset Management	I understand the importance of asset management and assume responsibility for lifecycle accountability.	Asset management policies and procedures are in place.	I understand how different groups of assets impact the various business objectives. I ensure that resources are available for all aspects of the asset management lifecycle.	Business Process Manager

Framework Implementation Level – Operations Manager

Function	Category	Sub-Category	Informative Reference(s)	FIL1	FIL2	FIL3	Role
KNOW	Asset Mgt	Hardware /Software Inventory	ISO/IEC 27001	An ad hoc asset tracking process is in place	A formal asset tracking process is in place with defined periodic revalidation of assets	Automated asset tracking exists with real-time validation and visualization.	Operations Manager
		Network Mapping	ISO/IEC 27002	FIL 1 Chars	FIL 2 Chars	FIL 3 Chars	

- Q & A