Cybersecurity Framework Development Overview

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

Adam Sedgewick
Senior IT Policy Advisor
IT Laboratory

NIST
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."

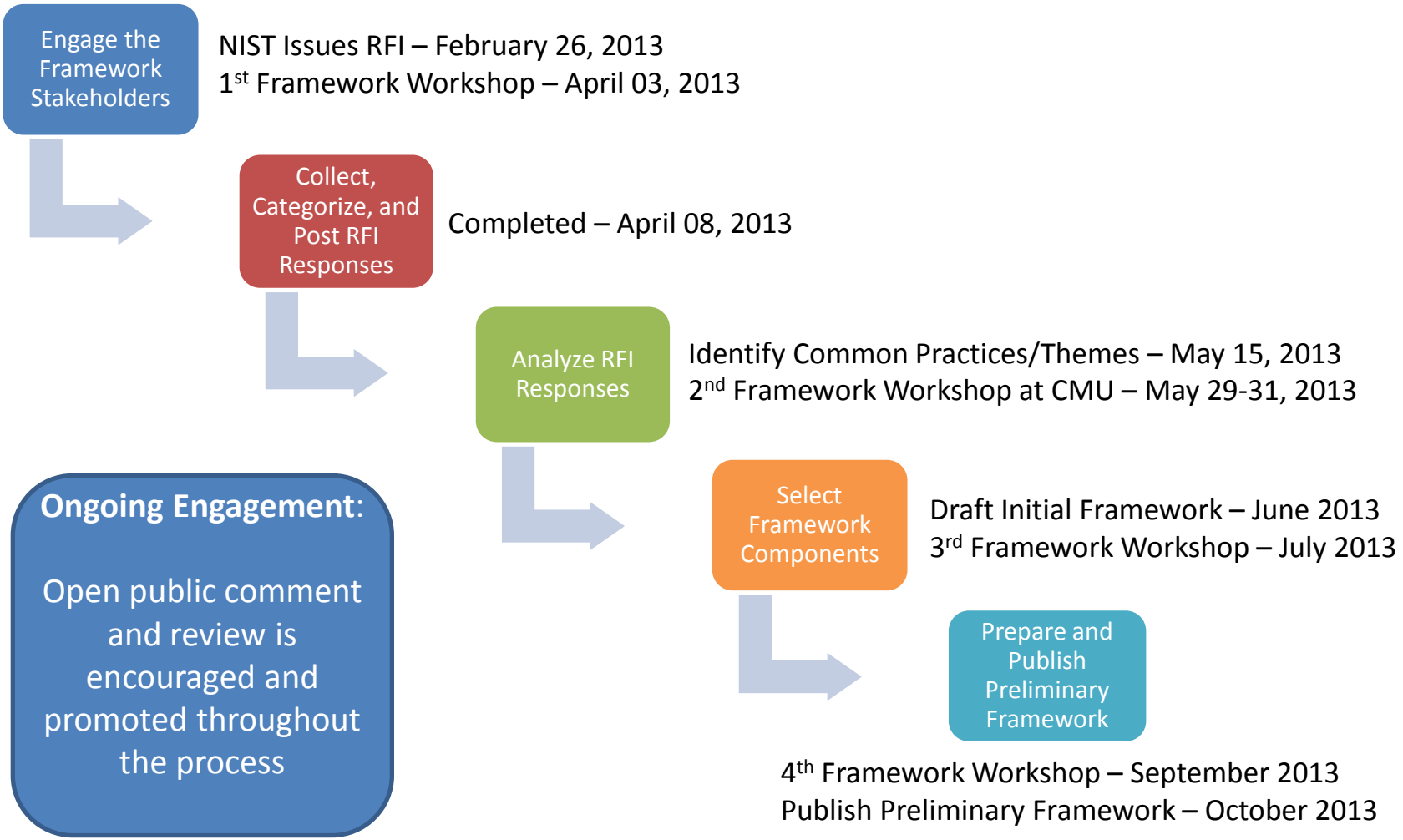
"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

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.

How Will the Framework be Developed?

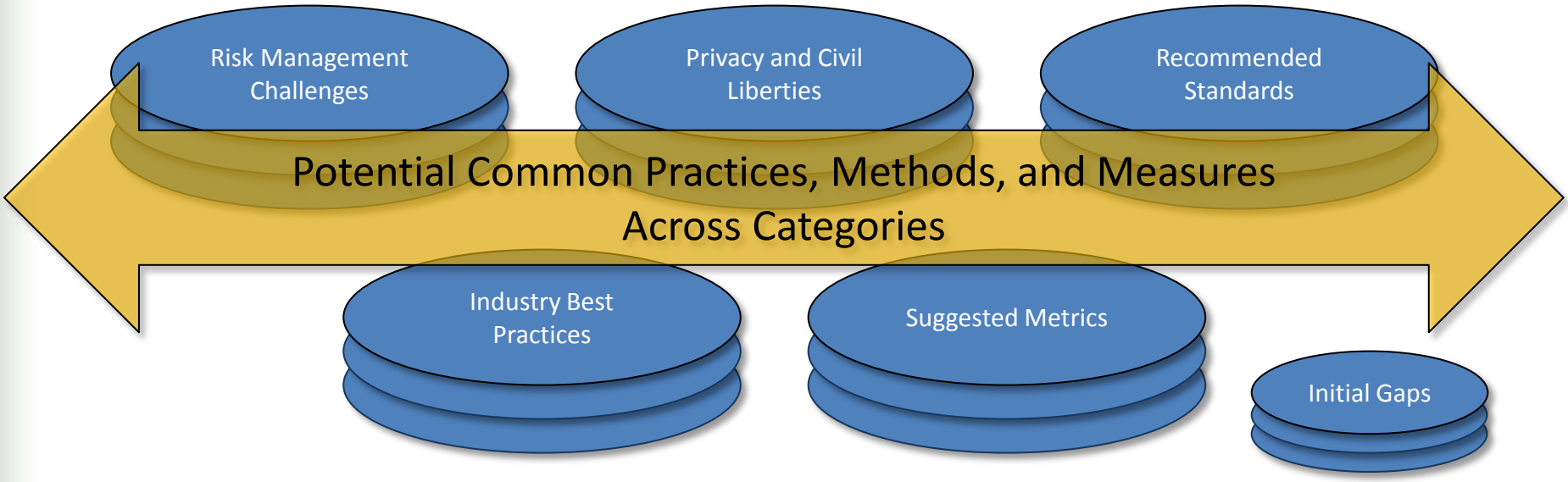


The NIST Framework Process

Analyze RFI Responses

Grouping of the RFI comments helped to:

- Identify common themes (e.g., practices having wide utility and adoption)
- Identify omissions (e.g., lack of standards or input related to a topic)



Cybersecurity Framework Categories and Themes

Category	Framework Principles	Common Points	Initial Gaps
Themes	• 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

Select Framework Components

The selection of Framework components is focused on identifying practices and approaches that support EO objectives (and related principles, practices, and measures) while continuing to support business needs.

Related Principles, Practices, and Measures:

- Fair Information Practice Principles
- Risk Assessment Method
- Critical Infrastructure Threat Model
- Workshop Inputs
- RFI Derived
- Performance Measures

Common Practices, Methods, and Measures

Does the practice, method, or measure support a core EO objective?

Identify Candidate Framework Components

a. **A candidate practice, method, or measure must demonstrate alignment with and support for some core EO objective to be considered for inclusion as a framework component**

b. **If a candidate practice, method, or measure does not operate in support of core a EO objective then it is not considered for inclusion in the framework**

c. **If, within the initial RFI inputs, no candidate practice, method or measure can be identified for a core EO objective, a gap exists**

The NIST Framework Process

Select Framework Components

- Draft initial Framework from the candidate framework components

- Present the Framework in a manner that is:
  - Usable
  - Clear and unambiguous
  - Suitable for multiple audiences
  - Multi-tiered
  - Practical and implementable

- Discuss and refine initial Framework at the 3rd Cybersecurity Framework Workshop

Topics for Discussion

Key topics for discussion throughout Framework development include:

- How to effectively present the Framework
- How to promote voluntary implementation
- Identification and resolution of gaps
- Framework sustainment (e.g., maintenance, frequency of updates, ensuring relevance and applicability)
- Governance models for out years
- Measuring and metrics
- Emerging capabilities/practices to potentially scope in