Cybersecurity Framework Development Overview

**NIST's Role in Implementing Executive Order 13636
"Improving Critical Infrastructure Cybersecurity"
Presentation to the Visiting Committee on Advanced Technology**

**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."

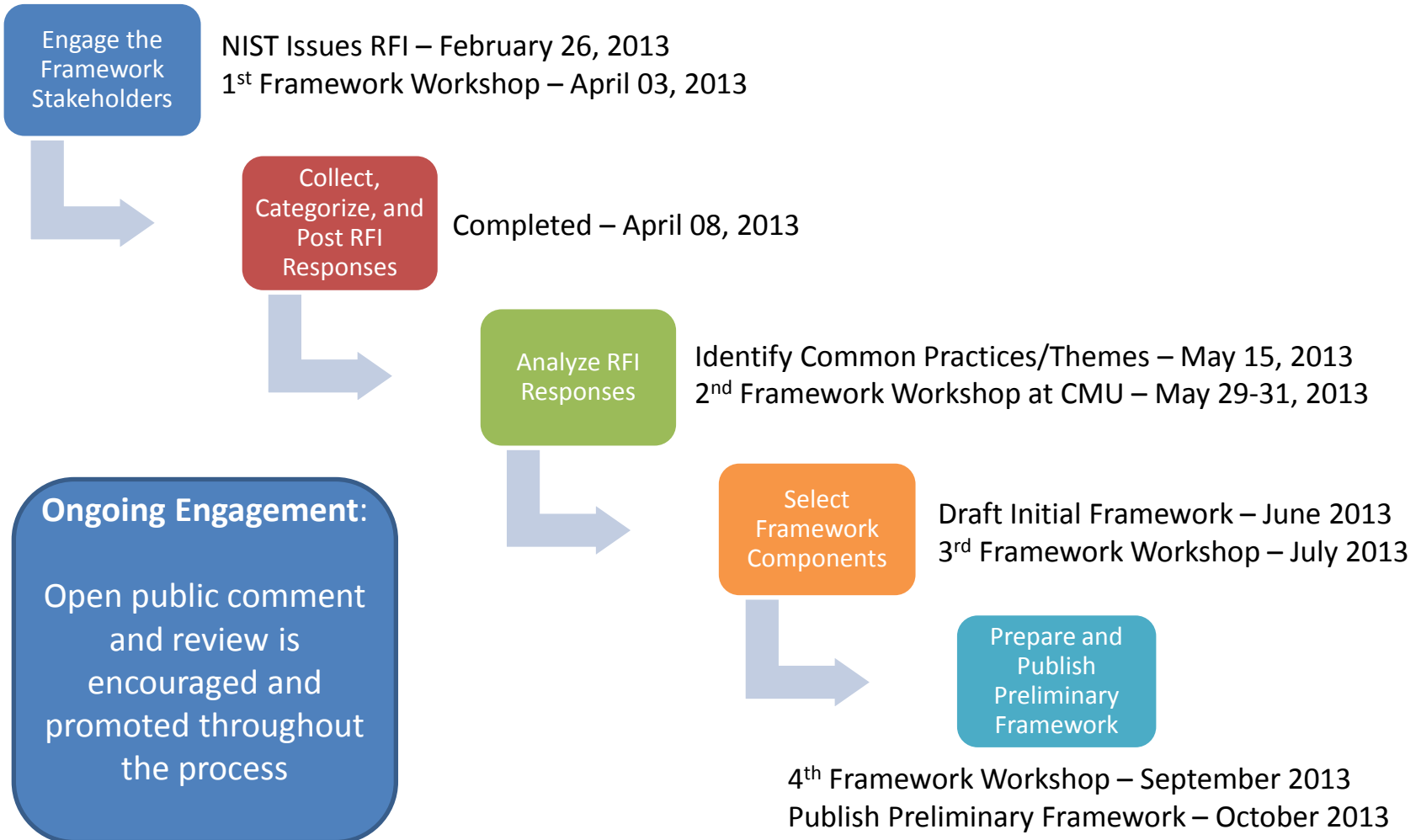"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

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.
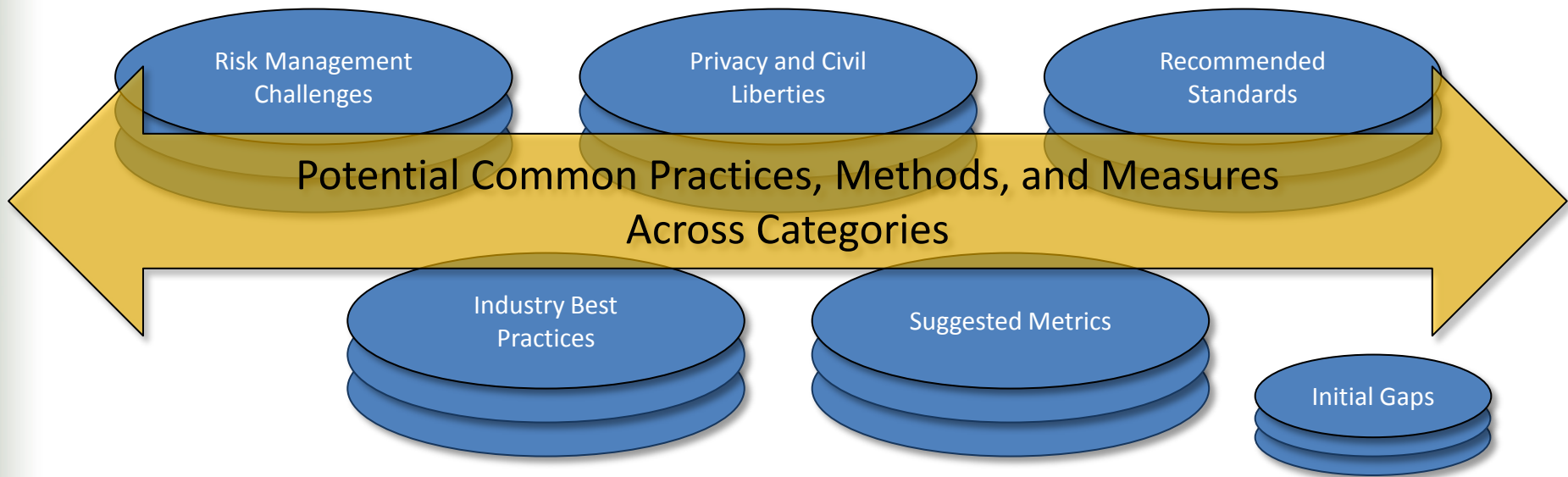
How Will the Framework be Developed?

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

Select Framework Components

Draft Initial Framework – June 2013
3rd Framework Workshop – July 2013

Prepare and Publish Preliminary Framework

Ongoing Engagement:

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

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

The NIST Framework Process

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)

Risk Management Challenges

Privacy and Civil Liberties

Recommended Standards

Potential Common Practices, Methods, and Measures Across Categories

Industry Best Practices

Suggested Metrics

Initial Gaps

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

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

The NIST Framework Process

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

- 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