Cybersecurity Framework Development Overview

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

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"

https://www.federalregister.gov/executive-order/13636

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 this “Cybersecurity Framework”

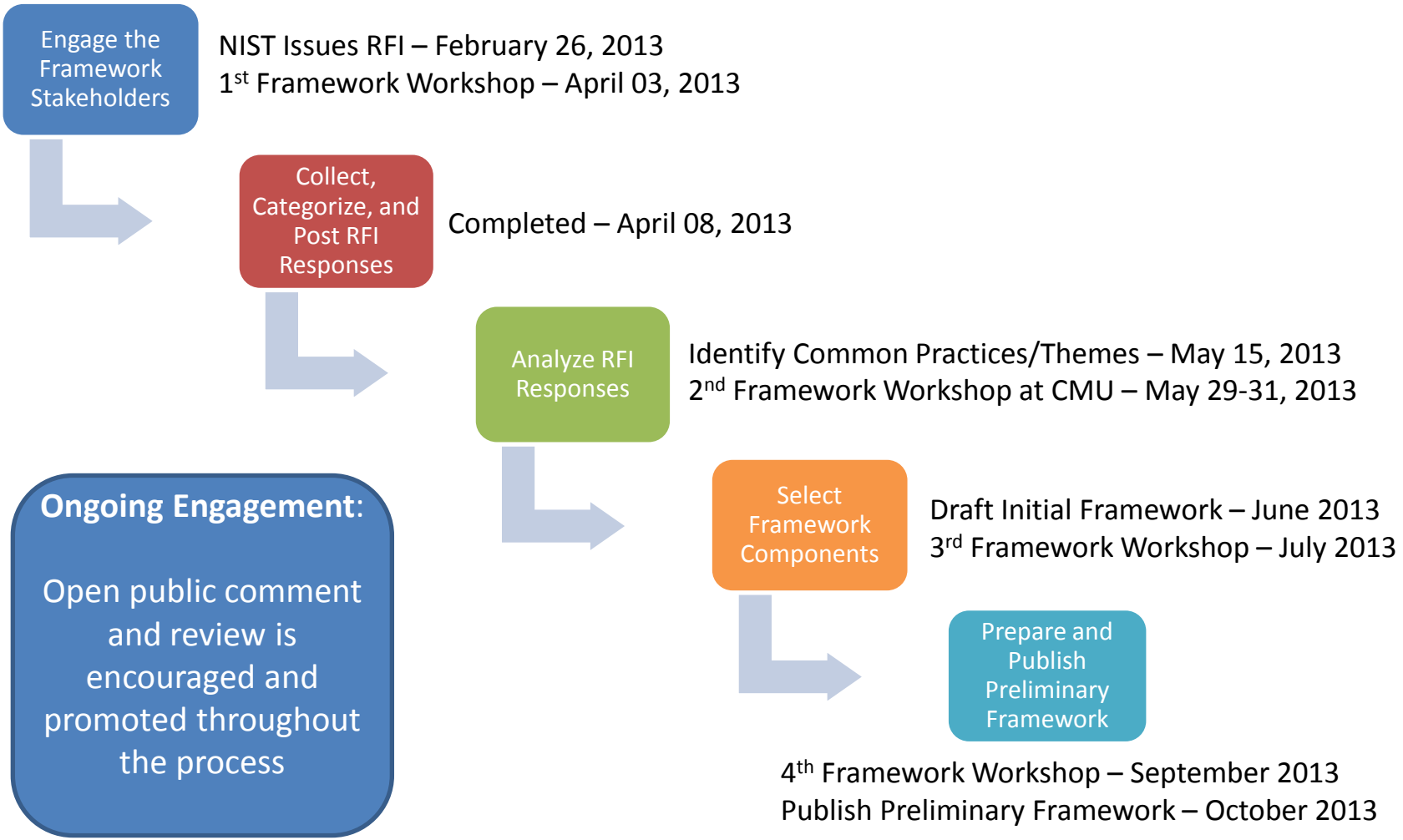
Why NIST?

- Non-regulatory federal agency
- Unbiased source of scientific data and practices
- Mission is to promote U.S. innovation and industrial competitiveness
- Long history of successful partnerships with industry, other government agencies, and academia to address critical national issues

The Cybersecurity Framework will

- Identify security standards and guidelines applicable across sectors of critical infrastructure, while identifying areas that should be addressed through future collaboration with particular sectors and standards-developing organizations
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach
- Help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Provide guidance that is technology neutral and enables critical infrastructure sectors to benefit from a competitive market for products and services
- Include guidance for measuring the performance of implementing the Cybersecurity Framework
- Include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on **business confidentiality**, and to protect individual **privacy and civil liberties**

How Will the Framework be Developed?



The NIST Framework Process

Engage the Framework Stakeholders

- Feb. 26, 2013: NIST issued a Request for Information (RFI) in the Federal Register https://federalregister.gov/a/2013-04413

- NIST sought comments regarding:
  - Current risk management practices
  - Use of frameworks, standards, guidelines, best practices
  - Specific industry practices

- April 8, 2013: RFI comments received

The NIST Framework Process

Collect, Categorize, and Post RFI Responses

- RFI responses were received by NIST and cataloged
  - Date of receipt
  - Submitter
  - Sector affiliation (e.g., energy, transportation)
  - Organization type (e.g., company, association)

- RFI responses were posted to the NIST Cybersecurity Framework website http://csrc.nist.gov/cyberframework/rfi_comments.html

The NIST Framework Process

Analyze RFI Responses

RFI content was reviewed and comments were grouped by the topics they address:

- Regulation/Legal
- Conformity/Standards
- Metrics
- Current practice
- Future practice
- Privacy/Civil liberties
- Framework Development
- Other

The NIST Framework Process

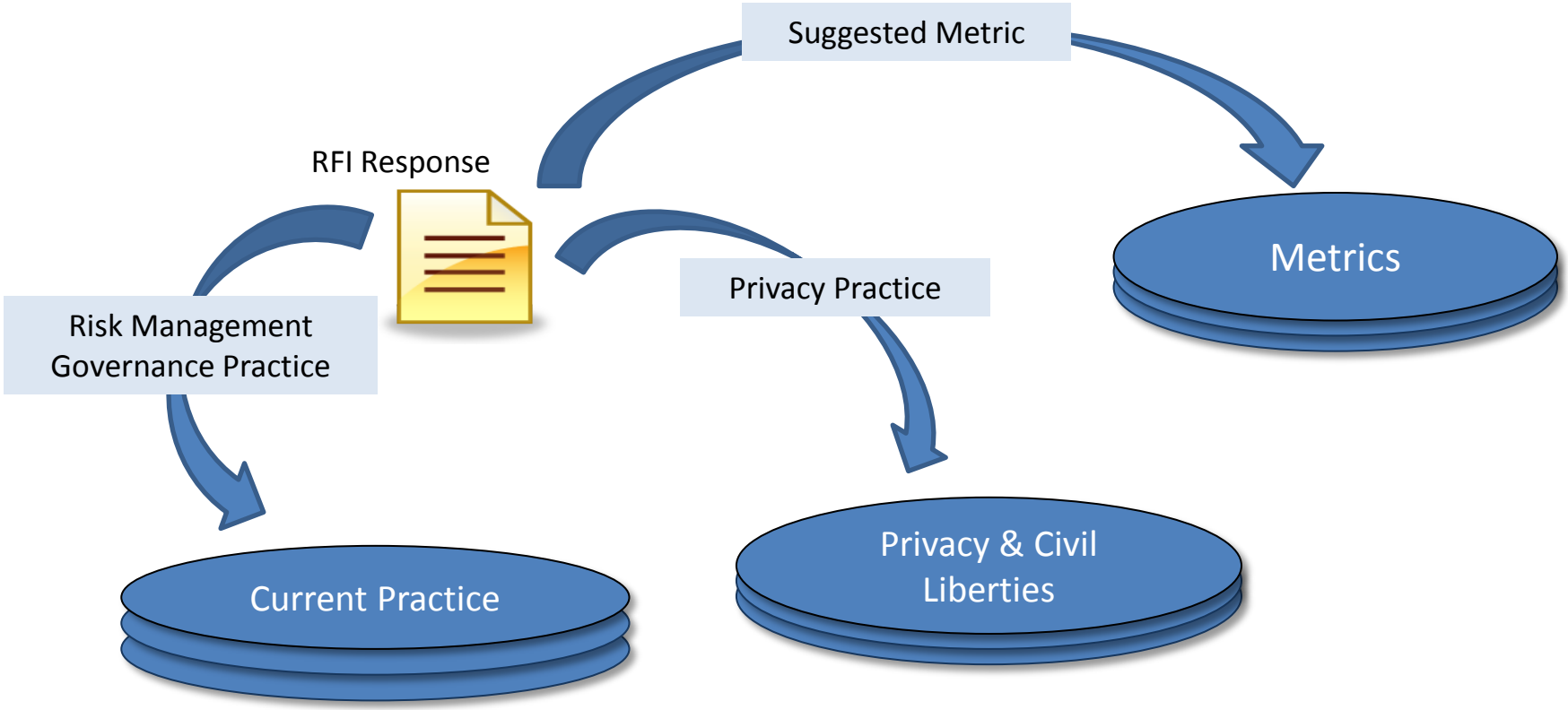
Analyze RFI Responses

The analysis of each RFI response included:

- Identifying sections of text relevant to one or more RFI questions
- Parsing and copying text sections into the EO Analysis Database
- Assigning the text to one or more relevant categories or sub-categories
- Tagging the text with “keywords” to facilitate searching and correlation
- Utilizing the categorizations and keywords to identify commonalities and recurring themes

Example of RFI Analysis

Analyze RFI Responses



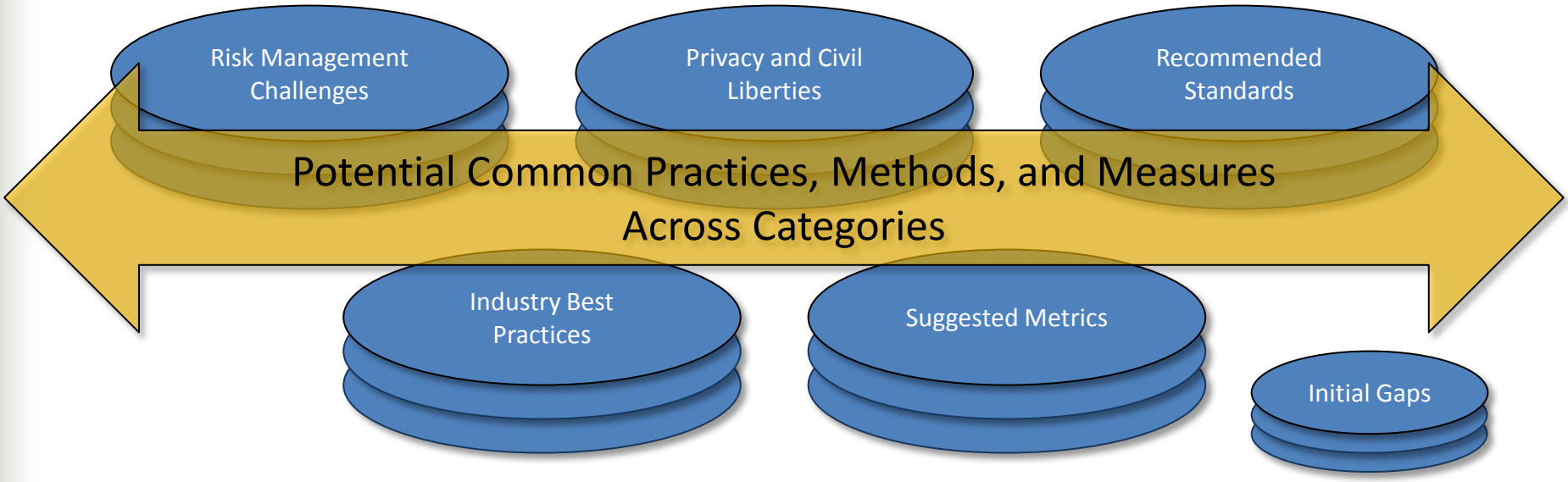
RFI Comments are Parsed and Grouped into Categories

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)



The NIST Framework Process

Analyze RFI Responses

The recurring and common themes were separated into three categories:

- Framework Principles: Critical characteristics and considerations the framework must encompass
- Common points: Practices having wide utility and adoption
- Initial Gaps: Areas where sufficient information was not provided from RFI responses

The NIST Framework Process

Select Framework Components

The Cybersecurity Framework will include approaches that:

- Are successfully used by organizations across a variety of sectors

AND

- Satisfy the criteria established in Executive Order 13636
  - Afford appropriate protections for privacy and civil liberties – using the Fair Information Practice Principles
  - Maintain business confidentiality
  - Are flexible, repeatable, performance-based, cost-effective, and technology neutral
  - Are well-aligned with established performance measures

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

The NIST Framework Process

Prepare and Publish Preliminary Framework

Key activities during this stage include:

- Validate draft Framework
- Confirm and document observed gaps
- Discuss action plans to address gaps
- Ensure Framework is well-aligned with established performance goals
- Present Preliminary Framework
- Refine Preliminary Framework at the 4th Cybersecurity Framework Workshop

Topics for Discussion for this Week and Beyond

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