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

According to the Executive Order, the Cybersecurity Framework will

- Identify security standards and guidelines applicable across sectors of critical infrastructure
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach
- Help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Enable technical innovation and account for organizational differences
- 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
- Identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations

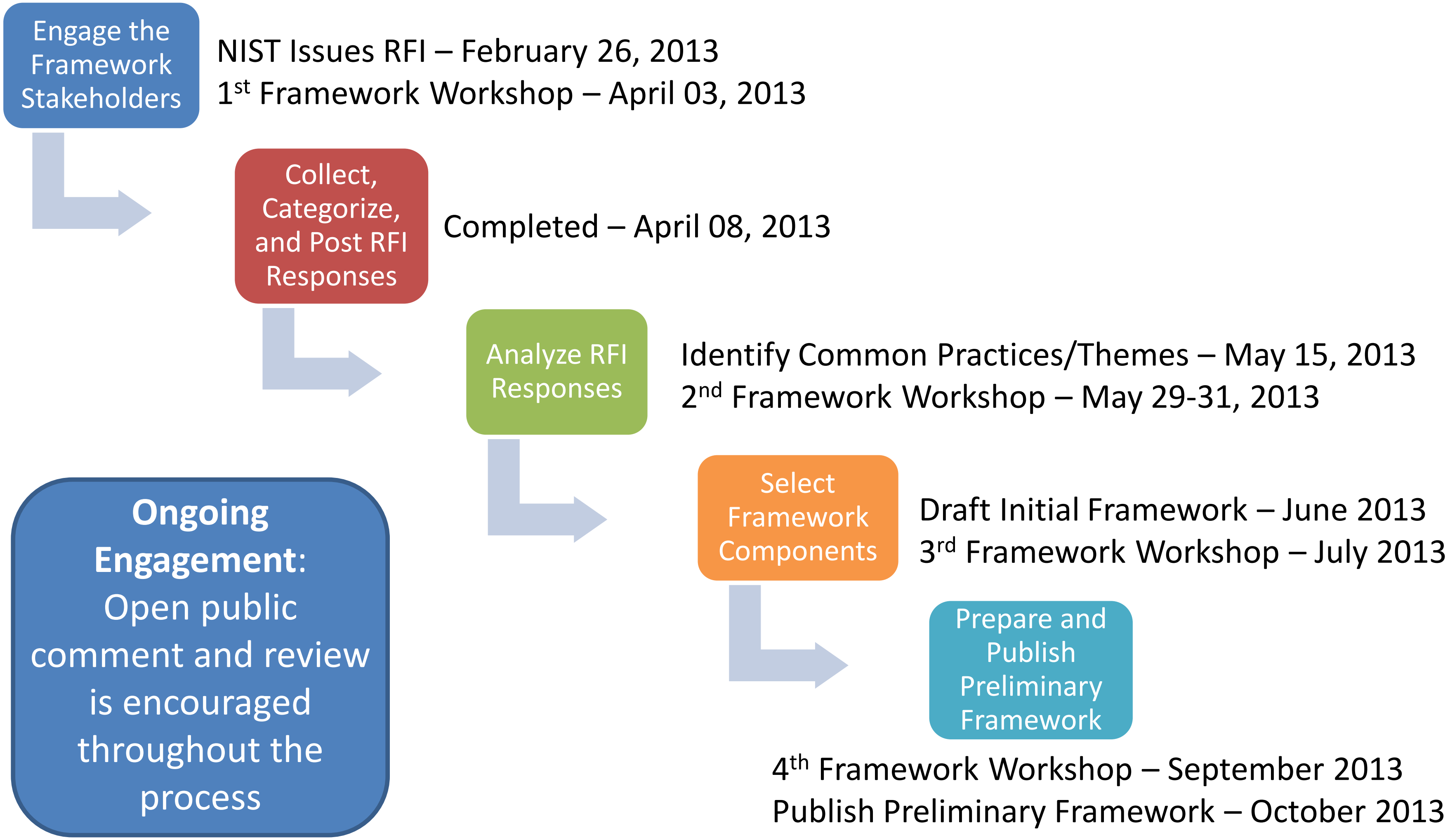
The Cybersecurity Framework: What it will…

According to the Executive Order, the Cybersecurity Framework shall	**That is, the framework will**
"Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks"	Be built in collaboration with stakeholders in government and industry, both users and innovators of cybersecurity solutions
"Incorporate voluntary consensus standards and industry best practices to the fullest extent possible"	Ask industry members to shape the framework by sharing the solutions they use

… And won’t do

According to the Executive Order, the Cybersecurity Framework shall	**That is, the framework will**
“Be consistent with voluntary international standards when such international standards will advance the objectives of the order”	**NOT** introduce new standards when existing voluntary standards are available that meet the objectives of the order
“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”	**NOT** introduce practices that compromise protection of intellectual property, privacy, or civil liberties

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

Identify Common Practices/Themes – May 15, 2013

2nd Framework Workshop – May 29-31, 2013

Select Framework Components

Draft Initial Framework – June 2013

3rd Framework Workshop – July 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 throughout the process

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 due

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

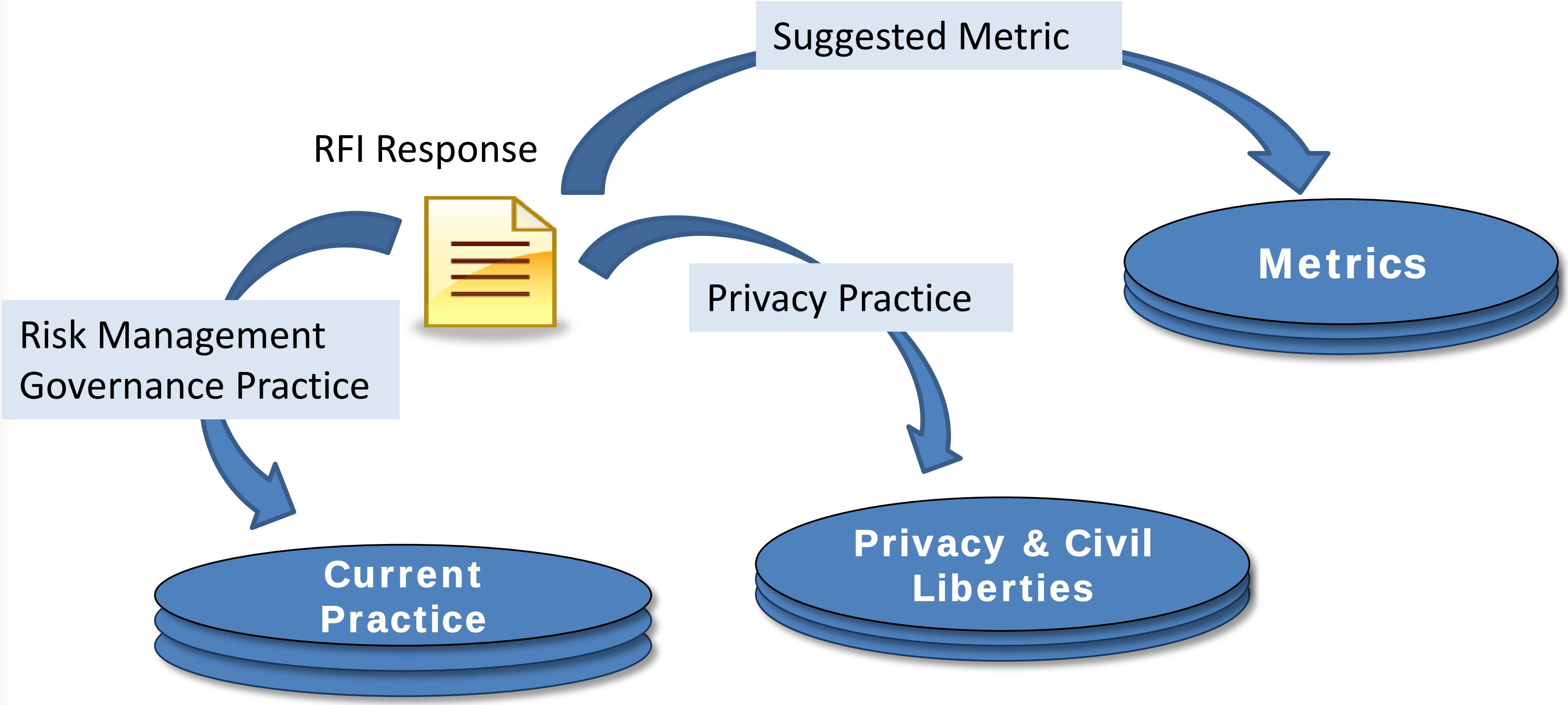
Analyze RFI Responses

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

Example of RFI Analysis

Analyze RFI Responses



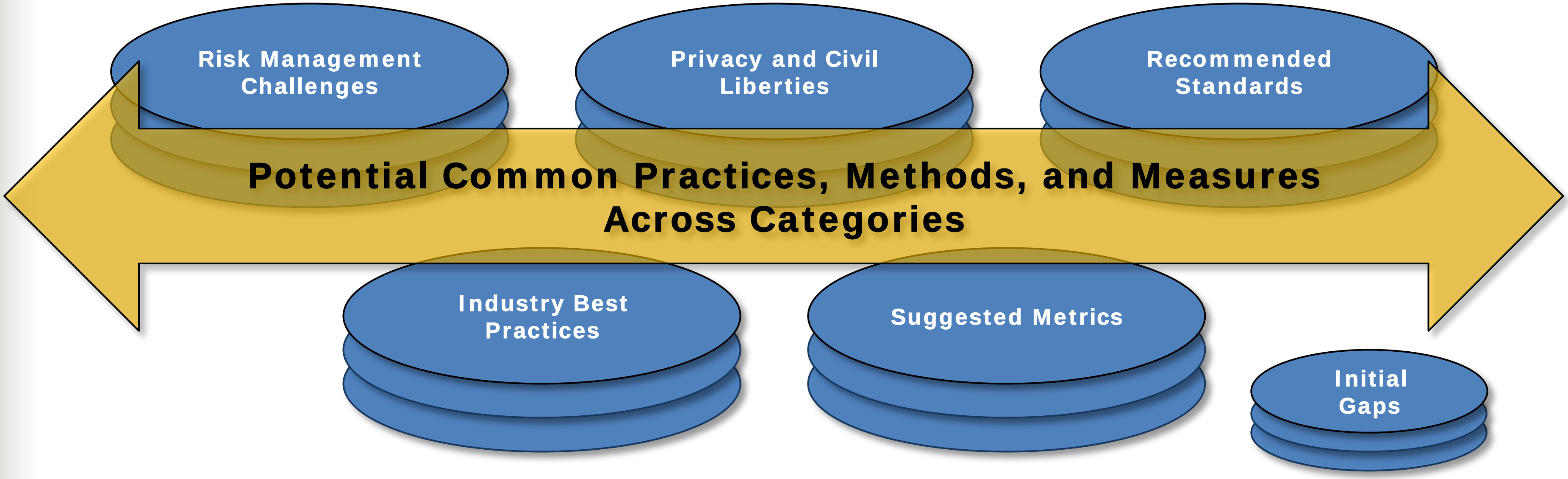
RFI Comments are Parsed and Grouped into Categories

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 initial 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 Across Categories
Industry Best Practices
Suggested Metrics
Initial Gaps

The NIST Framework Process

Analyze RFI Responses

The analysis of each RFI response included:

- Analysis of response coverage across critical infrastructure sectors and organization types
- Identification of sections of text relevant to one or more of the RFI questions
- Categorization of relevant text to category/sub-category
- Specification of terms and phrases that identify key points in each categorized section of relevant text.
- Utilizing the categorizations and keywords to identify commonalities and recurring themes

The NIST Framework Process

Analyze RFI Responses

The recurring and common themes were separated into three groupings:

Framework Principles: Characteristics and considerations the Framework must encompass.

Common Points: Practices identified as having wide utility and adoption.

Initial Gaps: For the purposes of RFI input analysis, initial gaps are those areas where RFI responses were not sufficient to meet the goal of the Executive Order.

The NIST Framework Process

Analyze RFI Responses

- Discuss initial RFI analysis at the 2nd Cybersecurity Framework Workshop

When: May 29-31, 2013

Where: Carnegie Mellon University, Pittsburgh, PA

Additional Workshop Information is available at:

http://www.nist.gov/itl/csd/cybersecurity-framework-workshop-may-29-31-2013.cfm

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

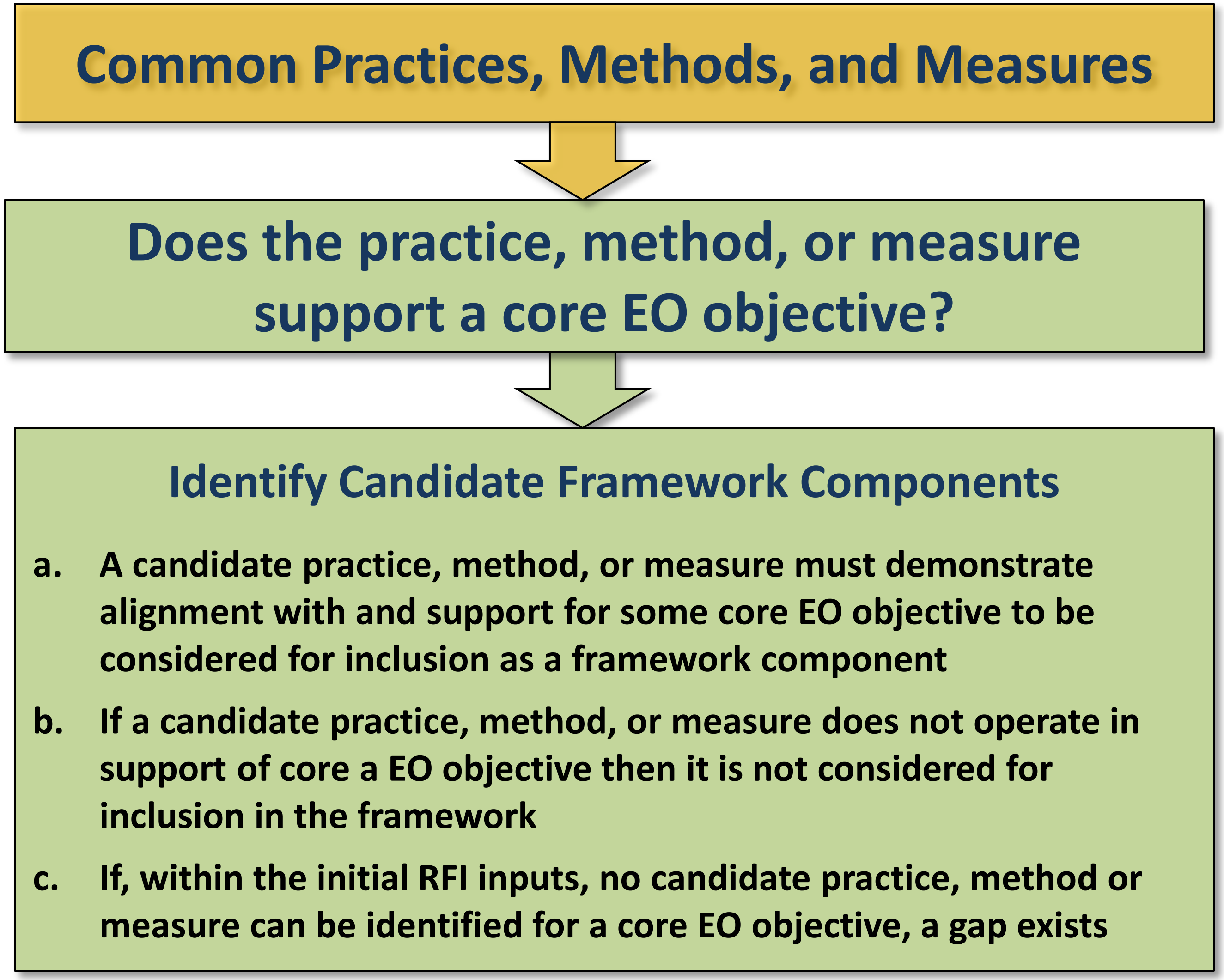
The NIST Framework Process

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

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

Questions