Cybersecurity Framework Overview

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

"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"

- NIST is directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure

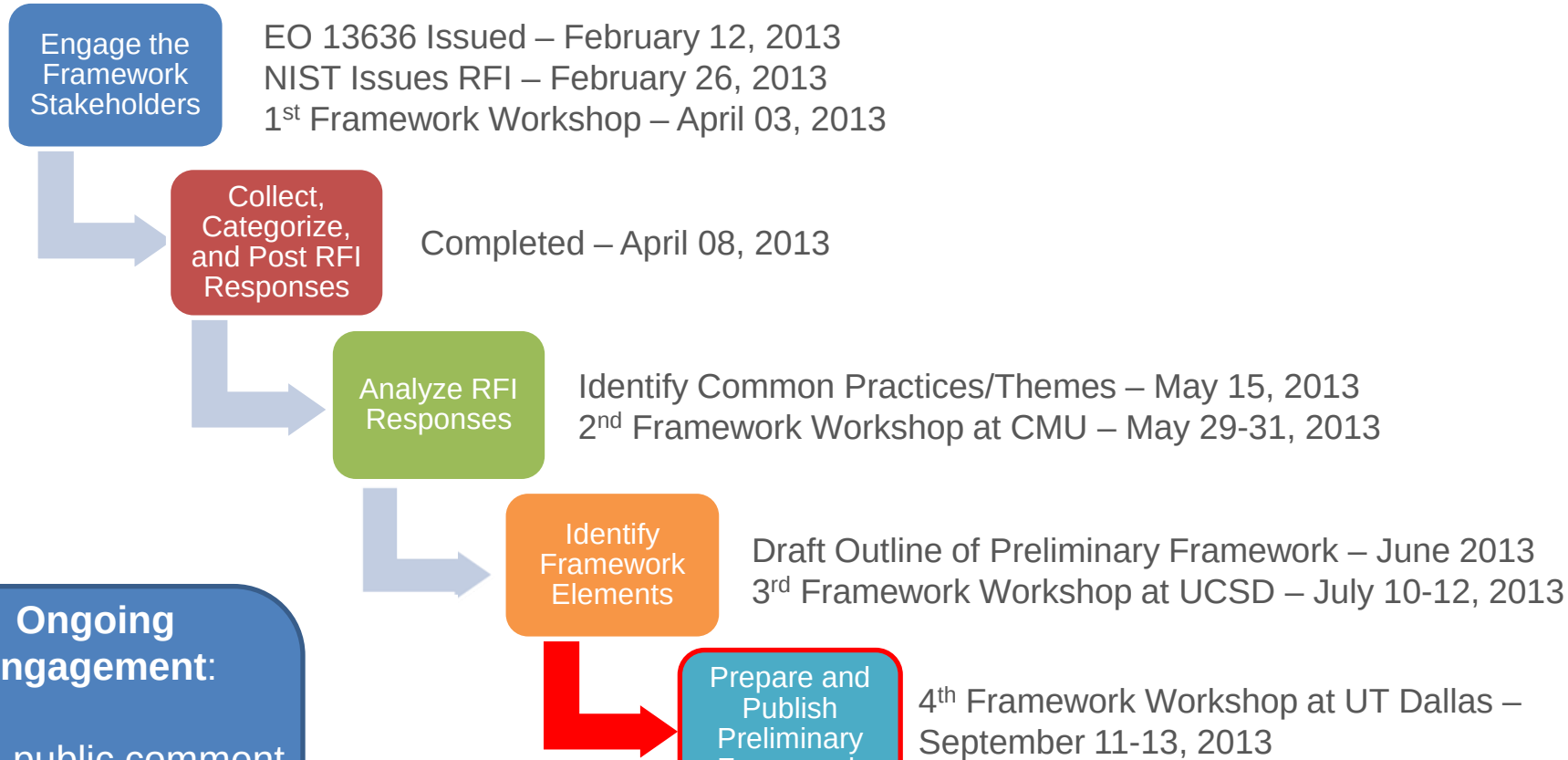
- This Cybersecurity Framework is being developed in an open manner with input from stakeholders in industry, academia, and government, including a public review and comment process, workshops, and other means of engagement.

The Cybersecurity Framework

For the Cybersecurity 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 able technical innovation and account for organizational differences include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

Development of the Preliminary Framework



NIST issued a Request for Information

- The purpose of the RFI was to:
  - Gather relevant input from industry and other stakeholders on the many interrelated considerations in developing the Framework
  - Encourage stakeholder participation in the Cybersecurity Framework development process

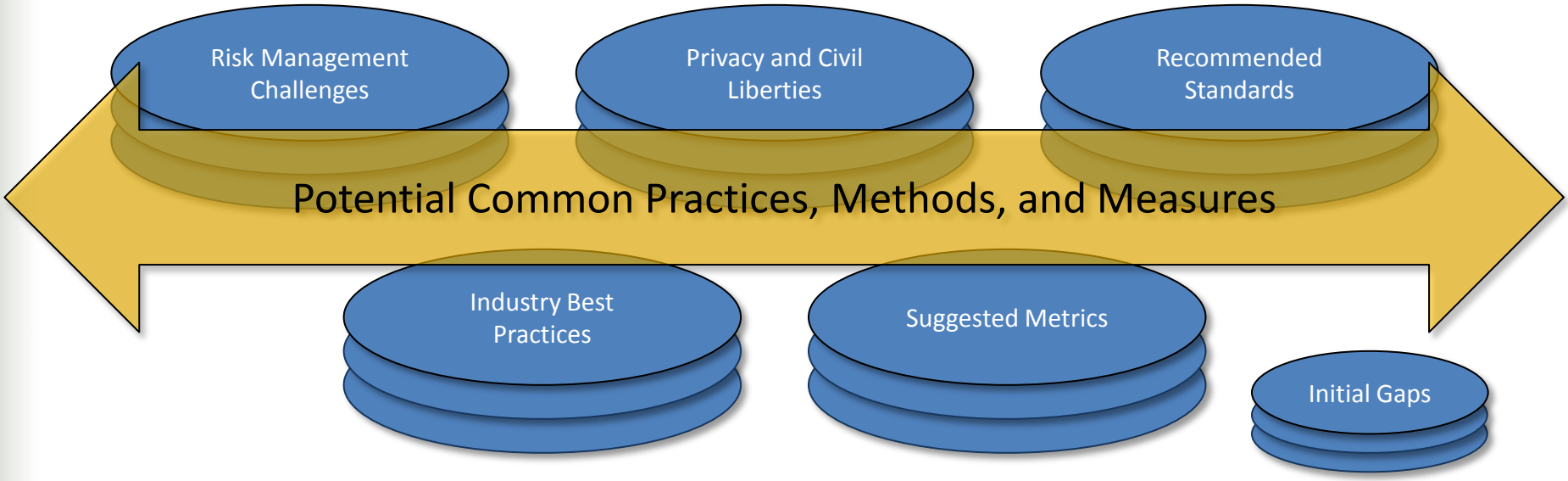
- Over 240 responses received from industry, associations, academics, and individuals

- NIST presented an initial analysis to describe the methodology used to perform the analysis, and to identify and describe the Cybersecurity Framework themes that emerged as part of the initial analysis.
  - This initial analysis served as the basis for discussion at Workshop #2 at Carnegie Mellon University.

The NIST Framework Process

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)



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 • **Cybersecurity Workforce** • Business Risk / Risk Assessment • Separation of Business and Operational Systems • Models / Levels of Maturity • Incident Response	• Metrics • Privacy / Civil Liberties • Tools • Dependencies • Industry Best Practices • Resiliency • Critical Infrastructure Cybersecurity Nomenclature

Framework Core: Functions

The five Framework Core Functions provide the highest level of structure:

- **Identify** – Develop the institutional understanding of which organizational systems, assets, data, and capabilities need to be protected, determine priority in light of organizational mission, and establish processes to achieve risk management goals.
- **Protect** – Develop and implement the appropriate safeguards, prioritized through the organization's risk management process, to ensure delivery of critical infrastructure services.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement the appropriate activities, prioritized through the organization's risk management process (including effective planning), to take action regarding a detected cybersecurity event.
- **Recover** - Develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the appropriate capabilities that were impaired through a cybersecurity event.

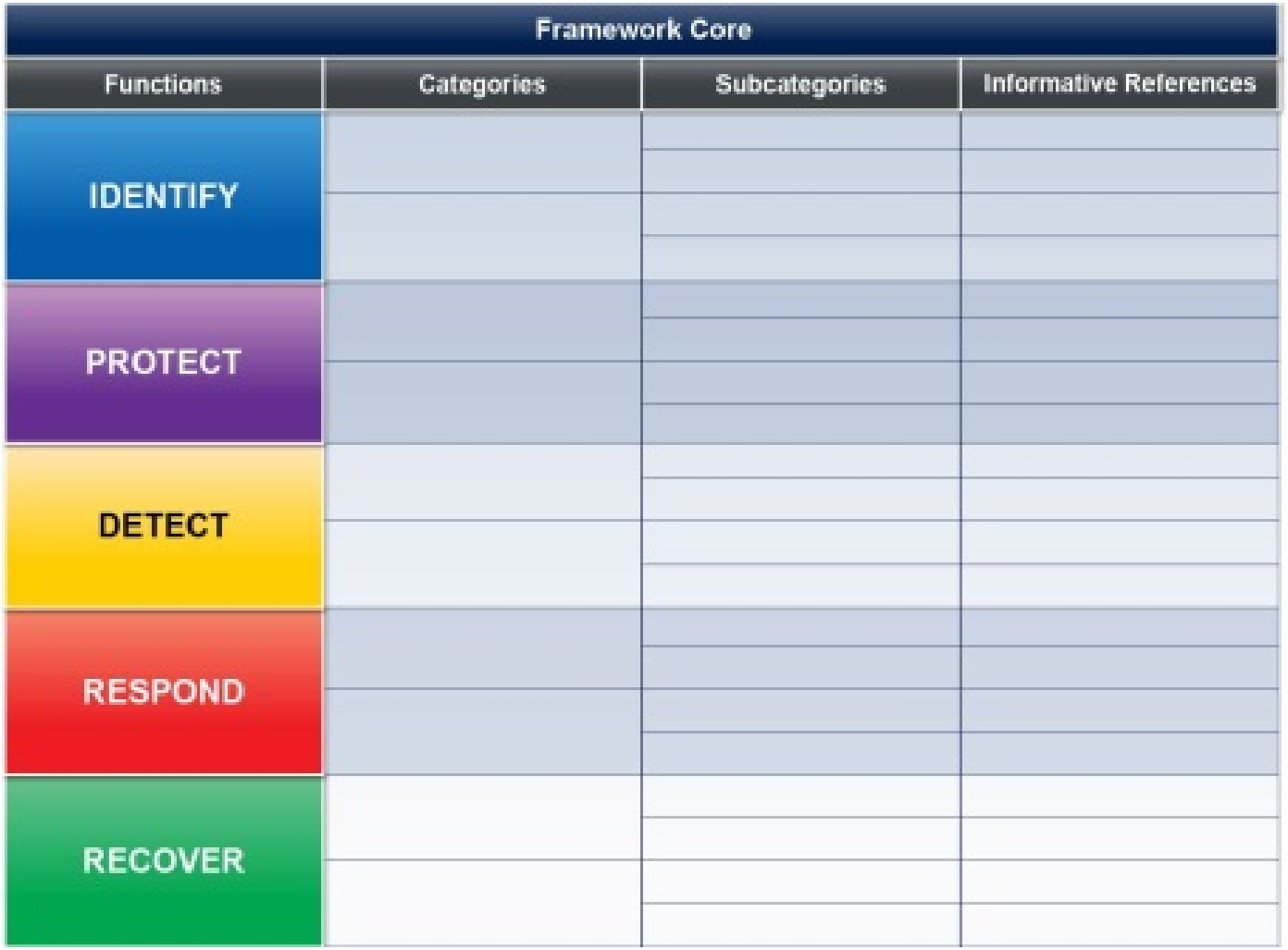
Categories, Subcategories, and Informative References

- **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.

Framework Core



The Framework Core

Function and Unique Identifier	Category and Unique Identifier	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (AM):** Identify and manage the personnel, devices, systems, and facilities that enable the organization to achieve business purposes, including their relative importance to business objectives, in support of effective risk decisions.	**ID.AM-1:** Inventory and track physical devices and systems within the organization	• **ISA 99.02.01** 4.2.3.4 • **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05 • **ISO/IEC 27001** A.7.1.1, A.7.1.2 • **NIST SP 800-53** Rev. 4 CM-8, PM-5, PM-6 • **CCS CSC** 1
		ID.AM-2: Inventory software platforms and applications within the organization	…
		…	…
		…	…
	…	…	…
PROTECT (PR)	**Awareness and Training (AT):** Ensure that organizational personnel and partners are adequately trained to carry out their assigned information security-related duties and responsibilities through awareness and training activities.	**PR.AT-1:** Provide awareness and training that ensures that general users understand roles & responsibilities and act accordingly	• **ISA 99.02.01** 4.3.2.4.2 • **COBIT** APO 07.03, BAI05.07 • **ISO/IEC 27001** A.8.2.2 • **NIST SP 800-53** Rev. 4 AT-2 • **CCS CSC** 9
		…	…
	…	…	…
DETECT (DE)	**Detection Processes (DP):** Ensure timely and adequate awareness of anomalous events through tested and implemented detection processes and procedures.	**DE.DP-1:** Ensure accountability by establishing organizational roles, responsibilities for event detection and response	• **ISA 99.02.01** 4.4.3.1 • **COBIT** DSS05.01 • **ISO/IEC 27001** A.10.4.1 • **CCS CSC** 5
		…	…
	…	…	…
RESPOND (RS)	**Mitigation (MI):** Conduct activities to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Contain the incident	• **ISO/IEC 27001** A.03.06, A.13.02.03 • **ISA 99.02.01** 4.3.4.5.6
		…	…
	…	…	…
RECOVER (RC)	**Recovery Planning (RP):** Execute Recovery Plan activities to achieve restoration of services or functions	**RC.RP-1:** Execute recover plan	• **COBIT** DSS02.05, DSS03.04 • **ISO/IEC 27001** A.14.1.3, A.14.1.4, A.14.1.5

Discussion Draft – Preliminary Cybersecurity Framework

- In August, NIST presented the following for community feedback:
  - Discussion Draft of the Preliminary Cybersecurity Framework
    - Introduction, Framework Basics, How to Use the Framework, Areas for Improvement, Framework Core
  - Executive Overview
    - Message to Senior Executives on the Cybersecurity Framework
  - Illustrative Examples
    - Threat Mitigation Examples (e.g., cybersecurity intrusion, malware, insider threat) – illustrate how organizations may apply the Framework to mitigate specific threats.
    - ICS Profile for the Electricity Subsector – illustrate how organizations within the electricity subsector may apply the Framework by leveraging existing sector-specific resources (e.g., ISA/IEC 62443, NIST SPs 800-82 and 800-53, DOE ES C2M2, NERC CIPs)

Questions for Reviewers to Consider

How can the Preliminary Framework:

- adequately define and address outcomes that strengthen cybersecurity and support business objectives?
- enable cost-effective implementation?
- appropriately integrate cybersecurity risk into business risk?
- provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?
- enable senior executive awareness of potential consequences of successful cyber attacks?
- provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?

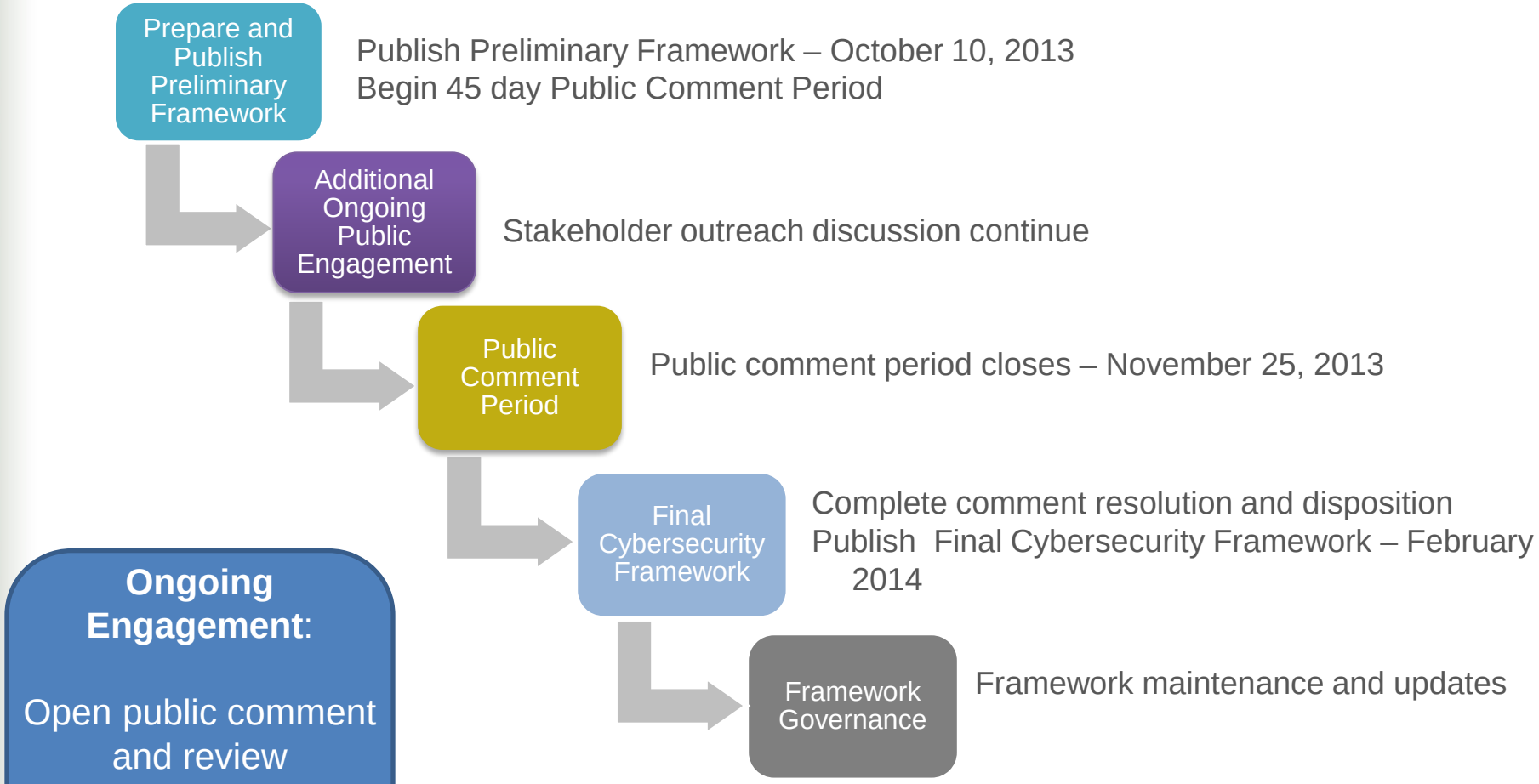
Will the Discussion Draft, as presented:

- be inclusive of, and not disruptive to, effective cybersecurity practices in use today?
- enable organizations to incorporate threat information?

Is the Discussion Draft:

- presented at the right level of specificity?
- sufficiently addressing unique privacy and civil liberties needs for critical infrastructure?

Getting from the Preliminary Framework to the Final Framework and Beyond



Next Steps

- NIST is planning additional workshops
- Focus on implementing the Framework
  - What do sector-wide implementations look like?
  - What do organizational implementations look like?
- Publish Preliminary Framework for Formal Public Comment (October 10th, 2013)

The Discussion Draft of the Preliminary Cybersecurity Framework, Executive Overview, Illustrative Examples, and other material is available at http://www.nist.gov/itl/cyberframework.cfm

Please send us your continued observations and further suggestions at cyberframework@nist.gov