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

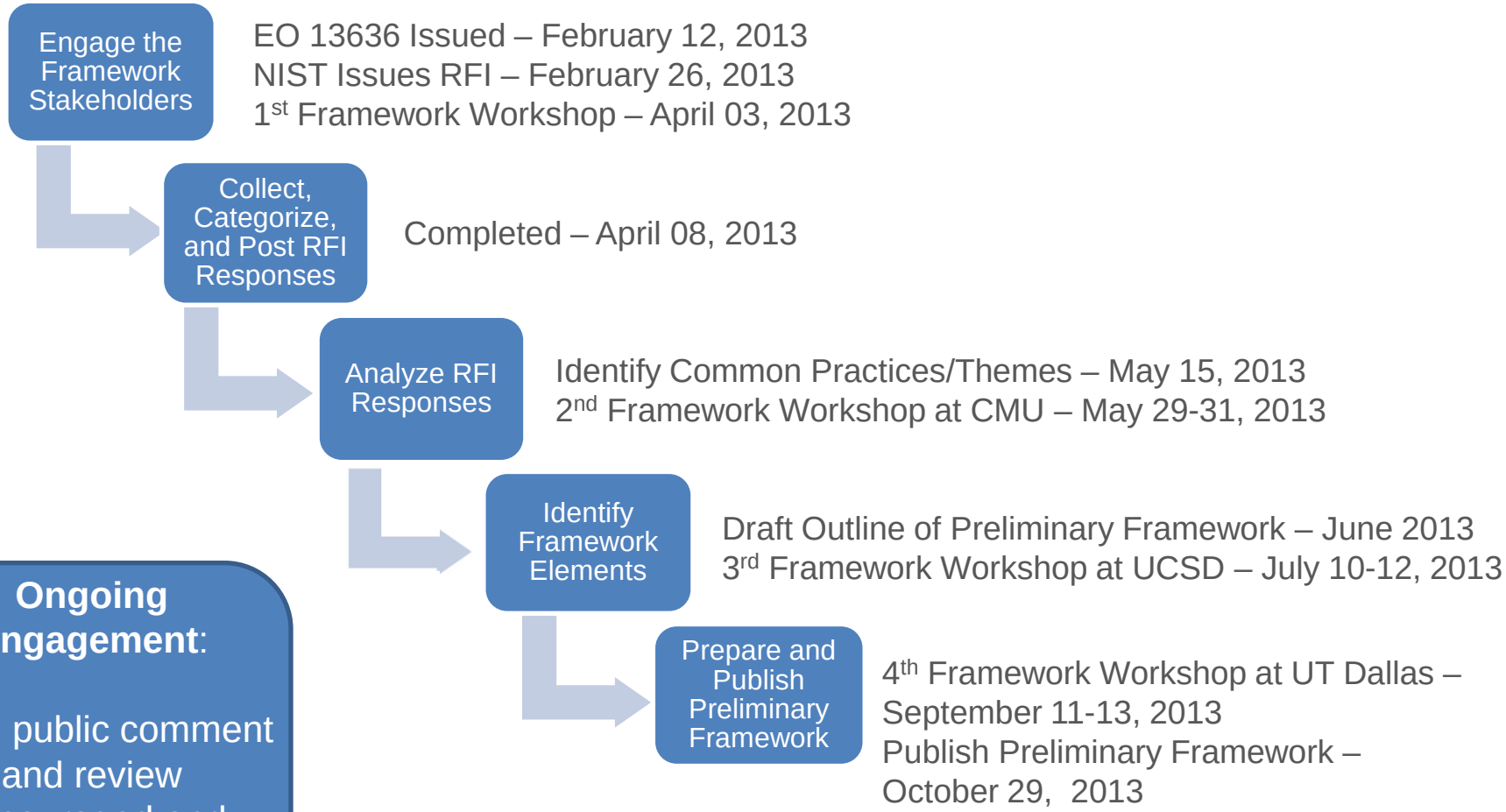
- This Cybersecurity Framework is being developed in an open manner with input from stakeholders in industry, academia, and government, including a public review and comment process, workshops, and other means of engagement.

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



Framework Components

Framework Core

- Cybersecurity activities and references that are common across critical infrastructure sectors organized around particular outcomes.
- Enables communication of cybersecurity risk across the organization.

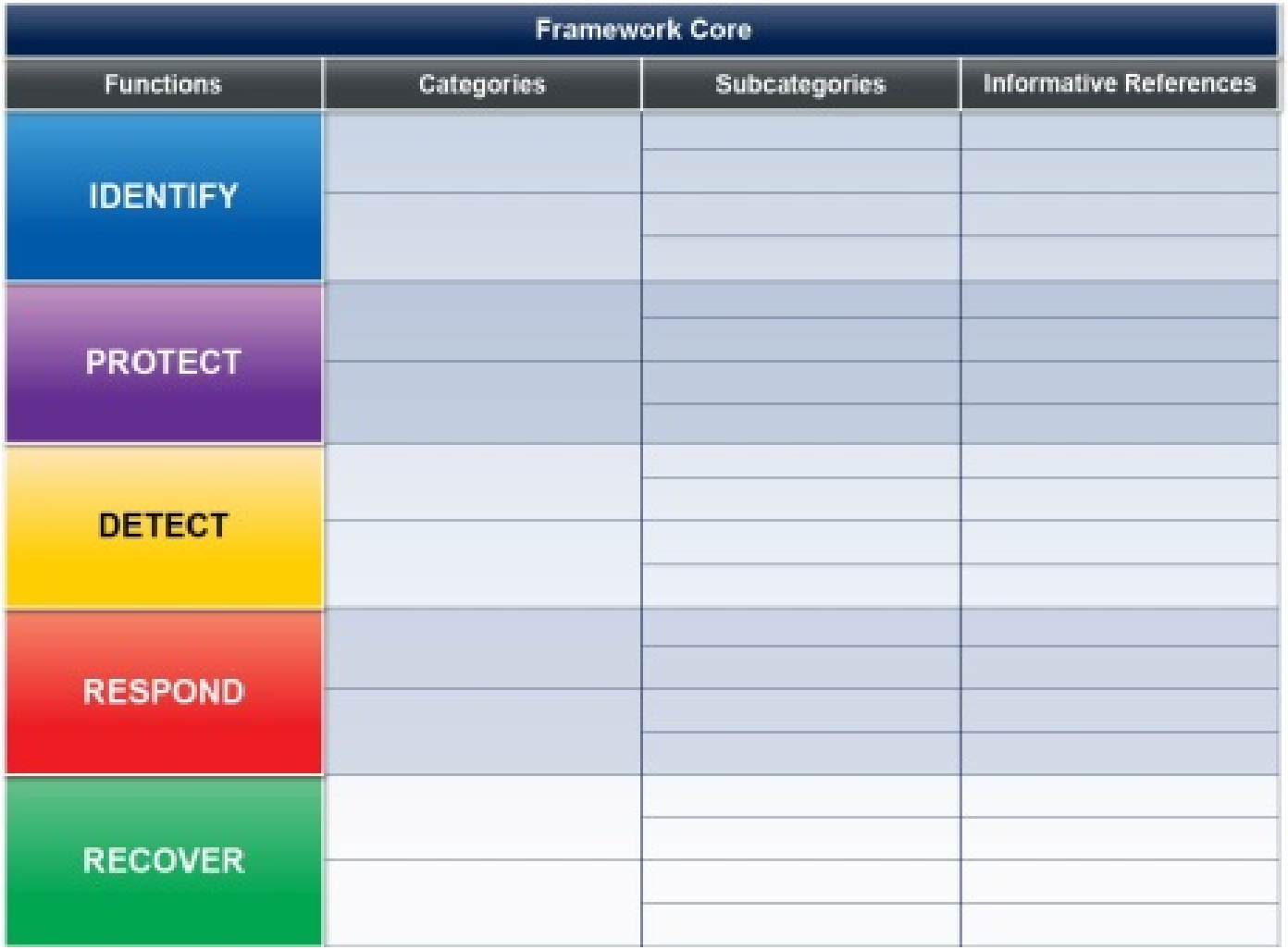
Framework Profile

- Alignment of industry standards and best practices to the Framework Core in a particular implementation scenario.
- Supports prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation.

Framework Implementation Tiers

- Describe how cybersecurity risk is managed by an organization.
- Describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics (e.g., risk and threat aware, repeatable, and adaptive).
- Partial (Tier 1), Risk-Informed (Tier 2), Risk-Informed and Repeatable (Tier 3), Adaptive (Tier 4).

Framework Core



Framework 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.

Framework Categories

- Categories are the subdivisions of a Function into groups of cybersecurity activities, more closely tied to programmatic needs

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Framework Subcategories and Informative References

- **Subcategories** further subdivide a Category into high-level tactical activities to support technical implementation.
- **Informative References** are specific sections of standards and practices common among critical infrastructure sectors and illustrate a method to accomplish the activities within each Subcategory.
- The Informative References presented in the Framework Core are not exhaustive, and organizations are free to implement other standards, guidelines, and practices.

Framework Core - Sample

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (AM):** The personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **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 • **CCS CSC**1
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **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 • **CCS CSC** 2
		ID.AM-3: The organizational communication and data flow is mapped	• **ISA 99.02.01** 4.2.3.4 • **COBIT** DSS05.02 • **ISO/IEC 27001** A.7.1.1 • **NIST SP 800-53 Rev. 4** CA-3, CM-8, CA-9 • **CCS CSC** 1

Areas for Improvement

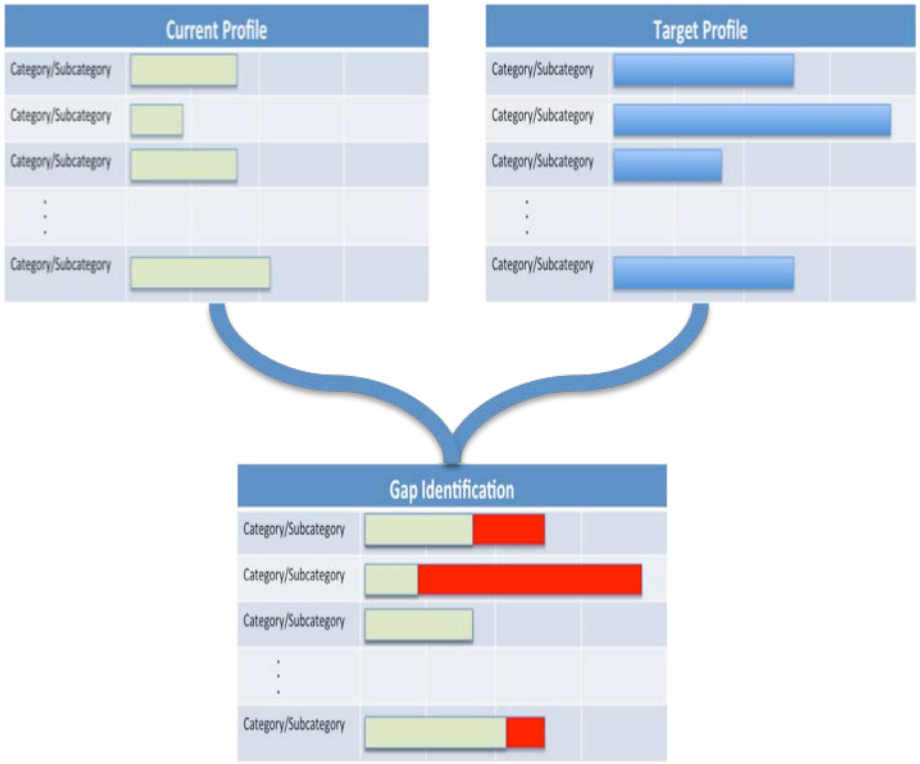
- The Cybersecurity Framework will "identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations."

- Initial Areas for Improvement provide a roadmap for stakeholder collaboration and cooperation to further understand and/or develop new or revised standards.

  - Authentication
  - Automated Indicator Sharing
  - Conformity Assessment
  - Cybersecurity Workforce
  - Data Analytics
  - International Aspects, Impacts, and Alignment
  - Privacy Standards
  - Supply Chains Risk Management

Framework Profiles

- Enables organizations to establish a roadmap to reducing cybersecurity risk
- Can be used to describe current state and desired target state of specific cybersecurity activities
- Created by determining which Categories are relevant to a particular organization, sector, or other entity
- An organization's risk management processes, legal / regulatory requirements, business / mission objectives, and organizational constraints guide the selection of activities during Profile development



Framework Implementation Tiers

- Feedback indicated the need for the Framework to allow for flexibility in implementation

- Responding to feedback, Framework Implementation Tiers were proposed to reflect how an organization implements the Framework Core functions and manages its risk.

- The characteristics expressed in the Tiers are progressive, ranging from Partial (Tier 1) to Adaptive (Tier 4), with each Tier building on the previous Tier.

Current Definitions of Tiers (Excerpts)

Tier 1: Partial

- **Risk Management Process:** Organizational cybersecurity risk management practices are not formalized and risk is managed in an ad hoc and sometimes reactive manner.
- **Integrated Program** – There is a limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established.

Tier 2: Risk-Informed

- **Risk Management Process** – Risk management practices are approved by management but may not be established as organizational-wide policy.
- **External Participation** – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally

Tier 3: Risk-Informed and Repeatable

- **Integrated Program:** There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and validated.
- **External Participation:** The organization understands its dependencies and partners and receives information from these partners enabling management decisions.

Tier 4: Adaptive

- **Risk Management Process:** The organization adapts its cybersecurity practices based on lessons learned and predictive.
- **External Participation:** The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed before an event occurs.

How to Use the Framework

The Framework can be leveraged by organizations looking to:

- **Establish or Improve a Cybersecurity Program**
  - Step 1: Identify
  - Step 2: Create a Current Profile
  - Step 3: Conduct Risk Assessment
  - Step 4: Create a Target Profile
  - Step 5: Determine, Analyze, and Prioritize Gaps
  - Step 6: Implement Action Plan
- **Communicate Cybersecurity Requirements with Stakeholders**
- **Identify Gaps**

Methodology to Protect Privacy and Civil Liberties

- The EO directs NIST to include a methodology to identify and mitigate impacts of the Framework and associated security measures to protect individual privacy and civil liberties.

- Appendix B presents a Privacy methodology that is coordinated with the Framework Core. This methodology provides organizations with flexibility in determining how to manage privacy risk.

- This methodology is based on the Fair Information Practice Principles (FIPPs) referenced in the EO, and is designed to complement existing processes organizations may have in place.

Questions for Reviewers to Consider

How can the Preliminary Framework:

- adequately define 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?
- provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?
- provide the right level of specificity and guidance for mitigating the impact of cybersecurity measures on privacy and civil liberties?
- express existing practices in a manner that allows for effective use?

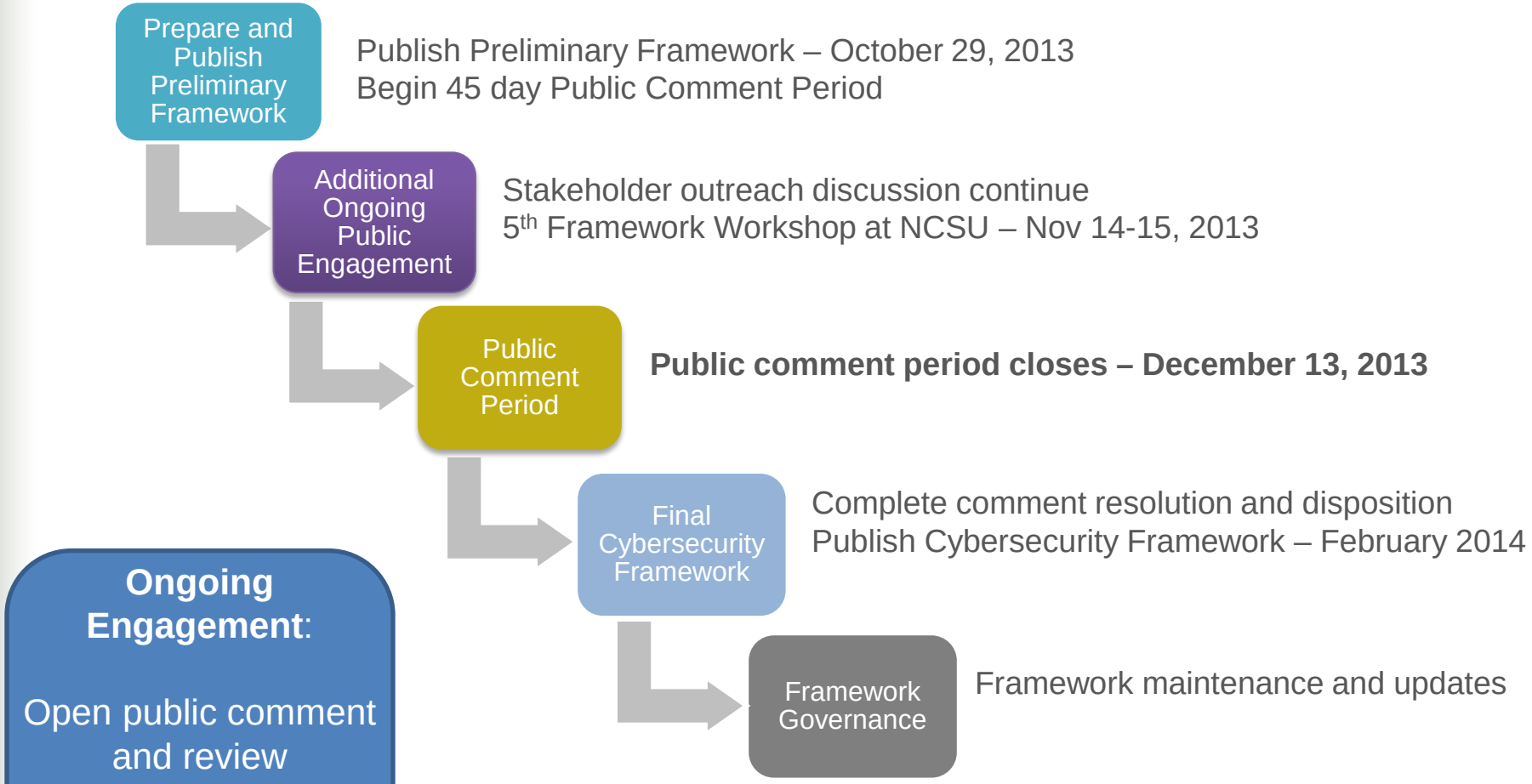
Will the Discussion Draft, as presented:

- be inclusive of, and not disruptive to, effective cybersecurity practices in use today, including widely-used voluntary consensus standards that are not yet final?
- enable organizations to incorporate threat information?

Is the Discussion Draft:

- presented at the right level of specificity?
- sufficiently clear on how the privacy and civil liberties methodology is integrated with the Framework Core?

Getting from the Preliminary Framework to the Final Framework and Beyond



Thank You

The Preliminary Cybersecurity Framework is available at http://www.nist.gov/cyberframework/

Public Comments should be submitted to csfcomments@nist.gov no later than 5:00pm on December 13, 2013.