NIST Cybersecurity Framework Overview

Executive Order 13636

“Improving Critical Infrastructure Cybersecurity”

2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises

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"

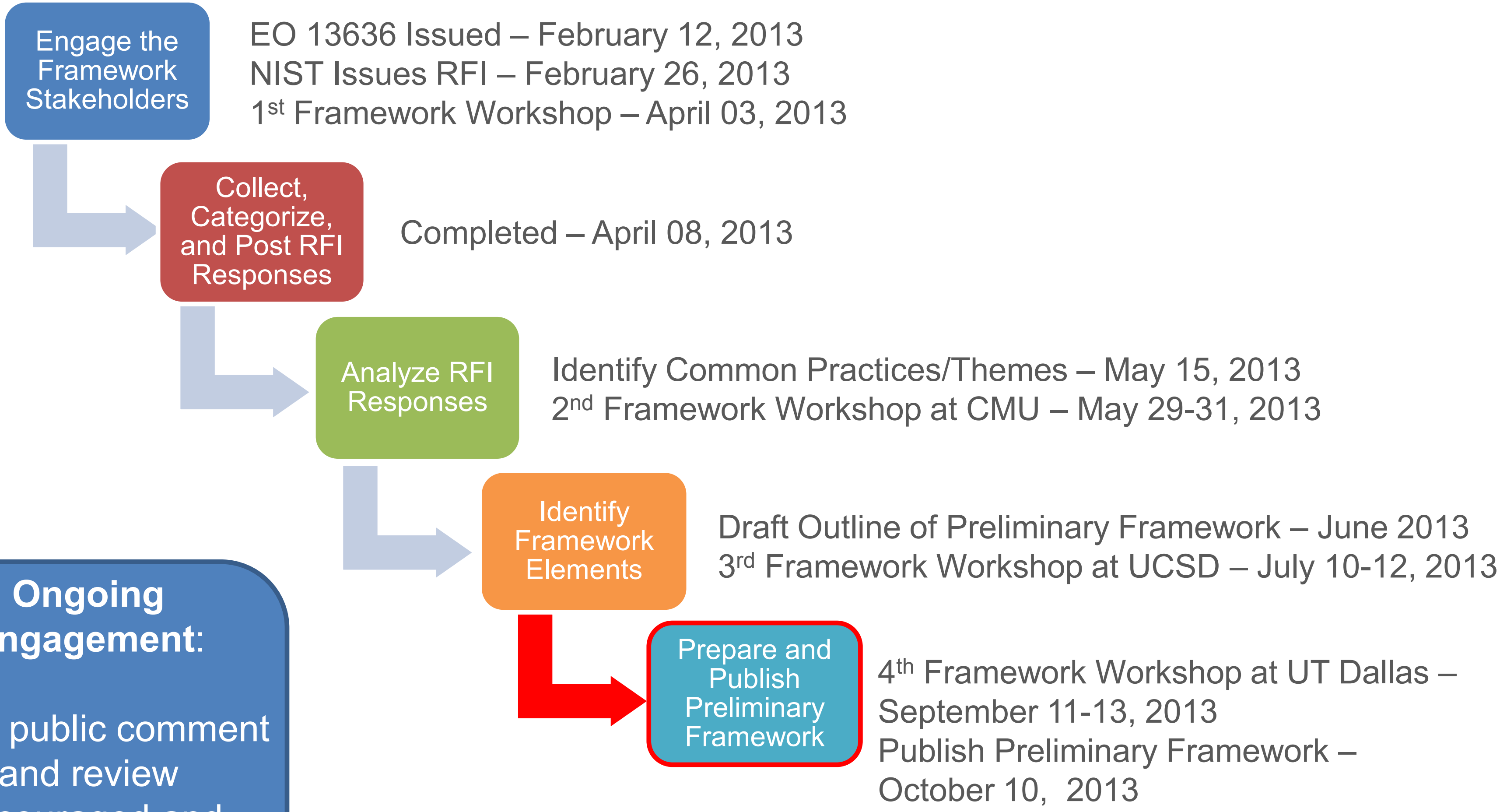
- NIST is directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- This Cybersecurity Framework is being developed in an open manner with input from stakeholders in industry, academia, and government, including a public review and comment 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



Engage the Framework Stakeholders

EO 13636 Issued – February 12, 2013
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

Identify Framework Elements

Draft Outline of Preliminary Framework – June 2013
3rd Framework Workshop at UCSD – July 10-12, 2013

Prepare and Publish Preliminary Framework

4th Framework Workshop at UT Dallas – September 11-13, 2013
Publish Preliminary Framework – October 10, 2013

Ongoing Engagement:

Open public comment and review encouraged and promoted throughout the process

Risk Management and the Cybersecurity Framework

- While not a risk management process itself, the Framework enables the integration of cybersecurity risk management into the organization’s overall risk management process.

- The Framework fosters:
  - Cybersecurity risk management approaches that take into account the interaction of multiple risks;
  - Cybersecurity risk management approaches that address both traditional information technology and operational technology (industrial control systems);
  - Cybersecurity risk management practices that encompass the entire organization, exposing dependencies that often exist within large, mature, and/or diverse entities, and with the interaction between the entities and their partners, vendors, suppliers, and others;
  - Cybersecurity risk management practices that are internalized by the organization to ensure that decision making is conducted by a risk-informed process of continuous improvement; and
  - Cybersecurity standards that can be used to support risk management activities

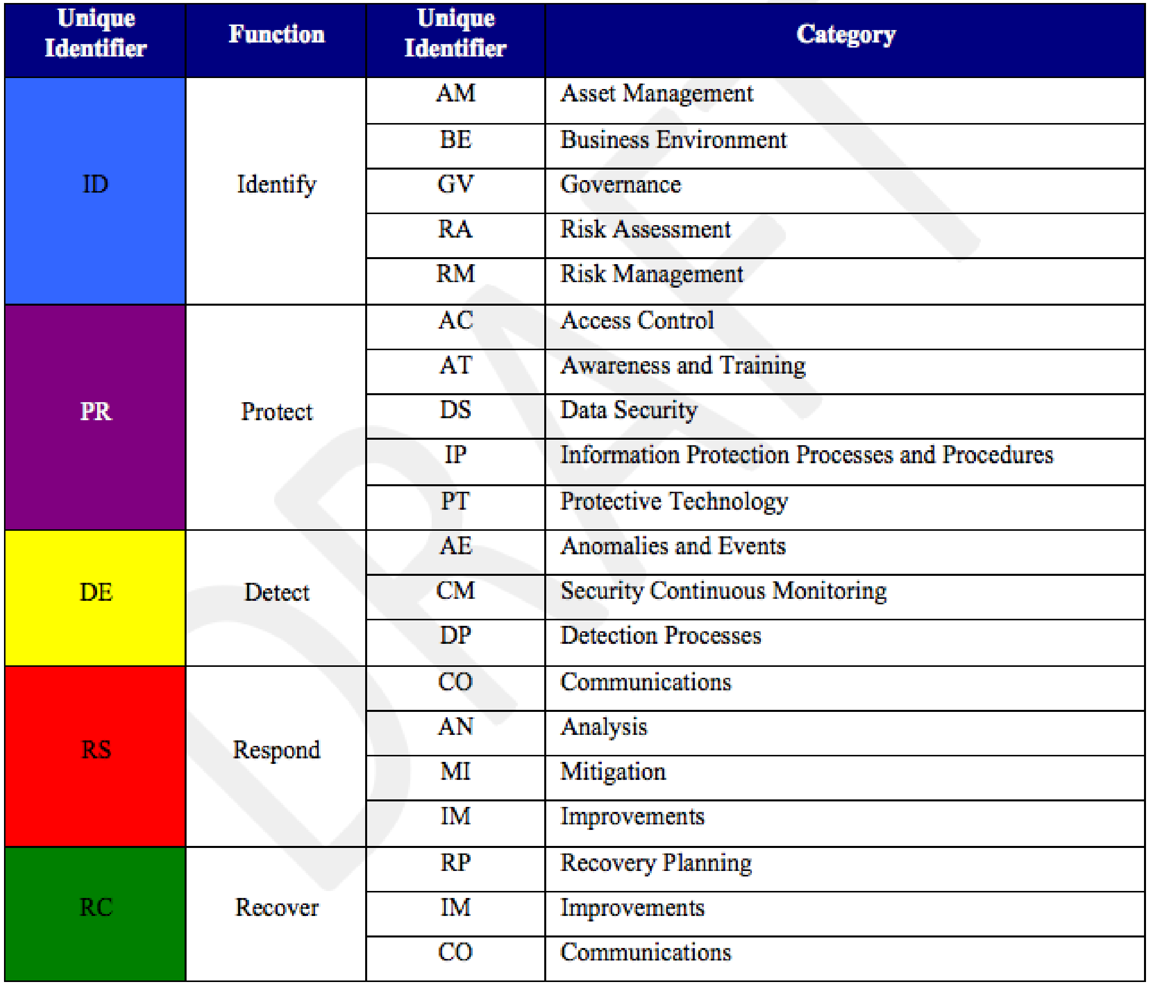
Framework Core: Functions

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.

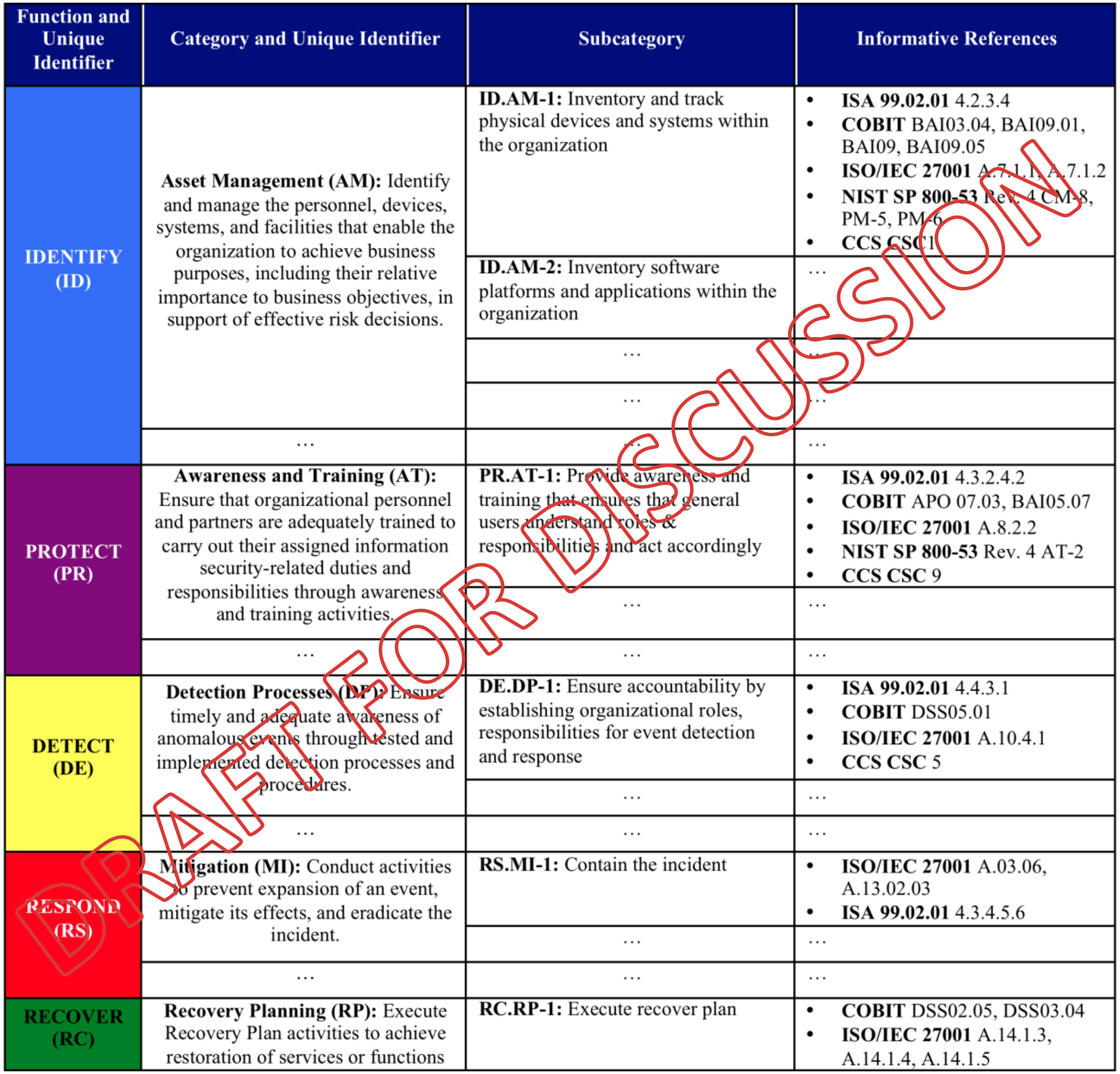
Framework Core: Categories

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



Unique Identifier	Function	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

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

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 0) to Adaptive (Tier 3), with each Tier building on the previous Tier.

- The Tier characteristics are defined at the organizational level and are applied to the Framework Core to determine how a category is implemented.

Discussion Drafts Posted August 28, 2013

Preliminary Cybersecurity Framework

- Framework Introduction
- Framework Basics
- How to Use the Framework
- Areas for Improvement for the Cybersecurity Framework
- Appendix A: Framework Core
- Appendix B: Methodology to Protect Privacy and Civil Liberties
- Appendix C: Framework Development Methodology
- Appendix D: Glossary
- Appendix E: Acronyms

Executive Overview

- Message to Senior Executives on the Cybersecurity Framework

Illustrative Examples

- Threat Mitigation Examples: Cybersecurity Intrusion, Malware, Mitigating Insider Threats
- ICS Profile for the Electricity Subsector

How to Use the Framework

The Framework can be leveraged by organizations looking to:

- **Establish or Improve a Cybersecurity Program**

  Step 1: Make Organization Wide Decisions

  Step 2: Establish a Target Profile

  Step 3: Establish a Current Profile

  Step 4: Compare Target and Current Profiles

  Step 5: Implement Target Profile

- **Communicate Cybersecurity Requirements with Stakeholders**

- **Identify Gaps**

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?

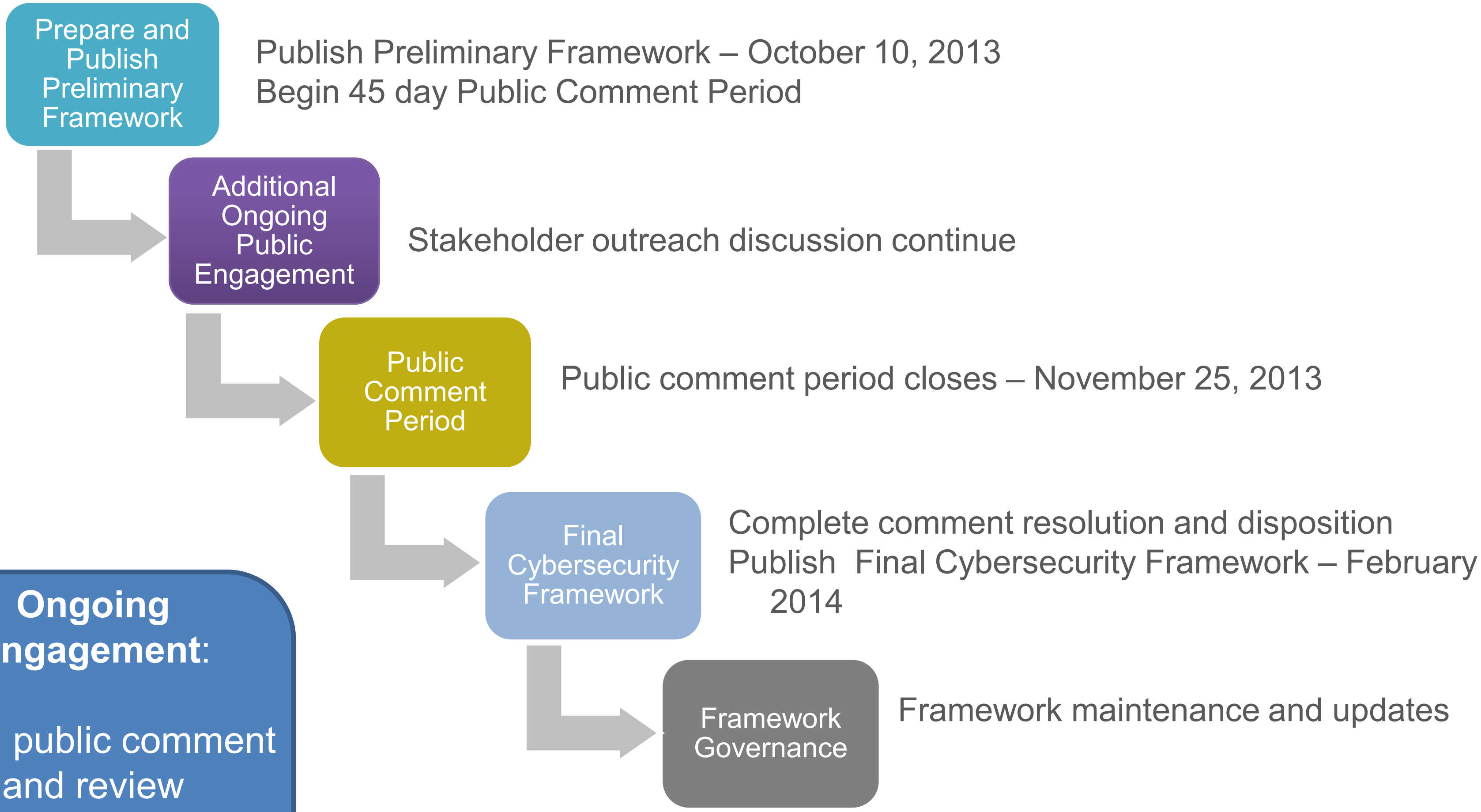
Will the Discussion Draft, as presented:

- 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



Prepare and Publish Preliminary Framework

Publish Preliminary Framework – October 10, 2013
Begin 45 day Public Comment Period

Additional Ongoing Public Engagement

Stakeholder outreach discussion continue

Public Comment Period

Public comment period closes – November 25, 2013

Final Cybersecurity Framework

Complete comment resolution and disposition
Publish Final Cybersecurity Framework – February 2014

Framework Governance

Framework maintenance and updates

Ongoing Engagement:

Open public comment and review encouraged and promoted throughout the process

Q & A

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 observations and suggestions to cyberframework@nist.gov