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.

Taking Action

President Obama announced two policies in February, 2013:

Executive Order 13636:
Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive 21:
Critical Infrastructure Security and Resilience

- Together, they create an opportunity to effect a comprehensive national approach
- Implementation efforts will drive action toward ***system*** **and** ***network*** security and resiliency

EO-PPD Deliverables

120 days – **June 12, 2013**

- Publish instructions: unclassified threat information
- Report on cybersecurity incentives
- Publish procedures: expand the Enhanced Cybersecurity Services

150 Days - **July 12, 2013**

- Identify cybersecurity critical infrastructure
- Evaluate public-private partnership models
- Expedite security clearances for private sector

240 Days – **October 10, 2013**

- Develop a situational awareness capability
- Update the National Infrastructure Protection Plan
- Publish draft voluntary Cybersecurity Framework

365 days – **February 12, 2014**

- Report on privacy and civil rights and civil liberties cybersecurity enhancement risks
- Stand up voluntary program based on finalized Cybersecurity Framework

Beyond 365 - **TBD**

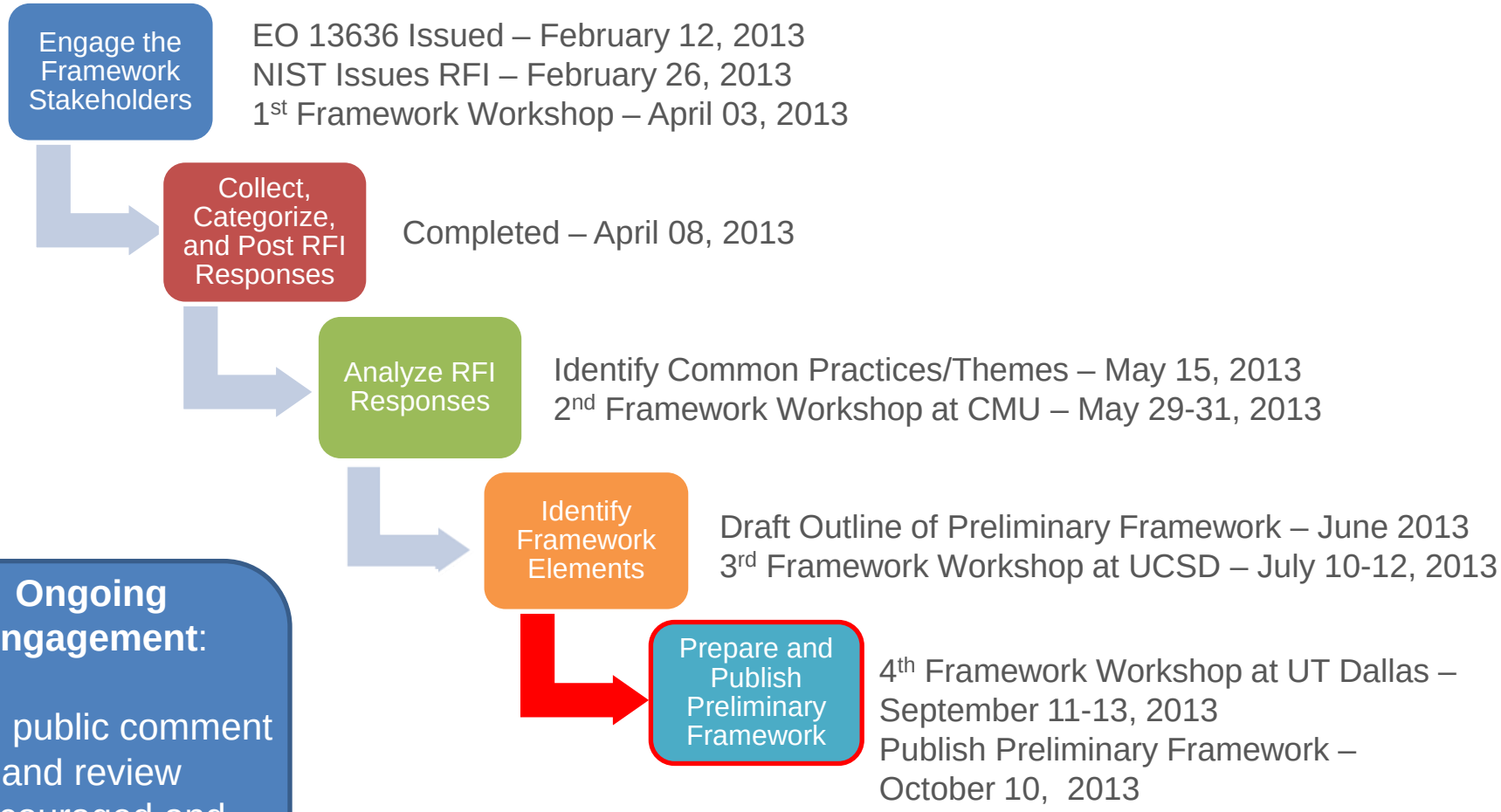
- Critical Infrastructure Security and Resilience R&D Plan

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

Collect, Categorize, and Post RFI Responses

- 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.

Cybersecurity Framework Categories and Themes

Analyze RFI Responses

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

What We Heard at Workshop #2

Analyze RFI Responses

- The Framework needs to have the following elements:
  - Identify effective existing practices to inform an organization's risk management decisions
  - Provide a modular and flexible approach to account for unique sector and organization business drivers, and be scalable and useful to diverse organizations
  - Reinforce the importance of senior leadership engagement in cybersecurity risk management process
  - Provide a means to express the maturity of an organization's cybersecurity risk management practices
  - Address the need for organizations to manage various types of dependencies, including those related to providers, processes, and technologies

Framework Core

Prepare and Publish Preliminary Framework

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Draft Outline - Preliminary Framework

Identify Framework Elements

- In June, NIST presented the following for community feedback:
  - Draft outline that defines the overall Framework structure
    - Executive Overview and Summary
    - How to Use the Framework
    - Role of Risk Management Processes
  - Framework Core Elements
    - A high-level view of key functions, categories, and subcategories of an organization's approach to managing cybersecurity risk
    - Framework Implementation Levels
  - Compendium of Informative References
    - Non-exhaustive listing of submitted informative references (e.g., standards, guidelines, and best practices) to assist with specific implementation
    - Illustrative resource; not intended as an endorsement of any reference

What We Heard at Workshop #3

Prepare and Publish Preliminary Framework

- Several points of consensus were identified and reinforced
  - The Framework needs to be scalable, actionable, threat-informed, and risk-based
  - The Framework needs to be informative, not prescriptive; it must have sufficient detail to be actionable and flexible in implementation
  - The Framework needs to acknowledge that cybersecurity risk management must incorporate people, process, and technology considerations
  - Participants supported the proposed functions (*Know, Prevent, Detect, Respond, Recover*), but suggested refinements (*Know → Identify, Prevent → Protect*)
  - The *Framework Implementation Levels* proposed in the draft outline can serve as an indicator of an organization's implementation of the Framework, and an indicator of how an organization is managing risk (*Levels → Tiers*)

What We Heard at Workshop #3 (continued)

Prepare and Publish Preliminary Framework

- Key points were identified in topic-specific sessions
  - Small business applicability – the Framework should not introduce costly burdens on small businesses; rather, it should provide guidance for implementing security commensurate with risk.
  - Executive engagement – CEO outreach is critical to promote a broader understanding of cybersecurity risk to critical infrastructure.
  - International engagement – Encourage and actively seek input from international participants.
  - Awareness and training – Awareness and training, tailored to the organization, is essential to effective implementation of the Framework.
  - Privacy – Acknowledgement that privacy is critical, but that the identification of common privacy standards and practices continues to be an area for improvement.

Framework Core: Functions

Prepare and Publish Preliminary Framework

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: Subcategories and Informative References

Prepare and Publish Preliminary Framework

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.

The Framework Core

Prepare and Publish Preliminary Framework

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

Prepare and Publish Preliminary Framework

- 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 Draft – Preliminary Cybersecurity Framework

Prepare and Publish Preliminary 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

Prepare and Publish Preliminary Framework

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?

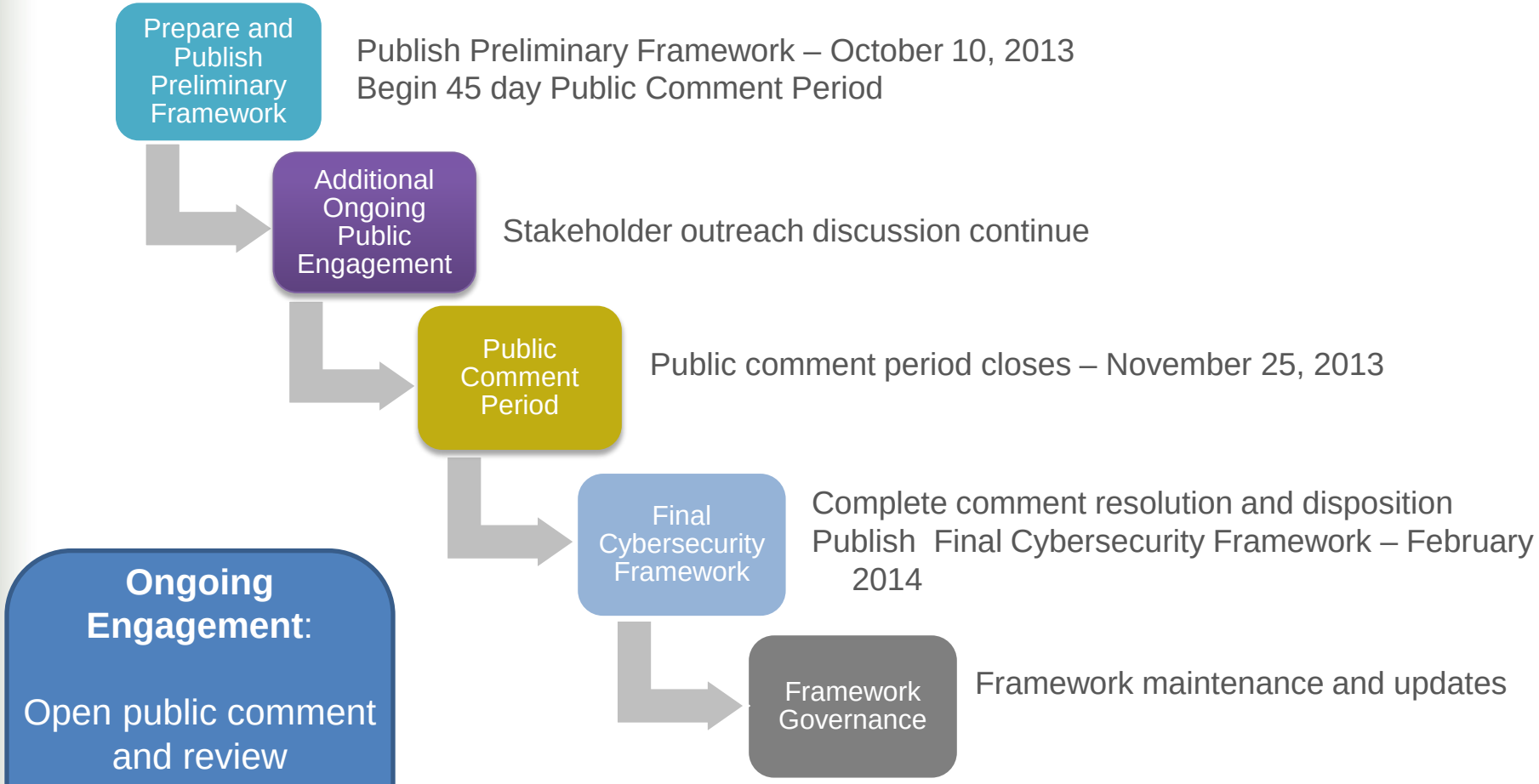
Will the Discussion Draft, as presented:

- 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



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