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

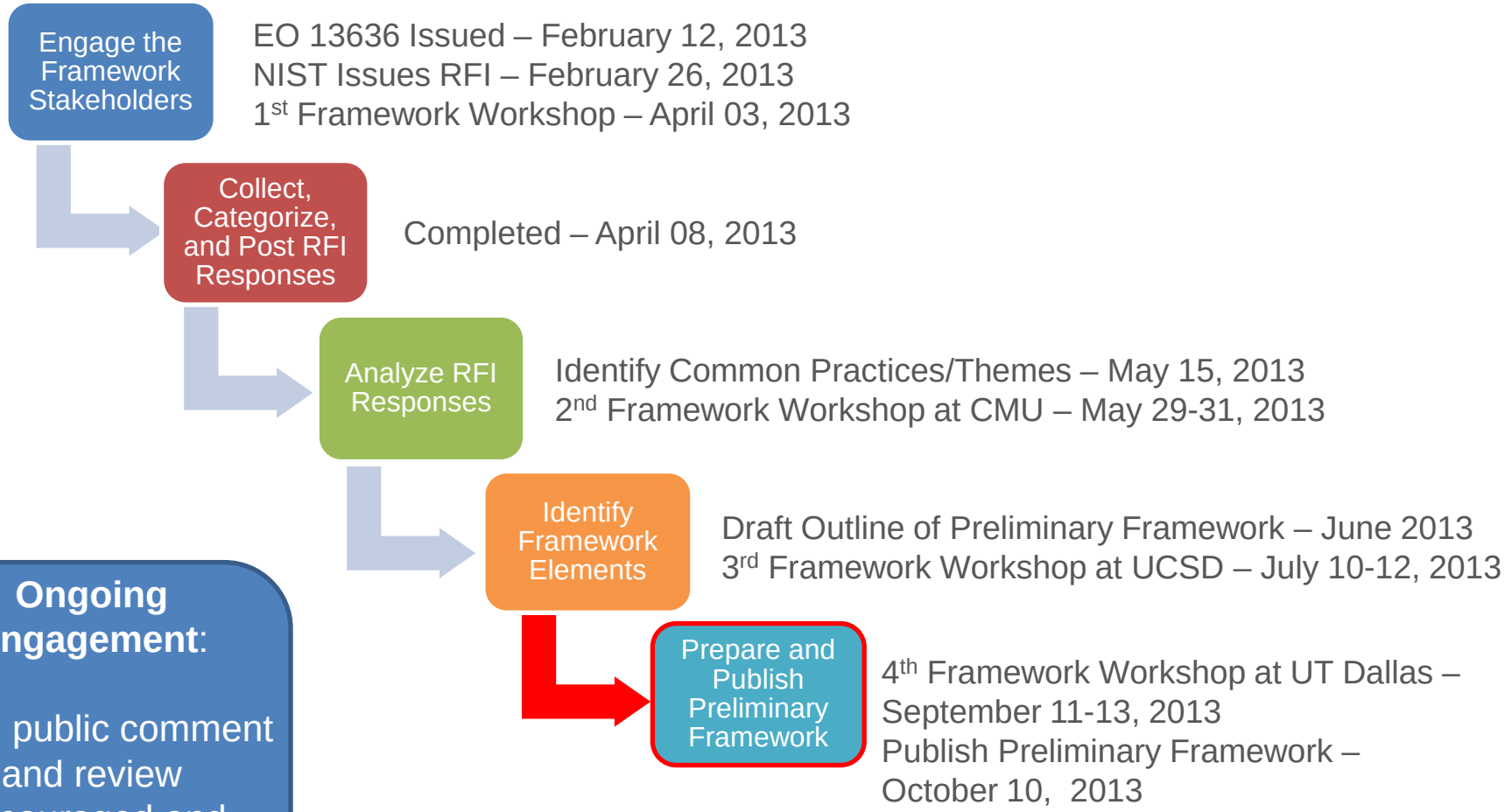
- This Cybersecurity Framework is being developed in an open manner with input from stakeholders in industry, academia, and government, including a public review and comment process, workshops, and other means of engagement.

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



Stakeholder Engagement Shaped the Framework Content

- The Framework language and communication is critical to success
- The Framework must reflect characteristics of people, processes, and technologies
- The Framework must be inclusive of and not disruptive to those good practices in use today
- The Framework must include the fundamentals
- Determination of risk tolerance for critical infrastructure must be informed by national interests
- Threat information must inform Framework implementation

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

Message to Senior Executives on the Cybersecurity Framework

- Cybersecurity risk is a reality that organizations must understand and manage like other business risks that can have critical impacts.

- Organizations must manage cybersecurity risk in order to gain and maintain customers, reduce cost, increase revenue, and innovate.

- The Framework is intended to help each organization manage cybersecurity risks while maintaining flexibility and the ability to meet business needs.

- Implementing the Framework will help organizations align and communicate their cybersecurity risk posture with their partners and help communicate expectations for managing cybersecurity risk consistent with their business needs.

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

Framework Core: 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.

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.

Framework Implementation Tiers

Tier 0: Partial – The organization:

- Has not yet implemented a formal, threat-aware risk management process to determine a prioritized list of cybersecurity activities.
- May implement some portions of the Framework on an irregular, case-by-case basis due to varied experience or information gained from outside sources.
- May not have the processes in place to share cybersecurity information internally between its organizational layers and may not have the processes in place to participate in coordination or collaboration with other entities.

Tier 1: Risk Informed – The organization:

- Uses a formal, threat-aware risk management process to develop a Profile of the Framework.
- Uses risk-informed, management-approved processes and procedures that are defined and implemented
- Has staff with adequate resources to perform their cybersecurity duties.
- Knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

Tier 2: Repeatable – The organization:

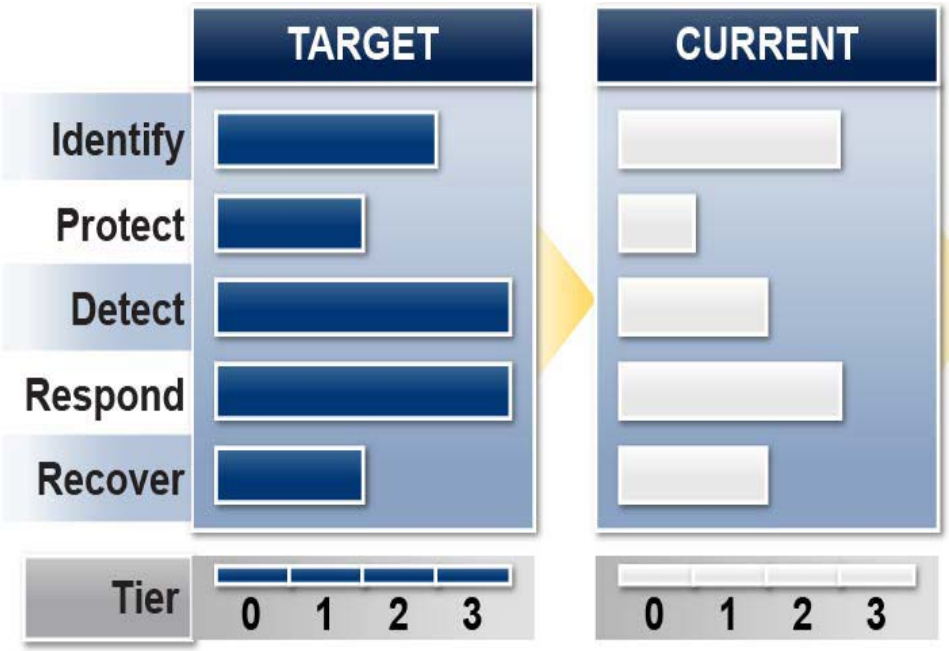
- Updates its Profile based on regular application of its risk management process to respond to a changing cybersecurity landscape.
- Has defined risk-informed policies, processes, and procedures that are implemented as intended, and validated.
- Will also have consistent methods in place to provide updates when a risk change occurs.
- Has personnel have adequate knowledge and skills to perform their defined roles and responsibilities.
- Understands its dependencies and partners and can consume information from these partners to help prevent and improve its reaction to events.

Tier 3: Adaptive – The organization:

- Updates its Profile based on predictive indicators derived from previous and anticipated cybersecurity activities.
- Has risk-informed policies, processes, and procedures are part of the organizational culture and evolve from previous activities (and from information shared by other sources) to predict and address potential cybersecurity events.
- Manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve Cybersecurity before an event occurs.

Framework Profile

- 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



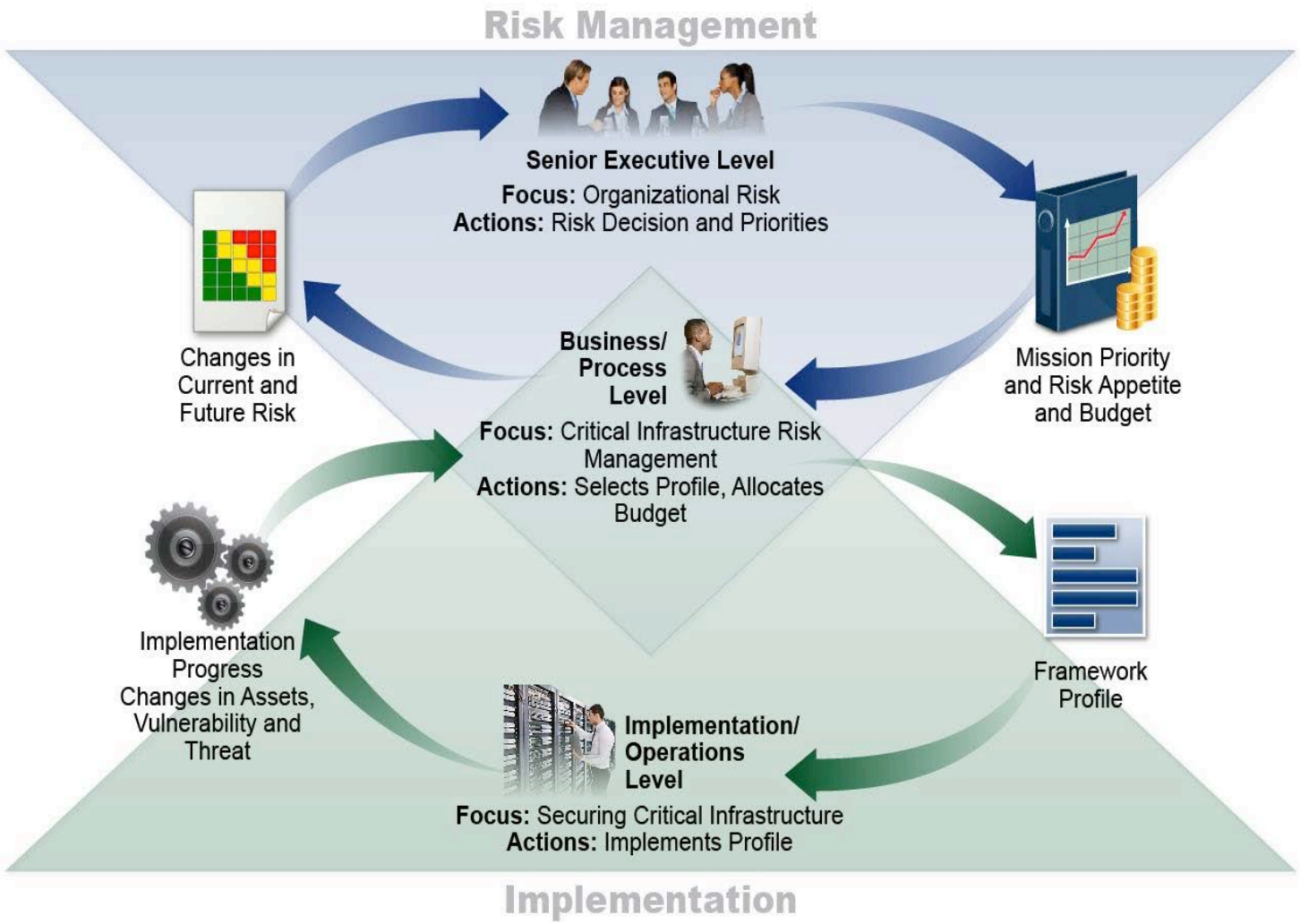
Framework Profile Implementation

- The method by which the Functions, Categories, and Subcategories described in the Core are aligned with business requirements, risk tolerance, and resources for the organization.

- The Framework provides a mechanism for organizations, sectors, and other entities to create their own Target Profiles.

- It does not provide Target Profile templates, nor identify Tier requirements that an organization should meet.

Notional Information and Decision Flows within an Organization



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**

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.

Areas for Improvement for the Cybersecurity Framework

Executive Order 13636 states that the Cybersecurity Framework will “identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations”.

Based on stakeholder input, several high-priority Areas for Improvement have been identified. Collaboration and cooperation must increase for these areas to further understanding and/or the development of new or revised standards.

- Authentication
- Automated Indicator Sharing
- Conformity Assessment
- Data Analytics
- International Aspects, Impacts, and Alignment
- Privacy
- Supply Chains and Interdependencies

Draft Illustrative Framework Profile Examples

Threat Mitigation Profile Examples

- While organizations and sectors may develop overall Profiles, these Threat Mitigation Profile examples illustrate how organizations may apply the Framework to mitigate specific threats.
- Discussion of 3 scenarios: Cybersecurity intrusion, malware, and insider threat scenarios

Industrial Control Systems Profile for the Electricity Subsector

- Includes an introduction that describes the application of the framework under a specific scenario.
- The scenarios will include adapting the framework to address the nuances of the particular risks that are relevant to a particular organization's business operations or mission.
- Includes ISO/ISA 27001, CCS CSC, NISTIR 7628, NIST SP 800-53, NERC CIP, and DOE ES-C2M2 as Informative References.

Draft Illustrative Framework Profile Example: Threat Mitigation

Function	Category	Subcategories	Informative Reference	Comment
Identify	Risk Assessment	Identify threats to organizational assets (both internal and external) Identify providers of threat information	**NIST SP 800-53** Rev. 4 PM-16 **ISO/IEC 27001** A.13.1.2	Allows the organization to identify current known IP addresses for adversary servers and block inbound and outbound connections to this source.
Protect	Information Protection Processes and Procedures	Develop, document, and maintain under configuration control a current baseline configuration of information technology / operations technology systems	**NIST SP 800-53** Rev. 4 CM-2	An effective patch management process provides another potential defense against malware. Many exploits use well-known software flaws for which patches are available. A mature patch management process makes it harder for an adversary to craft an initial exploit. It is important that critical infrastructure install updated patches; test patches for potential operational impacts; and ensure that the patches do not introduce new vulnerabilities.
Respond	Improvements	Incorporate lessons learned into plans Update response strategies	**ISO/IEC 27001** A.13.02.02 **NIST SP 800-53** Rev. 4 PM-9	Document the lessons learned from the intrusion and use them to enhance organizational cybersecurity processes.

Draft Illustrative Framework Profile Example: ICS Profile for the Electricity Subsector

- Includes an introduction that describes the application of the framework under a specific scenario – an electric utility.
- The electricity subsector has created several guidelines, standards, and programs based on cybersecurity practices and controls.
- This illustrative Framework example makes some *assumptions* regarding the electric utility, including that it:
  - Complies with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Version 3 standards and has identified Critical Cyber Assets (CCAs);
  - Is aware of other security standards and relies on the informative references used in the Framework Core;
  - Has performed a Department of Energy (DOE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) self-evaluation and is knowledgeable in the relevant domains and practices; and
  - Is familiar with risk management processes, such as those contained in both the NERC CIP standards and DOE Risk Management Process.

Draft Illustrative Framework Profile Example: ICS Profile for the Electricity Subsector

RECOVER	**Recovery Planning (RP):** Execute Recovery Plan activities to achieve restoration of services or functions commensurate with business decisions.	**RC.RP-1:** Execute recovery plan	• **NISTIR 7628** SG.CP • **NIST SP 800-53 rev 4** CP • **NIST SP 800-82** • **ISO/IEC 27001** • **NERC CIP-009-3** • **DOE ES-C2M2 RISK, THREAT, SITUATION, RESPONSE, CYBER**
		***RC.RP-2:** Hold exercises to practice/test implementation of recovery plan	
	Improvements (IM): Improve recovery planning and processes by incorporating lessons learned into future activities.	**RC.IM-1:** Incorporate lessons learned into plans	• **NISTIR 7628** SG.CP • **NIST SP 800-53 rev 4** CP • **ISO/IEC 27001** • **NERC CIP-009-3** • **DOE ES-C2M2 RISK, THREAT, SITUATION, RESPONSE, CYBER**
		RC.IM-2: Update recovery strategies	
	Communications (CO): Interact with outside parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Communicate with public affairs/media	• **NERC EOP-004-1** • **DOE Form OE-417** • **NERC CIP-001-2a, CIP-008-3** R1 • **CCS CSC #18** • **NIST SP 800-53 Rev 4** IR • **NIST SP 800-82 rev 1** 6.2.8 • **NIST SP 800-61 Rev 2** • **NIST IR 7628** SG.IR • **ISA-99.02.01-2009 A. 3.4.5** • **DOE ES-C2M2 RESPONSE**

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?

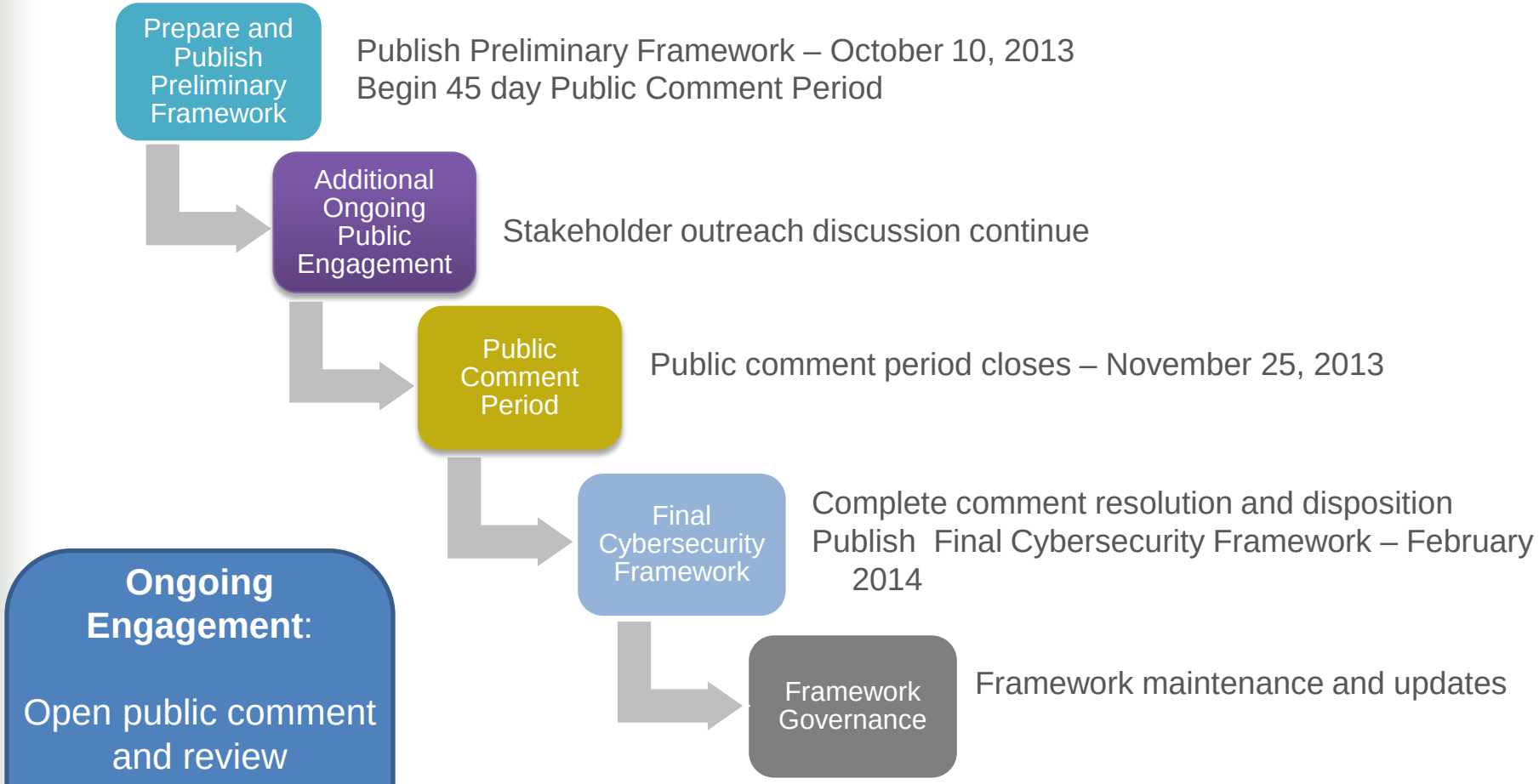
Will the Discussion Draft, as presented:

- 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



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