Proposed Updates to the Framework and Roadmap for Improving Critical Infrastructure Cybersecurity

December 2017

cyberframework@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Charter for Continued Development and Evolution

Framework and Roadmap for Improving Critical Infrastructure Cybersecurity

Amends the National Institute of Standards and Technology Act to say:

*"…**on an ongoing basis, facilitate and support the development** of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure"*

Cybersecurity Enhancement Act of 2014

18 December 2014

Input to the Proposed Framework Update

Framework and Roadmap for Improving Critical Infrastructure Cybersecurity

Draft Update #2 was based on feedback from the cybersecurity community including:

- Over 120 comments on January 2017 Draft Version 1.1 (V1.1)
- Discussions among 500+ participants at May 2017 Workshop

And previously….

- April 2016 Cybersecurity Framework workshop
- December 2015 request for information
- Ongoing lessons learned from Framework use
- Shared resources by NIST and industry partners
- Advances in areas identified in the Roadmap issued with the Framework in February 2014

Compatible with Version 1.0

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Clarifies, refines, and enhances the Framework

Industry feedback through workshops and RFIs made it clear:

- Changes should be minimal
- Framework must remain compatible with V1.0

Proposed Core Updates Are Fully Compatible

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

- Version 1.0 and 1.1 will work well together
- Additions, including new categories and subcategories, won't invalidate existing V1.0 work products

Component	Version 1.0	Version 1.1	Comments
Functions	5	5	
Categories	22	23	• Added a new category in ID.SC – Supply Chain
Subcategories	98	108	• Added 5 subcategories in ID.SC • Added 2 subcategories in PR.AC • Added 1 subcategory each to PR.DS, PR.PT, RS.AN • Clarified language in 7 others
Informative References	5	5	

Major Themes from Inputs: Draft #2

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Additional major themes addressed by Draft #2:

- Provides guidance for self-assessment, including use of Framework-based measurement
- Enhances guidance applying the Framework to manage cybersecurity within supply chains and for acquisition decisions
- Better accounts for Authorization, Authentication, and Identity Proofing
- Accounts for emerging vulnerability information (a.k.a., Coordinated Vulnerability Disclosure)
- Refinement of Implementation Tier criteria
- Clarity on Implementation Tiers and their relationship to Profiles

General Changes

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Affirms the Cybersecurity Enhancement Act of 2014 as the current chartering document

Declares Framework's applicability for "technology," minimally including

- Information Technology
- Operational Technology
- Cyber-Physical Systems, and
- Internet of Things

General Changes

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Declares Framework's applicability for all phases of the system lifecycle, including

- Design
- Development
- Deployment
- Operation
- Decommissioning

Administratively updates the Informative References

General Changes

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Removes previously proposed U.S. federal applicability statements. New federal policy and guidance has been provided since initial draft, such as:

- *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (Executive Order 13800)
- *Reporting Guidance for Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (OMB Memorandum M-17-25)
- Draft *The Cybersecurity Framework: Implementation Guidance for Federal Agencies* (draft NIST Interagency Report 8170)

Revised Section 4.0

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Self-Assessing Cybersecurity Risk with the Framework

Refined and simplified

Emphasizes the role of measurements in *self-assessment*

Stresses critical linkage of business results:

- Cost
- Benefit

…to cybersecurity risk management

Continued discussion of this linkage will occur under Roadmap area – Measuring Cybersecurity

Managing Cybersecurity Within Supply Chains

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

- Expands Section 3.3: ***Communicating Cybersecurity Requirements with Stakeholders*** including an updated entity diagram and taxonomy
- Adds Cyber SCRM as a Category to the Core
- Incorporates those supply chain considerations into the “External Participation” property of Implementation Tiers

Expanded Section 3.3

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Communicating Cybersecurity Requirements with Stakeholders

Primary objective of Cyber SCRM: Identify, assess, and mitigate cyber-related products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within supply chain. Activities may include:

- Determining cybersecurity requirements for suppliers
- Enacting cybersecurity requirements through formal agreement (e.g. contracts)
- Communicating to suppliers and partners how those cybersecurity requirements will be verified and validated
- Verifying cybersecurity requirements are met through a variety of assessment methodologies
- Governing and managing the above activities

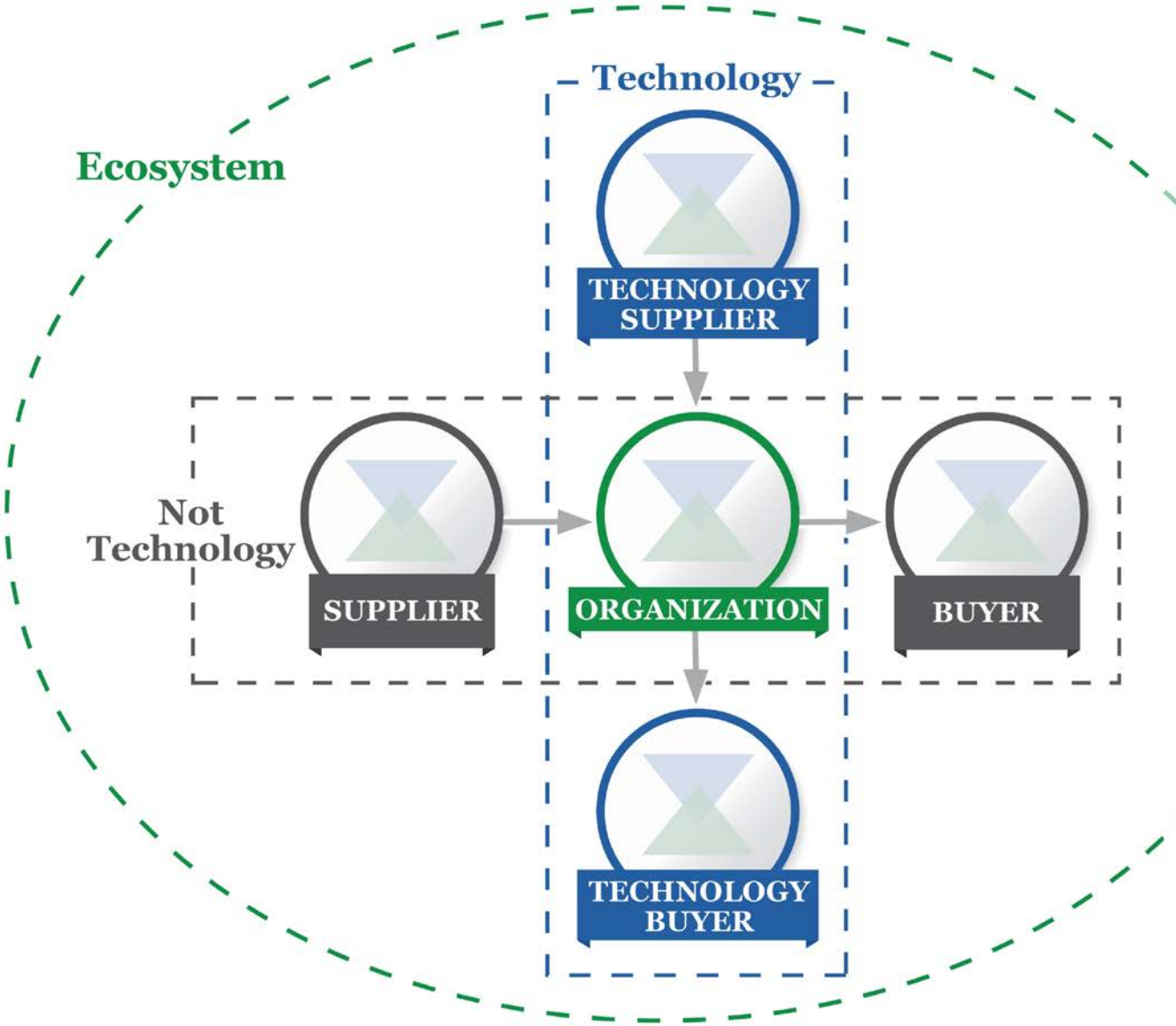
Expanded Section 3.3

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

- Cyber SCRM in the Framework aligns with Federal guidance:
  - ***Supply Chain Risk Management Practices for Federal Information Systems and Organizations*** (Special Publication 800-161)
- Stakeholders should be identified and factored into the protective, detective, response, and recovery capabilities
- Framework offers organizations and partners method to help ensure the product/service meets critical security outcomes
- Target profile can inform decisions about buying products, services – and assessing and tracking residual risk

Cyber SCRM Taxonomy

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1



- Simple Supplier-Buyer model
- Technology minimally includes IT, OT, CPS, IoT
- Applicable for public and private sector, including not-for-profits

Cyber SCRM in the Core

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
	ID.SC-2: Identify, prioritize and assess suppliers and third-party partners of information systems, components and services using a cyber supply chain risk assessment process
	ID.SC-3: Suppliers and third-party partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan
	ID.SC-4: Suppliers and third-party partners are routinely assessed to confirm that they are meeting their contractual obligations. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

Cyber SCRM in Implementation Tiers

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Tier	Key Cyber SCRM Language
1	…**does not understand its role in the larger ecosystem with respect to its dependencies and dependents**. …unaware of the cyber supply chain risks of the products and services it provides and that it uses.
2	…**understands its role in the larger ecosystem with respect to its own dependencies or dependents, but not both.** …aware of the cyber supply chain risks associated with the products and services it provides and that it uses, but does not act consistently or formally upon those risks.
3	…**understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks**. …aware of the cyber supply chain risks associated with the products and services it provides and that it uses. …acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.
4	…**understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks.** …uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. …communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

Identity Management, Authentication, and Access Control

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Category language refined to better account for authentication, authorization, and identity proofing

PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, ~~or~~and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Identity Management, Authentication, and Access Control

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Subcategories added on:

- **Identity Proofing (PR.AC-6), and**
- **Authentication (PR.AC-7)**

PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate	• **CIS CSC** 16 • **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 • **ISO/IEC 27001:2013** A.7.1.1, A.9.2.1 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	• **CIS CSC** 1, 12, 15, 16 • **COBIT 5** DSS05.04, DSS05.10, DSS06.10 • **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 • **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

Coordinated Vulnerability Disclosure

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Function: Respond

Category: Analysis

RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15

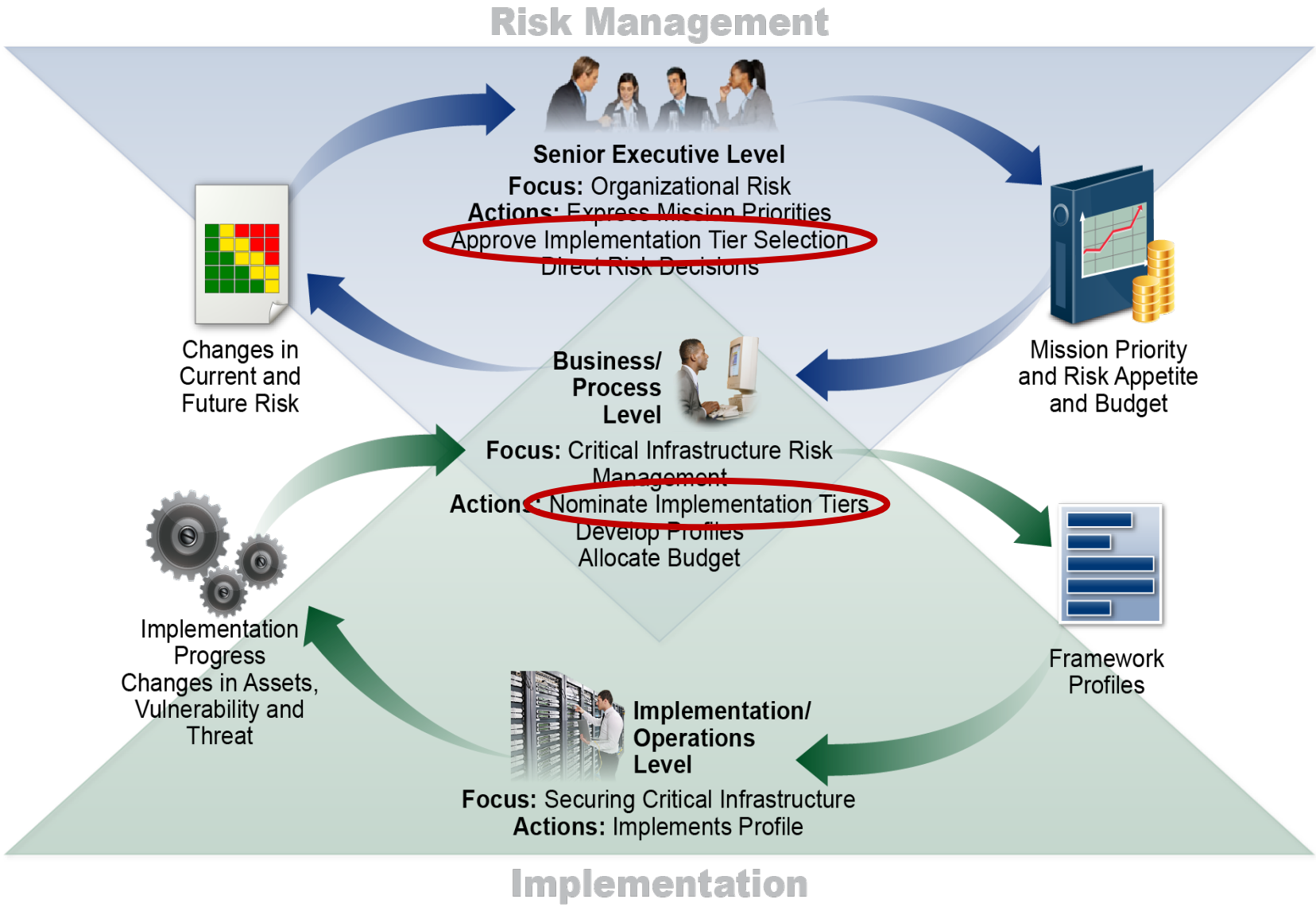
Integrated Risk Management in Implementation Tiers

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Tier	Excerpts from the new Integrated Risk Management Program Criteria
1	Minor Modifications
2	Consideration of **cybersecurity in organizational objectives may occur** at some levels of the organization, but not at all levels. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
3	The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure **consideration of cybersecurity through all lines of operation** in the organization.
4	The **relationship between cybersecurity risk and mission/business objectives is clearly understood and considered** when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of current and predicted risk environment and risk tolerances…Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.

Implementation Tiers and Profiles

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1



Tiers Included in the Framework 7-Step Process

Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

- **Step 1:** Prioritize and Scope
  - Implementation Tiers may be used to express varying risk tolerances
- **Step 2:** Orient
- **Step 3:** Create a Current Profile
- **Step 4:** Conduct a Risk Assessment
- **Step 5:** Create a Target Profile
  - When used in conjunction with an Implementation Tier, characteristics of the Tier level should be reflected in the desired cybersecurity outcomes
- **Step 6:** Determine, Analyze, and Prioritize Gaps
- **Step 7:** Implementation Action Plan

Roadmap Concepts

Roadmap to Improving Critical Infrastructure Cybersecurity

The Roadmap:

- identifies key areas of development, alignment, and collaboration
- provides a description of activities related to the Framework

Roadmap items are generally:

- Topics that are meaningful to critical infrastructure cybersecurity risk management
- Focus areas of both private sector and the federal government
- Related to Framework, but managed as separate efforts

Proposed Roadmap Topics

Draft Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1

9 topics

12 topics

Original Roadmap	New Topics	Proposed Roadmap
Conformity Assessment		*Confidence* Mechanisms reflect a broader range of activities that instill digital trust
Automated Indicator Sharing		*Cyber-Attack Lifecycle* reflects the importance of a holistic, approach that: - maximizes the value of threat intelligence, - discerns threat events from the large volumes of available data, and - reduces timelines to receive vulnerability information from researchers
Data Analytics		
	Coordinated Vulnerability Disclosure	

Proposed Roadmap Topics

Draft Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1

Original Roadmap	New Topics	Proposed Roadmap
Cybersecurity Workforce		Cybersecurity Workforce
Supply Chain Risk Management		*Cyber* Supply Chain Risk Management
Federal Agency Cybersecurity Alignment		Federal Agency Cybersecurity Alignment
	Governance and Enterprise Risk Management	*Governance and Enterprise Risk Management* continues stakeholder focus on board governance, organizational governance, and enterprise risk management

Proposed Roadmap Topics

Draft Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1

Original Roadmap	New Topics	Proposed Roadmap
Authentication		*Identity Management* accounts for a broader set of identity topics including authorization and identity proofing
International Aspects, Impacts, and Alignment		International Aspects, Impacts, and Alignment
	Measuring Cybersecurity	*Measuring Cybersecurity* addresses a growing need for cybersecurity measurement that is aligned and supportive of organizational objectives and decisions
Technical Privacy Standards		*Privacy Engineering* better aligns with the concepts in related NIST publications such as Interagency Report 8062 - *An Introduction to Privacy Engineering and Risk Management in Federal Systems*

Proposed Roadmap Topics

Draft Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1

Original Roadmap	New Topics	Proposed Roadmap
	Referencing Techniques	*Referencing Techniques* provides an understanding of future intent for the Informative References, as well as general process and methodology of relating one or more reference documents
	Small Business Awareness and Resources	*Small Business Awareness and Resources* continues focus on small business cybersecurity best practices and implementation - important to our Nation's cumulative cyber-posture

Feedback Is Always Appreciated!

Framework and Roadmap for Improving Critical Infrastructure Cybersecurity

- Public comments on Framework and Roadmap version 1.1 accepted until **11:59PM Eastern Standard Time on January 19, 2018**
- Comments received at cyberframework@nist.gov
- NIST expects to issue final V1.1 in 2018
- 2018 workshop will be held to:
    - Share and understand use and best practices
    - Determine early usage and utility of version 1.1
    - Roadmap topic area collaboration

Resources

Where to Learn More and Stay Current

Framework for Improving Critical Infrastructure Cybersecurity and related news and information:
www.nist.gov/cyberframework

Additional cybersecurity resources:
http://csrc.nist.gov/

Questions, comments, ideas:
cyberframework@nist.gov