The Framework for Improving Critical Infrastructure Cybersecurity

April 2018

cyberframework@nist.gov

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

Objective and Agenda

Objective: Convey Cybersecurity Framework use, while explaining features added in Version 1.1

- Charter
- Users
- Attributes, Components, & Approaches
- Draft Roadmap Version 1.1
- Framework Focus Areas
- Web Site
- Update Process

National Institute of Standards and Technology

About NIST

- Agency of U.S. Department of Commerce
- NIST's mission is to develop and promote measurement, standards and technology to enhance productivity, facilitate trade, and improve the quality of life.
- Federal, non-regulatory agency around since 1901

NIST Cybersecurity

- Cybersecurity since the 1970s
- Computer Security Resource Center – csrc.nist.gov

NIST Priority Research Areas


Advanced Manufacturing


IT and Cybersecurity


Healthcare


Forensic Science


Disaster Resilience


Cyber-physical Systems


Advanced Communications

Cybersecurity Framework *Current* Charter

Improving Critical Infrastructure Cybersecurity

February 12, 2013

"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"

Executive Order 13636

December 18, 2014

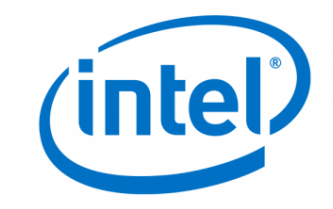
Amends the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) to say:

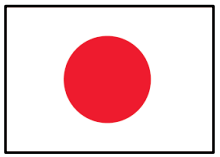
"…on an ongoing basis, facilitate and support the development of a ***voluntary***, ***consensus-based***, ***industry-led*** *set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure"*

Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

Cybersecurity Framework Users

Framework for Improving Critical Infrastructure Cybersecurity





AT&T

NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

THE UNIVERSITY OF CHICAGO

KAISER PERMANENTE®

ONTARIO ENERGY BOARD

DUKE ENERGY®

TORONTO

NOVANT HEALTH

SIEMENS

JPMorganChase

Version 1.0 and 1.1 Are Fully Compatible

Framework for Improving Critical Infrastructure Cybersecurity

- Additions, including new categories and subcategories, do not invalidate existing V1.0 uses or 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	

Key Framework Attributes

Principles of the Current and Future Versions of Framework

Common and accessible language

- Understandable by many professionals

It's adaptable to many **technologies**[1.1], **lifecycle phases**[1.1], sectors and uses

- Meant to be *customized*

It's risk-based

- A Catalog of cybersecurity outcomes
- Does not provide *how or how much* cybersecurity is appropriate

It's meant to be paired

- Take advantage of great pre-existing things

It's a living document

- Enable best practices to become *standard practices for everyone*
- Can be updated as *technology and threats* change
- Evolves *faster* than regulation and legislation
- Can be updated as stakeholders *learn from implementation*

Cybersecurity Framework Components

Cybersecurity outcomes and informative references

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

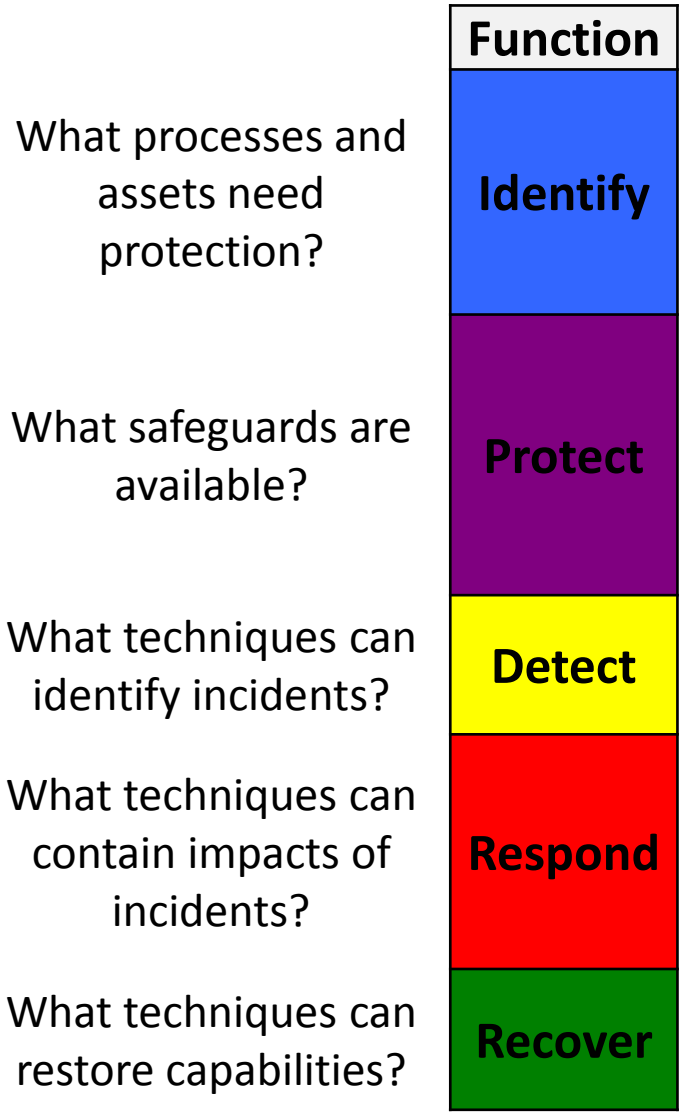
Aligns industry standards and best practices to the Framework Core in an implementation scenario
Supports prioritization and measurement while factoring in business needs

Implementation Tiers

	1 Partial	2 Risk Informed	3 Repeatable	4 Adaptive
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk[1.1]** • benefits my sharing or receiving information from outside parties			

Core

A Catalog of Cybersecurity Outcomes



- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

Core

A Catalog of Cybersecurity Outcomes

	Function	Category
What processes and assets need protection?	**Identify**	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management[1.1]
What safeguards are available?	**Protect**	**Identity Management, Authentication and Access Control**[1.1]
		Awareness and Training
		Data Security
		Information Protection Processes & Procedures
		Maintenance
		Protective Technology
What techniques can identify incidents?	**Detect**	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
What techniques can contain impacts of incidents?	**Respond**	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
What techniques can restore capabilities?	**Recover**	Recovery Planning
		Improvements
		Communications

Core – Example[1.1]

Cybersecurity Framework Component

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**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	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

Core – Example[1.1]

Cybersecurity Framework Component

Function	Category	Subcategory	Informative References
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, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**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

Core – Example

Cybersecurity Framework Component

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		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

1.1

Profile

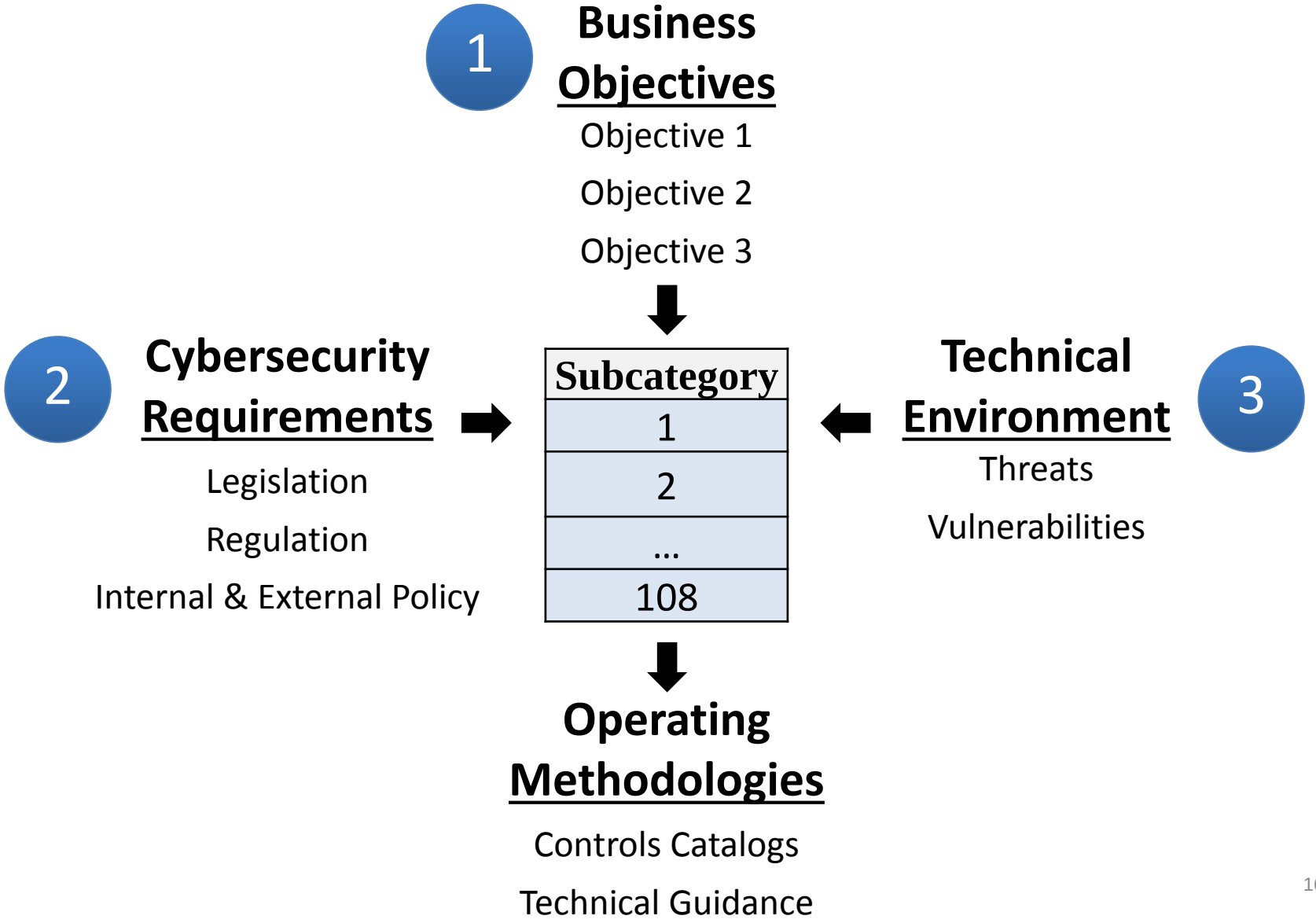
Customizing Cybersecurity Framework

Ways to think about a Profile:

- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity risk management

Profile Foundational Information

A Profile Can be Created from Three Types of Information



Framework Seven Step Process

Gap Analysis Using Framework Profiles

- **Step 1:** Prioritize and Scope
  - Implementation Tiers may be used to express varying risk tolerances[1.1]
- **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[1.1]
- **Step 6:** Determine, Analyze, and Prioritize Gaps
- **Step 7:** Implementation Action Plan

Resource and Budget Decisioning

Framework supports operating decisions and improvement

Sub-category	Priority	Gaps	Budget	Year 1 Activities	Year 2 Activities
1	moderate	small	$$$		X
2	high	large	$$	X	
3	moderate	medium	$	X	
…	…	…	…		
108	moderate	none	$$		reassess

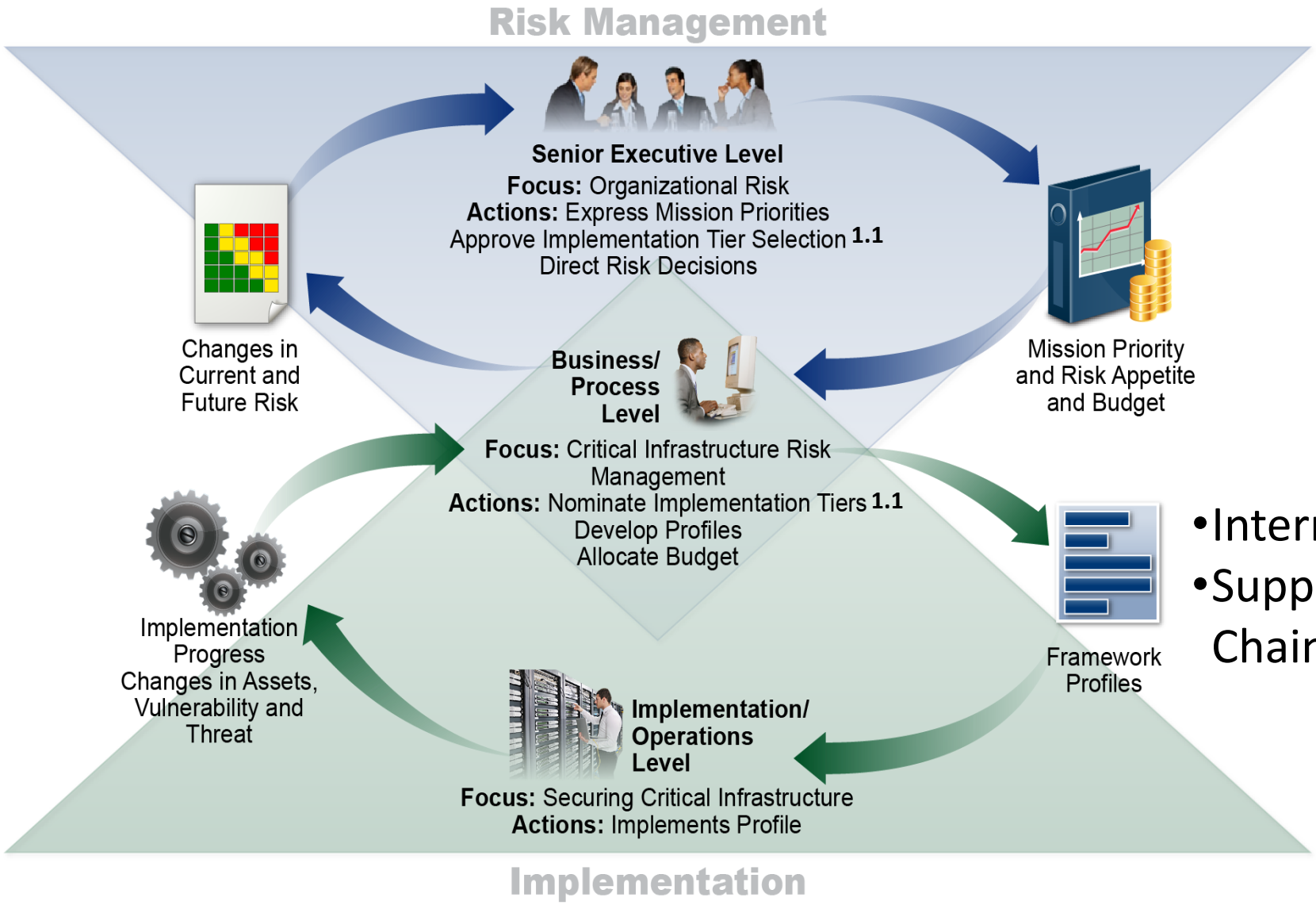
Resource and Budget Decisioning

Framework supports operating decisions and improvement

Sub-category	Priority	Gaps	Budget	Year 1 Activities	Year 2 Activities
1	moderate	small	$$$		X
2	high	large	$$	X	
3	moderate	medium	$	X	
…	…	…	…		
108	moderate	none	$$		reassess
Step 5 Target Profile		**Step 6**		**Step 7**	

Supporting Risk Management with Framework

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1



- Internal
- Supply Chain

Operate

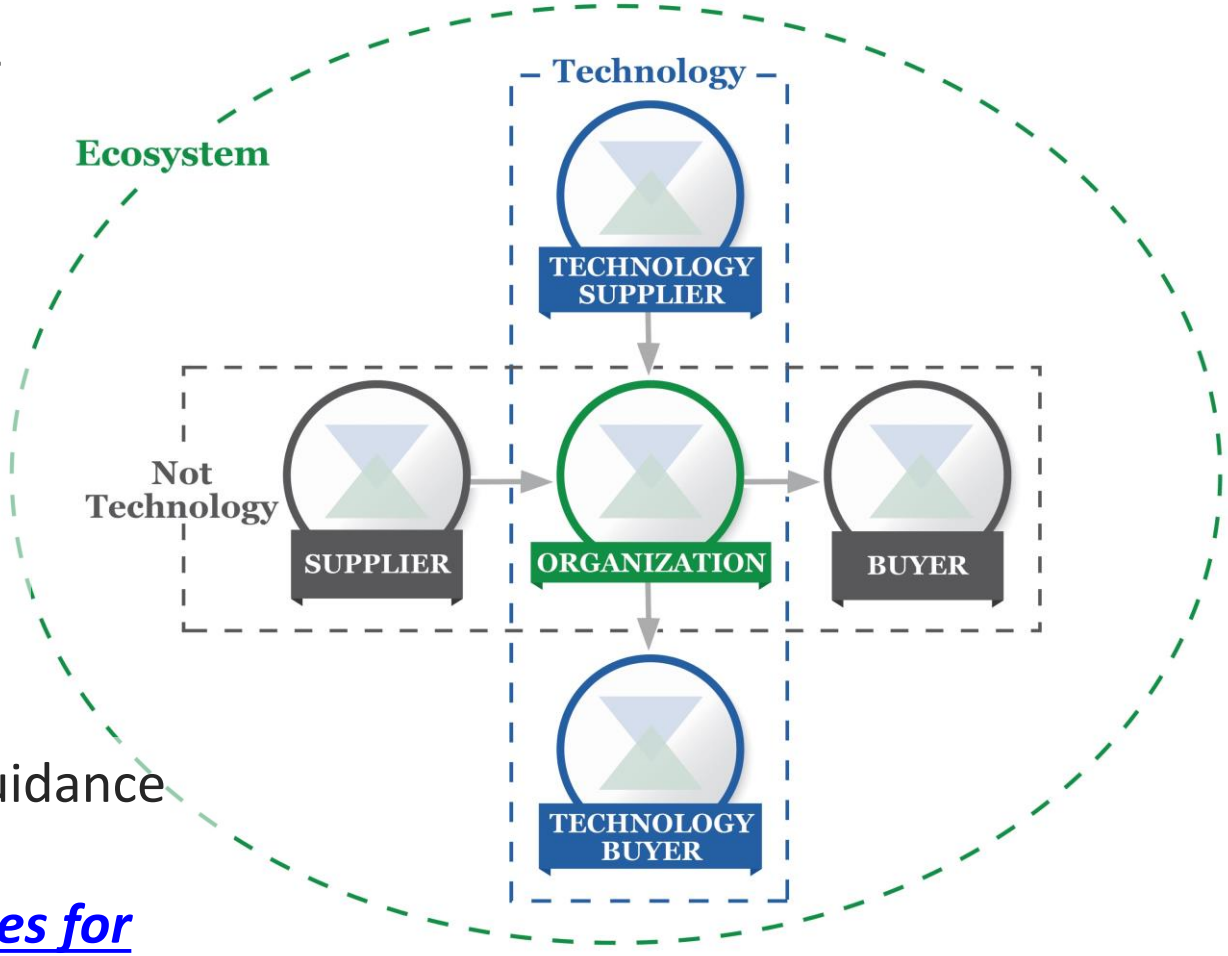
Use Cybersecurity Framework Profiles to distribute and organize labor

Subcats	Reqs	Priorities	Who	What	When	Where	How
1	A, B	High					
2	C, D, E, F	High					
3	G, H, I, J	Low					
…	…	…					
108	XX, YY, ZZ	Mod					

Cyber SCRM Taxonomy[1.1]

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
- Aligns with Federal guidance ***Supply Chain Risk Management Practices for Federal Information Systems and Organizations*** (Special Publication 800-161)



Self-Assessing Cybersecurity Risk[1.1]

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

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

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

Original Roadmap *9 topics*	Proposed Roadmap *12 topics*	
Conformity Assessment	*Confidence* Mechanisms	
Automated Indicator Sharing	*Cyber-Attack Lifecycle* Includes Coordinated Vulnerability Disclosure	
Data Analytics		
Cybersecurity Workforce	Cybersecurity Workforce	
Supply Chain Risk Management	*Cyber* Supply Chain Risk Management	
Federal Agency Cybersecurity Alignment	Federal Agency Cybersecurity Alignment	Focus
	Governance and Enterprise Risk Management	
Authentication	Identity Management	
International Aspects, Impacts, and Alignment	International Aspects, Impacts, and Alignment	Focus
	Measuring Cybersecurity	
Technical Privacy Standards	*Privacy Engineering*	
	Referencing Techniques	
	Small Business Awareness and Resources	Focus

Small Business Guidance and Initiatives

Framework for Improving Critical Infrastructure Cybersecurity

Small Business Information Security: the Fundamentals

NIST Computer Security Resource Center

Small Business Center

NIST Computer Security Resource Center

CyberSecure My Business

National Cyber Security Alliance

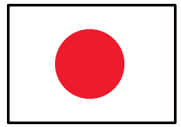
Small Business Starter Profiles

NIST Framework Team

International Use

Framework for Improving Critical Infrastructure Cybersecurity

- Japanese translation by Information-technology Promotion Agency
- Italian adaptation within Italy's National Framework for Cybersecurity
- Hebrew adaptation by Government of Israel
- Bermuda uses it within government and recommends it to industry
- Uruguay government is currently on Version 3.1 of their adaptation
- Focus of International Organization for Standardization & International Electrotechnical Commission



Proposed U.S. Federal Usage

NIST IR 8170 The Cybersecurity Framework: Implementation Guidance for Federal Agencies

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
Executive Order 13800

1. **Integrate enterprise and cybersecurity risk management**
2. **Manage cybersecurity requirements**
3. **Integrate and align cybersecurity and acquisition processes**
4. **Evaluate organizational cybersecurity**
5. **Manage the cybersecurity program**
6. **Maintain a comprehensive understanding of cybersecurity risk** *(supports RMF Authorize)*
7. **Report cybersecurity risks** *(supports RMF Monitor)*
8. **Inform the tailoring process** *(supports RMF Select)*

FISMA Implementation Pub Schedule

As of 8 February 2018, Subject to Change

NIST Special Publication 800-37, Revision 2: *Risk Management Framework for Security and Privacy*

Initial Public Draft: May 2018

Final Public Draft: July 2018

Final Publication: October 2018

NIST Special Publication 800-53, Revision 5: *Security and Privacy Controls*

Final Public Draft: October 2018

Final Publication: December 2018

NIST Special Publication 800-53A, Revision 5: *Assessment Procedures for Security and Privacy Controls*

Initial Public Draft: March 2019

Final Public Draft: June 2019

Final Publication: September 2019

FIPS Publication 200, Revision 1: *Minimum Security Requirements*

Initial Public Draft: October 2018

Final Public Draft: April 2019

Final Publication: July 2019

FIPS Publication 199, Revision 1: *Security Categorization*

Initial Public Draft: December 2018

Final Public Draft: May 2019

Final Publication: August 2019

Updates - https://csrc.nist.gov/Projects/Risk-Management/Schedule

Questions or comments - sec-cert@nist.gov

Supporting Healthy Regulatory Environments

Framework for Improving Critical Infrastructure Cybersecurity

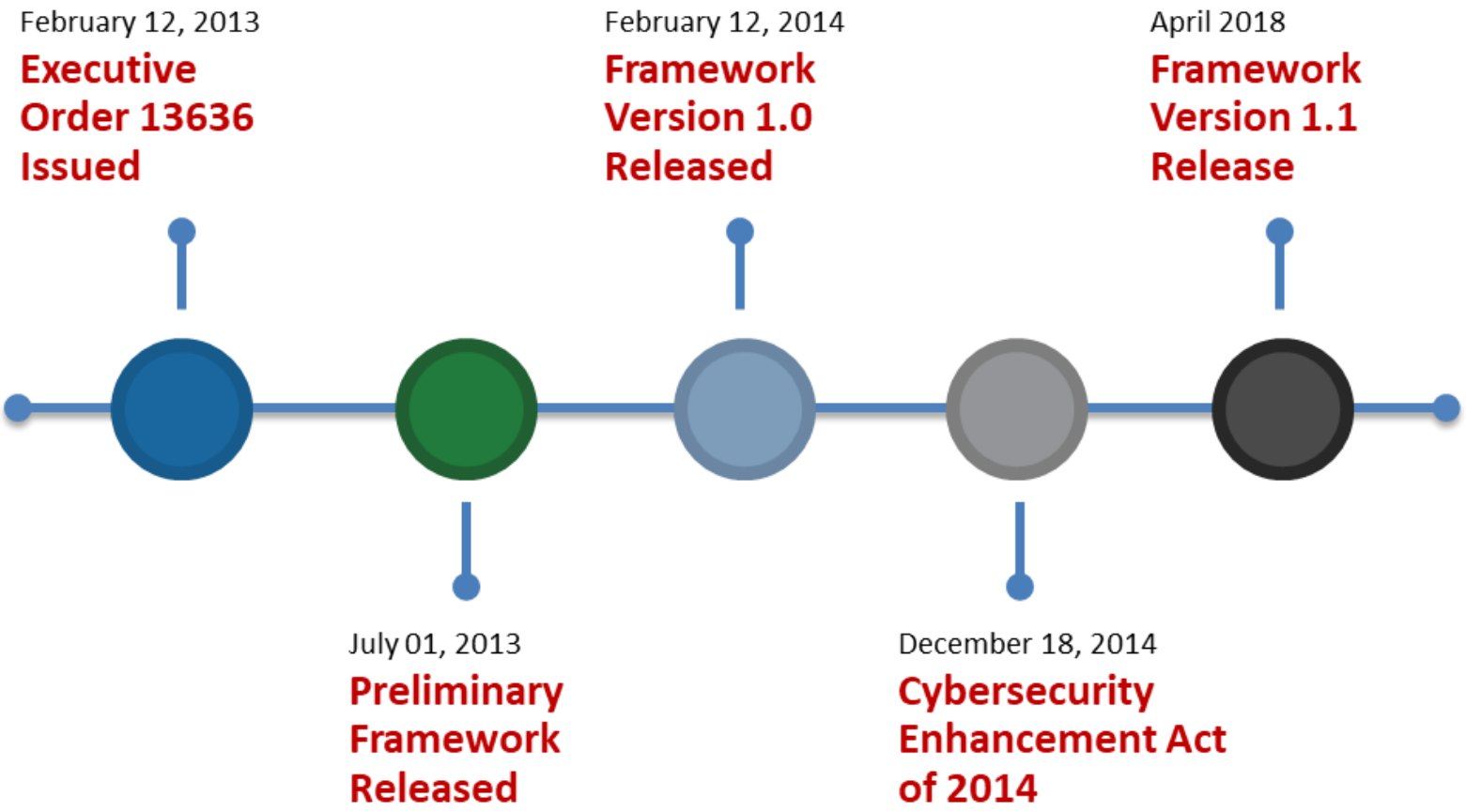
Bulk Liquid Transport Profile
U.S. Coast Guard

Financial Services Framework Customization and Profile
Financial Services Sector Coordinating Council

Connected Vehicle Profile
U.S. Department of Transportation Smart City Pilot

Cybersecurity Risk Management and Best Practices Working Group 4: Final Report
Communications Security, Reliability, and Interoperability Council

Eras of Cybersecurity Framework



The Framework Web Site

www.nist.gov/cyberframework

NIST Search NIST NIST MENU

CYBERSECURITY FRAMEWORK

Helping organizations to better understand and improve their management of cybersecurity risk

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources +
- Newsroom +

Credit: N. Hanacek/NIST

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

LATEST UPDATES

- Registration is now available for an upcoming Webcast providing an overview of Framework Version 1.1, hosted by NIST on April 27th.

Self-Help Web Materials

www.nist.gov/cyberframework

Self-Help Web Materials

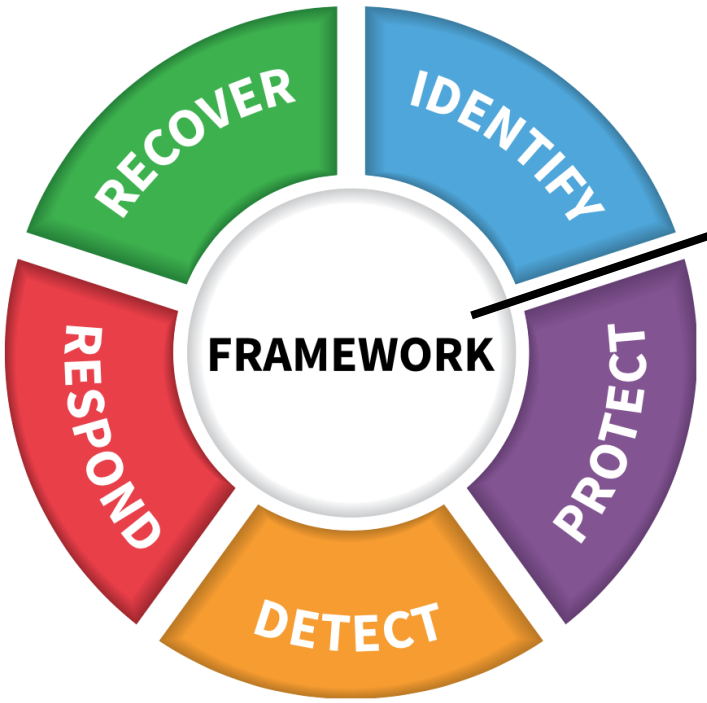
www.nist.gov/cyberframework

Resources

https://www.nist.gov/cyberframework/framework-resources-0

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources +
- Newsroom +

Framework Resources



General Resources sorted by User Group:

- Critical Infrastructure
- Small and Medium Business
- International
- Federal
- State Local Tribal Territorial Governments
- Academia
- Assessments & Auditing
- General

Over 150 Unique Resources for Your Understanding and Use!

Resources - State & Local

https://www.nist.gov/cyberframework/state-local-tribal-and-territorial-resources

Texas, Department of Information Resources

- Aligned Agency Security Plans with Framework
- Aligned Product and Service Vendor Requirements with Framework

North Dakota, Information Technology Department

- Allocated Roles & Responsibilities using Framework
- Adopted the Framework into their Security Operation Strategy

Houston, Greater Houston Partnership

- Integrated Framework into their Cybersecurity Guide
- Offer On-Line Framework Self-Assessment

National Association of State CIOs

- 2 out of 3 CIOs from the 2015 NASCIO Awards cited Framework as a part of their award-winning strategy

New Jersey

- Developed a cybersecurity framework that aligns controls and procedures with Framework

Recent NIST Work Products

https://www.nist.gov/cyberframework/framework-resources-0

Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Self-Assessment Criteria

Baldrige Cybersecurity Excellence Builder

Maritime Profile

U.S. Coast Guard Bulk Liquid Transport Profile

Resources

https://www.nist.gov/cyberframework/framework-resources-0

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources +
- Newsroom +

Framework Resources

NIST Special Publications

Computer Security Resource Center
800 Series @ csrc.nist.gov

National Cybersecurity Center of Excellence
1800 Series @ nccoe.nist.gov

Over 150 Unique Resources for Your Understanding and Use!

NIST Special Publications by Category

https://www.nist.gov/cyberframework/protect

PROTECT (PR)

Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

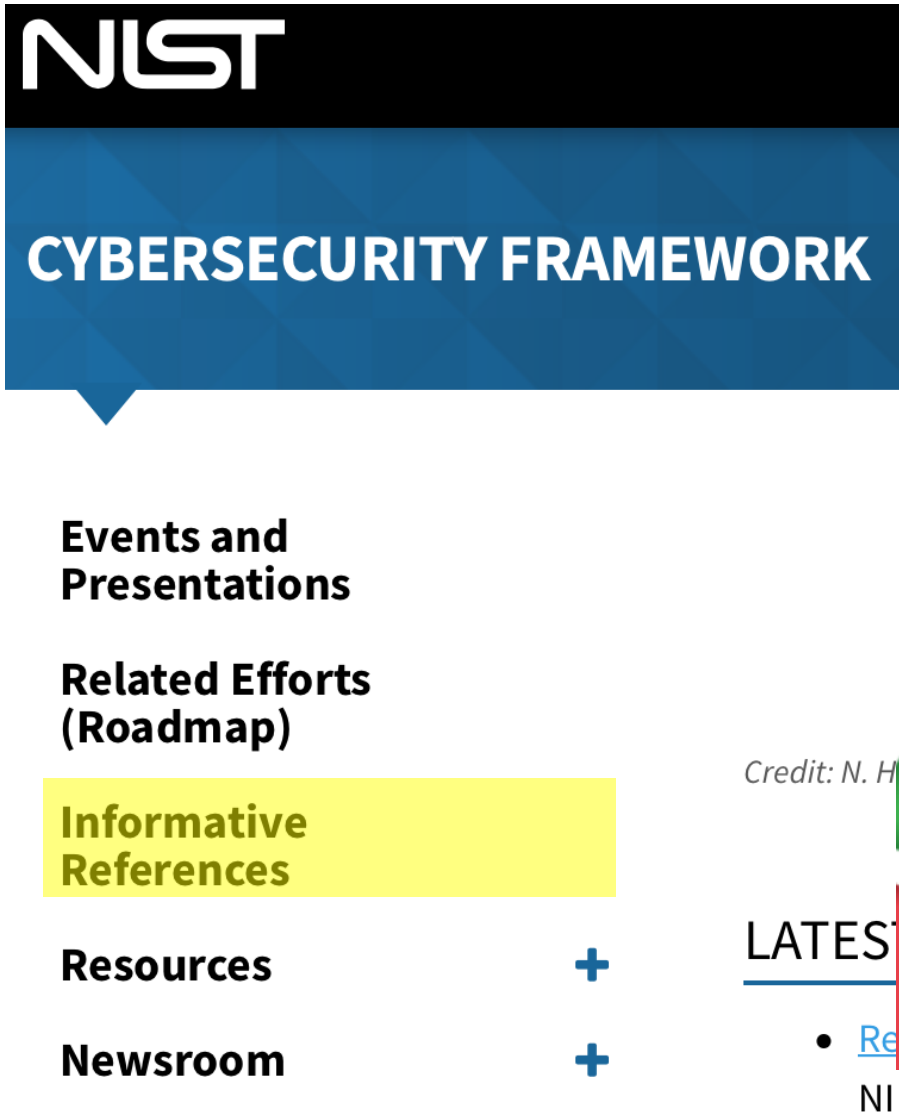
800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
800-181	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
800-50	Building an Information Technology Security Awareness and Training Program
800-16 Rev. 1	A Role-Based Model for Federal Information Technology/Cybersecurity Training
800-114 Rev. 1	User's Guide to Telework and Bring Your Own Device (BYOD) Security

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

800-133	Recommendation for Cryptographic Key Generation
800-111	Guide to Storage Encryption Technologies for End User Devices
800-175A	Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies
800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
800-89	Recommendation for Obtaining Assurances for Digital Signature Applications

Online Informative References

https://www.nist.gov/cyberframework/informative-references



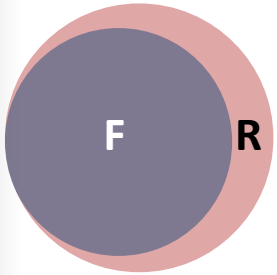
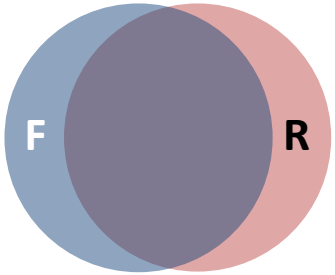
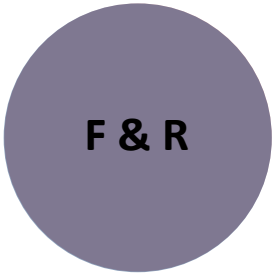
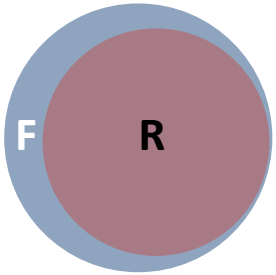
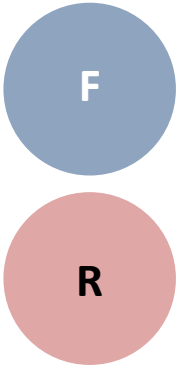
Core – Example[1.1]

Cybersecurity Framework Component

Function	Category	Subcategory	Informative References
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, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**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

Relationship Types

Online Informative References

Case 1	Case 2	Case 3	Case 4	Case 5
Subset of	**Intersects with**	**Equivalent to**	**Superset of**	**Not related to**
				

Key

Framework – blue

Reference Document - red

Continued Improvement of Critical Infrastructure Cybersecurity

Update Activities	Engagement
Request for Information – Views on the Framework for Improving Critical Infrastructure Cybersecurity – Dec 2015	105 Responses
7th Workshop – Apr 2016	653 Physical Attendees, 140 Online Attendees
Draft 1 – Framework Version 1.1 – Released Jan 2017	Approx. 42,000+ downloads As of 4/27/18
Request for Comment – Proposed update to the Framework for Improving Critical Infrastructure Cybersecurity – Jan 2017	129 Responses
8th Workshop – May 2017	517 Physical Attendees, 1528 Online Attendees
Draft 2 – Framework Version 1.1 – Released Dec 2017	Approx. 32,000+ downloads As of 4/27/18
Request for Comment – Cybersecurity Framework Version 1.1 – Draft 2 – Dec 2017	89 Responses
Framework Version 1.1 – Release April 2018	Approx. 27,000+ downloads thus far

Continued Improvement

Living Document Process

https://www.nist.gov/cyberframework/online-learning/update-process

NIST

Search NIST

NIST MENU

CYBERSECURITY FRAMEWORK

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning −
  - Components of the Framework
  - Uses and Benefits of the Framework
  - History and Creation of the Framework
  - Informative References
  - The Five Functions
  - Introduction to the Framework Roadmap
  - Update Process

Framework Update Process

Overview

This online learning module provides readers with insight into how NIST plans to maintain the Framework for Improving Critical Infrastructure Cybersecurity ("The Framework"). This online learning module builds on the History and Creation of the Framework by describing how lessons learned from developing the Framework and preparing for the release of version 1.1 of the Framework led to the Framework update process.

Update Process

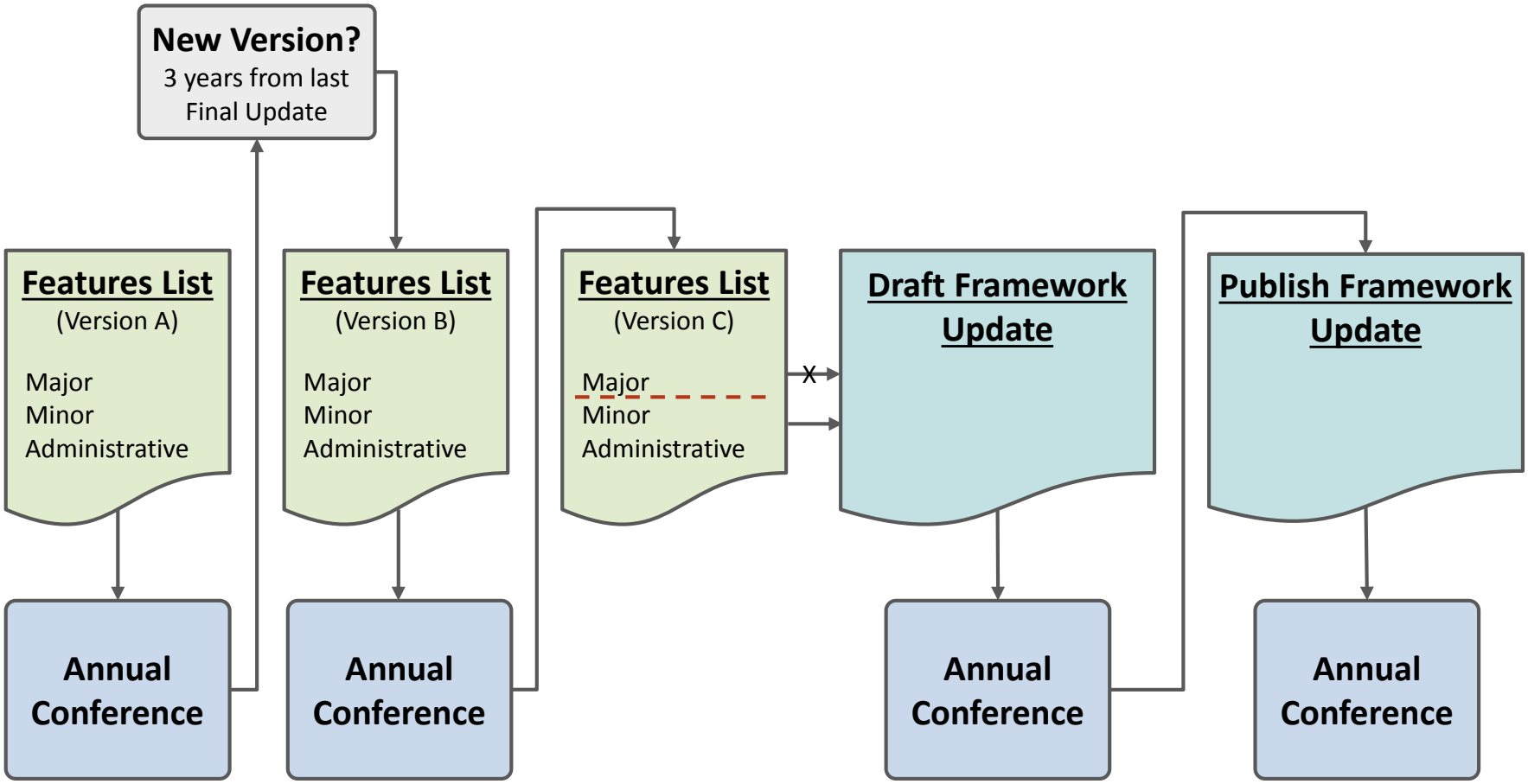
NIST routinely engages industry through three primary activities. First, NIST continually and regularly engages in community outreach activities by attending meetings, events, and roundtable dialogs. Second, NIST solicits direct feedback from industry through requests for information (RFI), requests for comments (RFC), and through the NIST Framework team's email alias (cyberframework@nist.gov). Finally, NIST observes and monitors relevant resources and references as published by the government, academia, and industry.

As described in Figure 1, below, NIST catalogs all comments and feature enhancements received on the Framework in a Features List. NIST then categorizes all comments and feature enhancement suggestions on the Features Lists as either Major, Minor, or Administrative comments based on the degree to which implementing the change would impact the backwards compatibility of the Framework. The features are also prioritized based on their importance to stakeholders.

Milestones

Three Year Minimum Update Cycle

https://www.nist.gov/cyberframework/online-learning/update-process



Ways to Help

Stakeholder Recommended Actions

- Create and share your Resources with others in coordination with NIST
  - Customize Framework for your sector or community
  - Publish a sector or community Profile or relevant Online Informative Reference
- Publish Success Stories of your Framework implementation in coordination with NIST
- Advocate for the Framework throughout your sector or community, with related sectors and communities.
- Submit an idea for the NIST Call for Speakers

cyberframework@nist.gov for all NIST coordination and communication

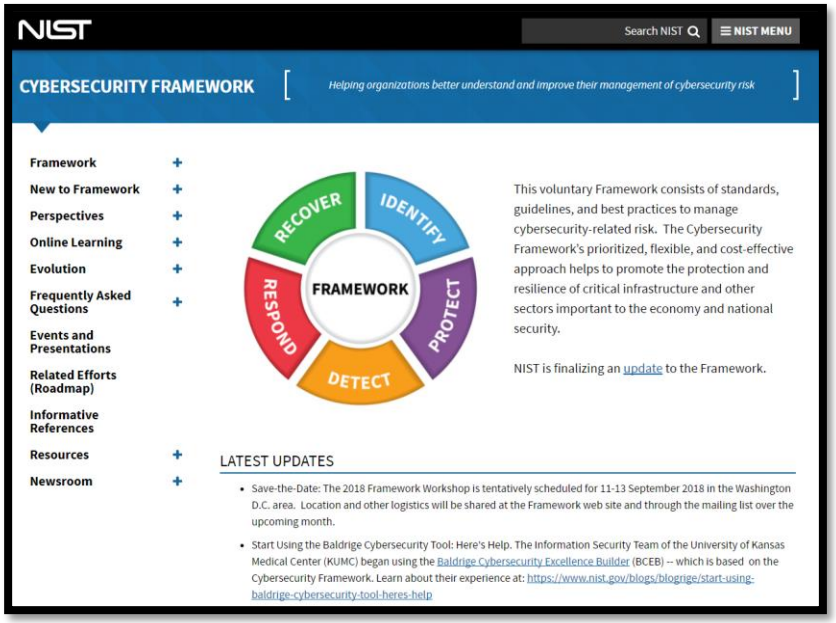
Upcoming

15-16 May 2018	Federal Computer Security Managers Forum https://csrc.nist.gov/Events/2018/Federal-Computer-Security-Managers-Forum-2-day
Spring 2018	Publication of Roadmap for Improving Critical Infrastructure Cybersecurity
Spring 2018	Publication of NIST Interagency Report 8170
Summer 2018	Spanish Language Framework Version 1.1
6-8 November 2018	NIST Cybersecurity Risk Management Conference - Call for Speakers
Winter 2018-19	Small Business Starter Profiles

Resources

- 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



Questions?