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
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
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

<table>
<thead>
<tr>
<th>Component</th>
<th>Version 1.0</th>
<th>Version 1.1</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functions</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Categories</td>
<td>22</td>
<td>23</td>
<td>- Added a new category in ID.SC – Supply Chain</td>
</tr>
<tr>
<td>Subcategories</td>
<td>98</td>
<td>108</td>
<td>- Added 5 subcategories in ID.SC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Added 2 subcategories in PR.AC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Added 1 subcategory each to PR.DS, PR.PT, RS.AN</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Clarified language in 7 others</td>
</tr>
<tr>
<td>Informative References</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>
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\textsuperscript{1.1}, lifecycle phases\textsuperscript{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

Cybersecurity Framework Components

Framework Core in an implementation scenario
Supports prioritization and measurement while factoring in business needs
# Implementation Tiers

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Partial</td>
<td>Risk Informed</td>
<td>Repeatable</td>
<td>Adaptive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Management Process</th>
<th>The functionality and repeatability of cybersecurity risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Risk Management Program</td>
<td>The extent to which cybersecurity is considered in broader risk management decisions</td>
</tr>
<tr>
<td>External Participation</td>
<td>The degree to which the organization:</td>
</tr>
<tr>
<td></td>
<td>• monitors and manages supply chain risk¹.¹</td>
</tr>
<tr>
<td></td>
<td>• benefits my sharing or receiving information from outside parties</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Asset Management&lt;br&gt;Business Environment&lt;br&gt;Governance&lt;br&gt;Risk Assessment&lt;br&gt;Risk Management Strategy&lt;br&gt;Supply Chain Risk Management¹¹</td>
</tr>
<tr>
<td>Protect</td>
<td>Identity Management, Authentication and Access Control¹¹&lt;br&gt;Awareness and Training&lt;br&gt;Data Security&lt;br&gt;Information Protection Processes &amp; Procedures&lt;br&gt;Maintenance&lt;br&gt;Protective Technology</td>
</tr>
<tr>
<td>Detect</td>
<td>Anomalies and Events&lt;br&gt;Security Continuous Monitoring&lt;br&gt;Detection Processes</td>
</tr>
<tr>
<td>Respond</td>
<td>Response Planning&lt;br&gt;Communications&lt;br&gt;Analysis&lt;br&gt;Mitigation&lt;br&gt;Improvements</td>
</tr>
<tr>
<td>Recover</td>
<td>Recovery Planning&lt;br&gt;Improvements&lt;br&gt;Communications</td>
</tr>
</tbody>
</table>
# Core – Example 1.1

## Cybersecurity Framework Component

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| 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  
CIS APO10.01, APO10.02, APO10.03, APO12.04, APO12.08, APO12.11, APO13.02, APO13.03, APO13.04, BAI02.07, BAI02.08, 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, APO10.03, APO12.04, APO12.08, APO12.11, APO13.02, APO13.03, APO13.04, BAI02.07, BAI02.08, BAI04.02  
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

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| 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 |
| PROTECT (PR) | | 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  
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

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESPOND (RS)</td>
<td><strong>Analysis (RS.AN):</strong> Analysis is conducted to ensure effective response and support recovery activities.</td>
<td><strong>RS.AN-1:</strong> Notifications from detection systems are investigated</td>
<td>CIS CSC 4, 6, 8, 19&lt;br&gt;COBIT 5 DSS02.04, DSS02.07&lt;br&gt;ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8&lt;br&gt;ISA 62443-3-3:2013 SR 6.1&lt;br&gt;ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5&lt;br&gt;NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RS.AN-2:</strong> The impact of the incident is understood</td>
<td>COBIT 5 DSS02.02&lt;br&gt;ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8&lt;br&gt;ISO/IEC 27001:2013 A.16.1.4, A.16.1.6&lt;br&gt;NIST SP 800-53 Rev. 4 CP-2, IR-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RS.AN-3:</strong> Forensics are performed</td>
<td>COBIT 5 APO12.06, DSS03.02, DSS05.07&lt;br&gt;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&lt;br&gt;ISO/IEC 27001:2013 A.16.1.7&lt;br&gt;NIST SP 800-53 Rev. 4 AU-7, IR-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RS.AN-4:</strong> Incidents are categorized consistent with response plans</td>
<td>CIS CSC 19&lt;br&gt;COBIT 5 DSS02.02&lt;br&gt;ISA 62443-2-1:2009 4.3.4.5.6&lt;br&gt;ISO/IEC 27001:2013 A.16.1.4&lt;br&gt;NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RS.AN-5:</strong> 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)</td>
<td>CIS CSC 4, 19&lt;br&gt;COBIT 5 EDM03.02, DSS05.07&lt;br&gt;NIST SP 800-53 Rev. 4 SI-5, PM-15</td>
</tr>
</tbody>
</table>
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

1. Business Objectives
   - Objective 1
   - Objective 2
   - Objective 3

2. Cybersecurity Requirements
   - Legislation
   - Regulation
   - Internal & External Policy

3. Technical Environment
   - Threats
   - Vulnerabilities

Subcategory
1
2
...  
108

Operating Methodologies
- Controls Catalogs
- Technical Guidance
Framework Seven Step Process
Gap Analysis Using Framework Profiles

• **Step 1:** Prioritize and Scope
  • Implementation Tiers may be used to express varying risk tolerances\(^11\)

• **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\(^11\)

• **Step 6:** Determine, Analyze, and Prioritize Gaps

• **Step 7:** Implementation Action Plan
## Resource and Budget Decisioning

*Framework supports operating decisions and improvement*

<table>
<thead>
<tr>
<th>Sub-category</th>
<th>Priority</th>
<th>Gaps</th>
<th>Budget</th>
<th>Year 1 Activities</th>
<th>Year 2 Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>moderate</td>
<td>small</td>
<td>$$ $$</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>high</td>
<td>large</td>
<td>$$</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>moderate</td>
<td>medium</td>
<td>$</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>moderate</td>
<td>medium</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>108</td>
<td>moderate</td>
<td>none</td>
<td>$$</td>
<td>reassess</td>
<td></td>
</tr>
</tbody>
</table>
## 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

Risk Management

Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions

Business/Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget

Implementation/Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

• Internal
• Supply Chain

Framework Profiles
**Operate**

*Use Cybersecurity Framework Profiles to distribute and organize labor*

<table>
<thead>
<tr>
<th>Subcats</th>
<th>Reqs</th>
<th>Priorities</th>
<th>Who</th>
<th>What</th>
<th>When</th>
<th>Where</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A, B</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>C, D, E, F</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>G, H, I, J</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>XX, YY, ZZ</td>
<td>Mod</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cyber SCRM Taxonomy\textsuperscript{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

\textit{Supply Chain Risk Management Practices for Federal Information Systems and Organizations} (Special Publication 800-161)
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
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*

<table>
<thead>
<tr>
<th>Original Roadmap</th>
<th>Proposed Roadmap</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>9 topics</strong></td>
<td><strong>12 topics</strong></td>
</tr>
<tr>
<td>Conformity Assessment</td>
<td><em>Confidence Mechanisms</em></td>
</tr>
</tbody>
</table>
| Automated Indicator Sharing | *Cyber-Attack Lifecycle*  
  Includes Coordinated Vulnerability Disclosure |
| Data Analytics     | *Cybersecurity Workforce*  |
| Cybersecurity Workforce | *Cyber Supply Chain Risk Management* |
| Supply Chain Risk Management | *Governance and Enterprise Risk Management* |
| Federal Agency Cybersecurity Alignment | *Federal Agency Cybersecurity Alignment* |
| Authentication     | Identity Management |
| International Aspects, Impacts, and Alignment | *International Aspects, Impacts, and Alignment* |
| Technical Privacy Standards | *Measuring Cybersecurity* |
| 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

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)*

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

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Executive Order 13800
<table>
<thead>
<tr>
<th>Publication</th>
<th>Status</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Final Publication: September 2019</td>
<td></td>
</tr>
<tr>
<td>NIST Special Publication 800-53, Revision 5: Security and Privacy Controls</td>
<td>Final Public Draft: October 2018</td>
<td>Final Publication: July 2019</td>
</tr>
<tr>
<td></td>
<td>Final Publication: July 2019</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Final Publication: August 2019</td>
<td></td>
</tr>
</tbody>
</table>


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

- **February 12, 2013**
  - Executive Order 13636 Issued
- **February 12, 2014**
  - Framework Version 1.0 Released
- **April 2018**
  - Framework Version 1.1 Release
- **July 01, 2013**
  - Preliminary Framework Released
- **December 18, 2014**
  - Cybersecurity Enhancement Act of 2014
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.

Credit: N. Hanacek/NIST

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

CYBERSECURITY FRAMEWORK

- Framework
- New to Framework
- Perspectives
- Success Stories
- Online Learning
- Evolution
- Frequently Asked Questions
Self-Help Web Materials
www.nist.gov/cyberframework

Events and Presentations

Related Efforts (Roadmap)

Informative References

Resources +

Newsroom +

Credit: N. H

LATES

• Re
NI
Over 150 Unique Resources for Your Understanding and Use!
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

Over 150 Unique Resources for Your Understanding and Use!
| 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 |
| 800-89 | 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

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| 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  
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
- **Subset of**
- **Framework (F)**
- **Reference Document (R)**

### Case 2
- **Intersects with**
- **Framework (F)**
- **Reference Document (R)**

### Case 3
- **Equivalent to**
- **Framework (F)**
- **Reference Document (F & R)**

### Case 4
- **Superset of**
- **Framework (F)**
- **Reference Document (R)**

### Case 5
- **Not related to**
- **Framework (F)**
- **Reference Document (R)**

### Key
- **Framework** – blue
- **Reference Document** – red
# Continued Improvement of Critical Infrastructure Cybersecurity

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spring 2018</td>
<td>Publication of Roadmap for Improving Critical Infrastructure Cybersecurity</td>
<td></td>
</tr>
<tr>
<td>Spring 2018</td>
<td>Publication of NIST Interagency Report 8170</td>
<td></td>
</tr>
<tr>
<td>Summer 2018</td>
<td>Spanish Language Framework Version 1.1</td>
<td></td>
</tr>
<tr>
<td>6-8 November 2018</td>
<td>NIST Cybersecurity Risk Management Conference - Call for Speakers</td>
<td></td>
</tr>
<tr>
<td>Winter 2018-19</td>
<td>Small Business Starter Profiles</td>
<td></td>
</tr>
</tbody>
</table>
Resources

- Framework for Improving Critical Infrastructure Cybersecurity and related news and information:
  - [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)

- Additional cybersecurity resources:

- Questions, comments, ideas:
  - [cyberframework@nist.gov](mailto:cyberframework@nist.gov)
Questions?