The Framework for Improving Critical Infrastructure Cybersecurity

May 2018

cyberframework@nist.gov
Objective and Agenda

Objective: Convey Cybersecurity Framework v1.1, relevant CSF happenings, and status of NISTIR 8170

- Charter
- Attributes & Components
- NISTIR 8170
- Web Site
- Upcoming events
- Informative References
Cybersecurity Framework Current Charter

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”

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)
**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</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>References</td>
<td></td>
<td></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

- **Core**: Enables communication of cyber risk across an organization.
- **Tiers**: Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics.
- **Profile**: 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

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

<table>
<thead>
<tr>
<th><strong>Risk Management Process</strong></th>
<th>The functionality and repeatability of cybersecurity risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrated Risk Management Program</strong></td>
<td>The extent to which cybersecurity is considered in broader risk management decisions</td>
</tr>
</tbody>
</table>
| **External Participation** | The degree to which the organization:  
  • monitors and manages supply chain risk\(^1\)  
  • 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

What processes and assets need protection?
What safeguards are available?
What techniques can identify incidents?
What techniques can contain impacts of incidents?
What techniques can restore capabilities?

[Diagram with functions: Identify, Protect, Detect, Respond, Recover]
## Core
### A Catalog of Cybersecurity Outcomes

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identify</strong></td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td><strong>Protect</strong></td>
<td>Identity Management, Authentication and Access Control</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes &amp; Procedures</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
</tr>
<tr>
<td><strong>Detect</strong></td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
</tr>
<tr>
<td><strong>Respond</strong></td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
</tr>
<tr>
<td><strong>Recover</strong></td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>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>
<tbody>
<tr>
<td>IDENTIFY</td>
<td>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.</td>
<td><strong>ID.SC-1:</strong> Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ID.SC-2:</strong> Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process</td>
<td>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</td>
</tr>
</tbody>
</table>
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

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>108</td>
</tr>
</tbody>
</table>

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

• **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
### 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></td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>moderate</td>
<td>medium</td>
<td>$</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>moderate</td>
<td>none</td>
<td>$$</td>
<td></td>
<td>reassess</td>
</tr>
</tbody>
</table>
Resource and Budget Decisioning
Framework supports operating decisions and improvement

<table>
<thead>
<tr>
<th>Sub-category</th>
<th>Priority</th>
<th>Gaps</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>
</tr>
<tr>
<td>2</td>
<td>high</td>
<td>large</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>moderate</td>
<td>medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>moderate</td>
<td>none</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step 5
Target Profile

Step 6

Step 7

As-Is

Year 1 To-Be

Year 2 To-Be

---

15
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

- Internal
- Supply Chain

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

Framework Profiles

Implementation Progress
Changes in Assets, Vulnerability and Threat
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
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)*
Proposed U.S. Federal Usage

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

Level 1
Org

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

Level 2
Mission/Business Processes

8. Inform the tailoring process
   supports RMF Select

Level 3
System

Core
Profile(s)
Imp. Tiers
Profile(s)
Core
Profile(s)
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.
Resources
https://www.nist.gov/cyberframework/framework-resources-0

Over 150 Unique Resources for Your Understanding and Use!

General Resources sorted by User Group:
- Critical Infrastructure
- Small and Medium Business
- International
- Federal
- State Local Tribal Territorial Governments
- Academia
- Assessments & Auditing
- General
Resources
https://www.nist.gov/cyberframework/framework-resources-0

Over 150 Unique Resources for Your Understanding and Use!

NIST Special Publications
Computer Security Resource Center
800 Series @ csrc.nist.gov

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

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>800-84</td>
<td>Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities</td>
</tr>
<tr>
<td>800-181</td>
<td>National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework</td>
</tr>
<tr>
<td>800-50</td>
<td>Building an Information Technology Security Awareness and Training Program</td>
</tr>
<tr>
<td>800-16</td>
<td>A Role-Based Model for Federal Information Technology/Cybersecurity Training</td>
</tr>
<tr>
<td>800-114</td>
<td>User’s Guide to Telework and Bring Your Own Device (BYOD) Security</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>800-133</td>
<td>Recommendation for Cryptographic Key Generation</td>
</tr>
<tr>
<td>800-111</td>
<td>Guide to Storage Encryption Technologies for End User Devices</td>
</tr>
<tr>
<td>800-89</td>
<td>Recommendation for Obtaining Assurances for Digital Signature Applications</td>
</tr>
</tbody>
</table>
Online Informative References
https://www.nist.gov/cyberframework/informative-references

Events and Presentations

Related Efforts (Roadmap)

Informative References

Resources +

Newsroom +

Credit: N. H
## Core – Example 1.1

**Cybersecurity Framework Component**

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTECT (PR)</td>
<td><strong>Identity Management, Authentication and Access Control (PR.AC):</strong> 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.</td>
</tr>
</tbody>
</table>
| **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions | **Informative References:**
| &nbsp; | CIS CSC, 16
| &nbsp; | COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03
| &nbsp; | 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
| &nbsp; | ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1
| &nbsp; | ISO/IEC 27001:2013 A.7.1.1, A.9.2.1
| &nbsp; | 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) | **Informative References:**
| &nbsp; | CIS CSC 1, 12, 15, 16
| &nbsp; | COBIT 5 DSS05.04, DSS05.10, DSS06.10
| &nbsp; | 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
| &nbsp; | 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
| &nbsp; | 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 |
## 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>
Milestones

Three Year Minimum Update Cycle

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

New Version?
3 years from last Final Update

Features List (Version A)
Major
Minor
Administrative

Features List (Version B)
Major
Minor
Administrative

Features List (Version C)
Major
Minor
Administrative

Draft Framework Update

Publish Framework Update

Annual Conference

Annual Conference

Annual Conference

Annual Conference
## 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

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

• Questions, comments, ideas:
  • cyberframework@nist.gov