Framework for Improving Critical Infrastructure Cybersecurity

12 November 2015

cyberframework@nist.gov
“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”

President Barack Obama
Executive Order 13636, 12 February 2013
Cybersecurity Framework Components

- **Framework Profile**: Aligns industry standards and best practices to the Framework Core in a particular implementation scenario. Supports prioritization and measurement while factoring in business needs.

- **Framework Core**: Cybersecurity activities and informative references, organized around particular outcomes. Enables communication of cyber risk across an organization.

- **Framework Implementation Tiers**: Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics.
Implementation Tiers
Cybersecurity Framework Component

- Allow for flexibility in implementation and bring in concepts of maturity models
- Reflect how an organization implements the Framework Core functions and manages its risk
- Progressive, ranging from Partial (Tier 1) to Adaptive (Tier 4), with each Tier building on the previous Tier
- Characteristics are defined at the organizational level and are applied to the Framework Core to determine how a category is implemented.
## Framework Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>What processes and assets need protection?</td>
<td>IDENTIFY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What safeguards are available?</td>
<td>PROTECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What techniques can identify incidents?</td>
<td>DETECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What techniques can contain impacts of incidents?</td>
<td>RESPOND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What techniques can restore capabilities?</td>
<td>RECOVER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Core

### Cybersecurity Framework Component

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Asset Management</td>
<td>ID.AM</td>
</tr>
<tr>
<td>Identify</td>
<td>Business Environment</td>
<td>ID.BE</td>
</tr>
<tr>
<td>Identify</td>
<td>Governance</td>
<td>ID.GV</td>
</tr>
<tr>
<td>Identify</td>
<td>Risk Assessment</td>
<td>ID.RA</td>
</tr>
<tr>
<td>Identify</td>
<td>Risk Management Strategy</td>
<td>ID.RM</td>
</tr>
<tr>
<td>Protect</td>
<td>Access Control</td>
<td>PR.AC</td>
</tr>
<tr>
<td>Protect</td>
<td>Awareness and Training</td>
<td>PR.AT</td>
</tr>
<tr>
<td>Protect</td>
<td>Data Security</td>
<td>PR.DS</td>
</tr>
<tr>
<td>Protect</td>
<td>Information Protection Processes &amp; Procedures</td>
<td>PR.IP</td>
</tr>
<tr>
<td>Protect</td>
<td>Maintenance</td>
<td>PR.MA</td>
</tr>
<tr>
<td>Protect</td>
<td>Protective Technology</td>
<td>PR.PT</td>
</tr>
<tr>
<td>Detect</td>
<td>Anomalies and Events</td>
<td>DE.AE</td>
</tr>
<tr>
<td>Detect</td>
<td>Security Continuous Monitoring</td>
<td>DE.CM</td>
</tr>
<tr>
<td>Detect</td>
<td>Detection Processes</td>
<td>DE.DP</td>
</tr>
<tr>
<td>Respond</td>
<td>Response Planning</td>
<td>RS.RP</td>
</tr>
<tr>
<td>Respond</td>
<td>Communications</td>
<td>RS.CO</td>
</tr>
<tr>
<td>Respond</td>
<td>Analysis</td>
<td>RS.AN</td>
</tr>
<tr>
<td>Respond</td>
<td>Mitigation</td>
<td>RS.MI</td>
</tr>
<tr>
<td>Respond</td>
<td>Improvements</td>
<td>RS.IM</td>
</tr>
<tr>
<td>Recover</td>
<td>Recovery Planning</td>
<td>RC.RP</td>
</tr>
<tr>
<td>Recover</td>
<td>Improvements</td>
<td>RC.IM</td>
</tr>
<tr>
<td>Recover</td>
<td>Communications</td>
<td>RC.CO</td>
</tr>
</tbody>
</table>

### Subcategory

| ID.BE-1: | The organization’s role in the supply chain is identified and communicated |
| ID.BE-2: | The organization’s place in critical infrastructure and its industry sector is identified and communicated |
| ID.BE-3: | Priorities for organizational mission, objectives, and activities are established and communicated |
| ID.BE-4: | Dependencies and critical functions for delivery of critical services are established |
| ID.BE-5: | Resilience requirements to support delivery of critical services are established |

### Informative References

- COBIT 5 APO01.02, DSS06.03
- ISA 62443-2-1:2009 4.3.2.3.3
- ISO/IEC 27001:2013 A.6.1.1
- NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
- COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05
- ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2
- NIST SP 800-53 Rev. 4 CP-2, SA-12
- COBIT 5 APO02.06, APO03.01
- NIST SP 800-53 Rev. 4 PM-8
- NIST SP 800-53 Rev. 4 PM-11, SA-14
- NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
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
Building a Profile

A Profile Can be Created in Three Steps

1. **Mission**
   
<table>
<thead>
<tr>
<th>Priority</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>B</td>
</tr>
<tr>
<td>3</td>
<td>C</td>
</tr>
</tbody>
</table>

2. **Subcategory**
   
   | 1       |
   | 2       |
   | 3       |
   | ...     |
   | 98      |

3. **Operating Methodologies**
   
   Guidance and methodology on implementing, managing, and monitoring

---

**Cybersecurity Requirements**

- Legislation
- Regulation
- Internal & External Policy
- Best Practice

---
## Conceptual Profile

### Value Proposition

<table>
<thead>
<tr>
<th>2</th>
<th>Cybersecurity Requirements</th>
<th>Subcategory</th>
<th>1</th>
<th>Priority</th>
<th>3</th>
<th>Operating Methodologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>1</td>
<td>moderate</td>
<td>I</td>
<td>II</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>2</td>
<td>high</td>
<td>III</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td>3</td>
<td>moderate</td>
<td>IV</td>
<td>V</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
<td>...</td>
<td>...</td>
<td>VI</td>
<td>VII</td>
<td></td>
</tr>
<tr>
<td>G</td>
<td></td>
<td>98</td>
<td>moderate</td>
<td>VIII</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When you organize yourself in this way:

- Compliance reporting becomes a byproduct of running your security operation
- Adding new security requirements is straightforward
- Adding or changing operational methodology is non-intrusive to on-going operation
## Resource and Budget Decisioning

*What Can You Do with a CSF Profile*

<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>X</td>
</tr>
<tr>
<td>2</td>
<td>high</td>
<td>large</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>moderate</td>
<td>medium</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>moderate</td>
<td>none</td>
<td></td>
<td>reassess</td>
</tr>
</tbody>
</table>

...and supports on-going operational decisions too
Key Attributes

• **It’s a framework, not a prescription**
  • It provides a common language and systematic methodology for managing cyber risk
  • It is meant to be adapted
  • It does not tell a company *how* much cyber risk is tolerable, nor does it claim to provide “the one and only” formula for cybersecurity
  • Having a common lexicon to enable action across a very diverse set of stakeholders will enable the best practices of elite companies to become standard practices for everyone

• **The framework is a living document**
  • It is intended to be updated over time as stakeholders learn from implementation, and as technology and risks change
  • That’s one reason why the framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, and standards will change over time—principals will not
Industry Use

The Framework is designed to complement existing business and cybersecurity operations, and has been used to:

• Self-Assessment, Gap Analysis, Budget & Resourcing Decisions
• Standardizing Communication Between Business Units
• Harmonize Security Operations with Audit
• Communicate Requirements with Partners and Suppliers
• Describe Applicability of Products and Services
• Identify Opportunities for New or Revised Standards
• Categorize College Course Catalogs
• As a Part of Cybersecurity Certifications
• Categorize and Organize Requests for Proposal Responses
• Consistent dialog, both within and amongst countries
• Common platform on which to innovate, by identifying market opportunities where tools and capabilities may not exist today
Collect, Reflect, and Connect – understand where industry is having success, help others understand those successes, and facilitate relationships that support use and implementation

- Continue education efforts, including creation of self-help and re-use materials for those who are new to the Framework

- Continue awareness and outreach with an eye toward industry communities who are still working toward basal Framework knowledge and implementation

- Educate on the relationship between Framework and the larger risk management process, including how organizations can use Tiers
On-Going NIST Community Dialogs

- Domestic Industry
  - Not only Critical Infrastructure, but also Non-CI
  - Product and Services
- Standards Organizations
  - British Standards Institute, Cloud Security Alliance, AXELOS, etc.
- Regulator
  - Every Federal Financial Services regulator
- Auditor
  - Information Systems Audit and Control Association
  - “The Big 4” Audit Firms
- Insurance
- Legal
Since the Release of the Cybersecurity Framework...

Request for Information: Experience with the Cybersecurity Framework
Questions focused on: awareness, experiences, and roadmap areas
August 26, 2014

6th Cybersecurity Framework Workshop
Goal: Raise awareness, encourage use as a tool, highlight examples of sector-specific efforts, implementation efforts, gather feedback
Oct. 29-30, 2014
Florida Center for Cybersecurity

Update on the Cybersecurity Framework
Summary posted that includes analysis of RFI responses, feedback from the 6th workshop, an update on Roadmap areas, and next steps
December 5, 2014

February 13, 2015
White House Releases
Fact Sheet on Cybersecurity and Consumer Protection

1 Year Anniversary of the Release
NIST Cybersecurity Framework site update to include: FAQs, Upcoming Events, and Industry Resources. Ongoing, targeted outreach continues
February 12, 2015
Examples of Industry Resources

The Cybersecurity Framework in Action: An Intel Use Case

Cybersecurity Guidance for Small Firms

Energy Sector Cybersecurity Framework Implementation Guidance


CFORUM and other online communities of interest
Examples of State & Local 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
Framework Roadmap Items

Authentication
Automated Indicator Sharing
Conformity Assessment
Cybersecurity Workforce
Data Analytics
Federal Agency Cybersecurity Alignment
International Aspects, Impacts, and Alignment
Supply Chain Risk Management
Technical Privacy Standards
Standards/Guidelines for FISMA & RM

**FIPS - Federal Information Processing Standards**
- FIPS 199 – Standards for Security Categorization
- FIPS 200 – Minimum Security Requirements

**SPs – Special Publications**
- SP 800-18 – Guide for System Security Plan development
- SP 800-30 – Guide for Conducting Risk Assessments
- SP 800-34 – Guide for Contingency Plan development
- SP 800-37 – Guide for Applying the Risk Management Framework
- SP 800-39 – Managing Information Security Risk
- SP 800-53/53A – Security controls catalog/assessment procedures
- SP 800-60 – Mapping Information Types to Security Categories
- SP 800-128 – Security-focused Configuration Management
- SP 800-137 – Information Security Continuous Monitoring
- Many others for operational and technical implementations
Organizing and Communicating Security Controls
Use Case for Risk Management Framework & Cybersecurity Framework

SP 800-53 security controls
CobIT controls
ISO 27002 controls
Etc...
Supporting the RMF Categorize Step

Profile
A sector, subsector, or organization’s customization of the Core for their purposes. Aligns conflicts in organizational inputs, and cyber objectives commensurate with mission objectives.

Category
Business Environment (ID.BE)
The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Tailoring SP 800-53 Security Controls

Use Case for Risk Management Framework & Cybersecurity Framework

Tailoring Guidance

- Identifying and Designating Common Controls
- Applying Scoping Considerations
- Selecting Compensating Controls
- Assigning Security Control Parameter Values
- Supplementing Baseline Security Controls
- Providing Additional Specification Information for Implementation

Creating Overlays

Assessment of Organizational Risk

DOCUMENT SECURITY CONTROL DECISIONS

Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.
Building a Notional Profile

A Profile Can be Created in Three Steps

1. **Mission**
   - Priority | Objective |
   - 1        | A         |
   - 2        | B         |
   - 3        | C         |

2. **Cybersecurity Requirements**
   - Legislation
   - Regulation
   - Internal & External Policy
   - Best Practice

3. **Operating Methodologies**
   - Guidance and methodology on implementing, managing, and monitoring
## Applicability to FedRAMP and CDM

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>ID</th>
<th>Cloud</th>
<th>Continuous Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identify</strong></td>
<td>Asset Management</td>
<td>ID.AM</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
<td>ID.BE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>ID.GV</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
<td>ID.RA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
<td>ID.RM</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Protect</strong></td>
<td>Access Control</td>
<td>PR.AC</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
<td>PR.AT</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
<td>PR.DS</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes &amp; Procedures</td>
<td>PR.IP</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>PR.MA</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td>PR.PT</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Detect</strong></td>
<td>Anomalies and Events</td>
<td>DE.AE</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
<td>DE.CM</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>DE.DP</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Respond</strong></td>
<td>Response Planning</td>
<td>RS.RP</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RS.CO</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
<td>RS.AN</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>RS.MI</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RS.IM</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Recover</strong></td>
<td>Recovery Planning</td>
<td>RC.RP</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RC.IM</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RC.CO</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Industry Dialog

Will it soon be time for a Framework update?

What governance models do you believe will work for future Framework maintenance and evolution?
The National Institute of Standards and Technology Web site is available at http://www.nist.gov


The Framework for Improving Critical Infrastructure Cybersecurity and related news and information are available at www.nist.gov/cyberframework

For additional Framework info and help cyberframework@nist.gov