Cybersecurity Framework

Executive Order 13636
“Improving Critical Infrastructure Cybersecurity”
National Institute of Standards and Technology (NIST)
Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology ...

... in ways that enhance economic security and improve our quality of life.
Executive Order 13636—Improving Critical Infrastructure Cybersecurity

“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”

- NIST is directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure

- This Cybersecurity Framework is being developed in an open manner with input from stakeholders in industry, academia, and government, including a public review and comment process, workshops, and other means of engagement.
The Cybersecurity Framework

For the Cybersecurity Framework to meet the requirements of the Executive Order, it must:

• include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

• provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

• identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations able technical innovation and account for organizational differences include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.
Development of the Preliminary Cybersecurity Framework

EO 13636 Issued – February 12, 2013
NIST Issues RFI – February 26, 2013
1st Framework Workshop – April 03, 2013
Completed – April 08, 2013

Identify Common Practices/Themes – May 15, 2013
2nd Framework Workshop at CMU – May 29-31, 2013

Draft Outline of Preliminary Framework – June 2013
3rd Framework Workshop at UCSD – July 10-12, 2013

Publish Preliminary Framework – October 29, 2013

Ongoing Engagement:
Open public comment and review encouraged and promoted throughout the process
Includes a Note to Reviewers with questions for readers to consider and a comment template

Preliminary Cybersecurity Framework

- Framework Introduction
- Framework Basics
- How to Use the Framework
- Appendix A: Framework Core
- Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program
- Appendix C: Areas for Improvement for the Cybersecurity Framework
- Appendix D: Framework Development Methodology
- Appendix E: Glossary
- Appendix F: Acronyms

The Preliminary Cybersecurity Framework was posted in the Federal Register for a 45-day public comment period through December 13, 2013.

http://www.nist.gov/itl/cyberframework.cfm
Questions for Reviewers to Consider

Does the Preliminary Framework:

• adequately define outcomes that strengthen cybersecurity and support business objectives?
• enable cost-effective implementation?
• appropriately integrate cybersecurity risk into business risk?
• provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?
• provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?
• provide the right level of specificity and guidance for mitigating the impact of cybersecurity measures on privacy and civil liberties?
• express existing practices in a manner that allows for effective use?

Will the Preliminary Framework, as presented:

• be inclusive of, and not disruptive to, effective cybersecurity practices in use today?
• enable organizations to incorporate threat information?

Is the Preliminary Framework:

• presented at the right level of specificity?
• sufficiently clear on how the privacy and civil liberties methodology is integrated with the Framework Core?
Risk Management and the Cybersecurity Framework

- Cybersecurity risk management approaches that take into account the interaction of multiple risk disciplines;

- Cybersecurity risk management approaches that address both traditional information technology and operational technology (industrial control systems);

- Cybersecurity risk management practices that encompass the entire organization, exposing dependencies that often exist within large, mature, and/or diverse entities, and with the interaction between the entities and their partners, vendors, suppliers, and others;

- Cybersecurity risk management practices that are internalized by the organization to ensure that decision making is conducted by a risk-informed process of continuous improvement; and

- Cybersecurity standards that can be used to support risk management activities
Framework Components

Framework Core

• Cybersecurity activities and references that are common across critical infrastructure sectors and organized around particular outcomes.
• Enables communication of cybersecurity risk across the organization.

Framework Profile

• Alignment of industry standards and best practices to the Framework Core in a particular implementation scenario.
• Supports prioritization and measurement of progress, while factoring in other business needs including cost-effectiveness and innovation.

Framework Implementation Tiers

• Describe how cybersecurity risk is managed by an organization.
• Describe the degree to which an organization’s cybersecurity risk management practices exhibit general characteristics (e.g., risk and threat aware, repeatable, and adaptive).
• Partial (Tier 1), Risk-Informed (Tier 2), Risk-Informed and Repeatable (Tier 3), Adaptive (Tier 4).
Framework Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Framework Core: Functions

The five Framework Core Functions provide the highest level of structure:

- **Identify** – Develop the institutional understanding of which organizational systems, assets, data, and capabilities need to be protected, determine priority in light of organizational mission, and establish processes to achieve risk management goals.

- **Protect** – Develop and implement the appropriate safeguards, prioritized through the organization’s risk management process, to ensure delivery of critical infrastructure services.

- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

- **Respond** – Develop and implement the appropriate activities, prioritized through the organization’s risk management process (including effective planning), to take action regarding a detected cybersecurity event.

- **Recover** - Develop and implement the appropriate activities, prioritized through the organization’s risk management process, to restore the appropriate capabilities that were impaired through a cybersecurity event.
Framework Core: Categories

- **Categories** are the subdivisions of a Function into groups of cybersecurity activities, more closely tied to programmatic needs.

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

- **Subcategories** further subdivide a Category into high-level tactical activities to support technical implementation.

- **Informative References** are specific sections of standards and practices common among critical infrastructure sectors and illustrate a method to accomplish the activities within each Subcategory.

- The Informative References presented in the Framework Core are not exhaustive, and organizations are free to implement other standards, guidelines, and practices.
### The Framework Core

<table>
<thead>
<tr>
<th>Function and Unique Identifier</th>
<th>Category and Unique Identifier</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| **IDENTIFY** (ID)             | Asset Management (AM): Identify and manage the personnel, devices, systems, and facilities that enable the organization to achieve business purposes, including their relative importance to business objectives, in support of effective risk decisions. | ID.AM: Physical devices and systems within the organization are inventoried | - ISA 99.02.01 4.2.3.4  
- COBIT BA03.04, BA09.01, BA09.05  
- ISO/IEC 27001 A.7.1.1, A.7.1.2  
- NIST SP 800-53 Rev. 4 CM-8 CSC1 |
| **PROTECT** (PR)              | Awareness and Training (AT): Ensure that organizational personnel and partners are adequately trained to carry out their assigned information security-related duties and responsibilities through awareness and training activities. | PRAT: General users are informed and trained | - ISA 99.02.01 4.3.2.4.2  
- COBIT APO07.03, BA07.07  
- ISO/IEC 27001 A.8.2.2  
- NIST SP 800-53 Rev. 4 AT-2  
- CCS CSC 9 |
| **DETECT** (DE)               | Detection Processes (DP): Ensure timely and adequate awareness of anomalous events through tested and implemented detection processes and procedures. | DE.DP: Roles and responsibilities for detection are well defined to ensure accountability | - ISA 99.02.01 4.4.3.1  
- COBIT DSS05.01  
- NIST SP 800-53 Rev. 4 IR-2, IR-4, IR-8  
- CCS CSC 5 |
| **RESPOND** (RS)              | Mitigation (MI): Conduct activities to prevent expansion of an event, mitigate its effects, and eradicate the incident. | RS.MI: Incidents are contained | - ISO/IEC 27001 A.3.6, A.13.2.3  
- ISA 99.02.01 4.3.1.5.6  
- NIST SP 800-53 Rev. 4 IR-4 |
| **RECOVER** (RC)              | Recovery Planning (RP): Execute Recovery Plan activities to achieve restoration of services or functions. | RC.RP: Recovery plan is executed | - COBIT DSS02.05, DSS03.04  
Framework Profile

- Enables organizations to establish a roadmap to reducing cybersecurity risk
- Can be used to describe current state and desired target state of specific cybersecurity activities
- Created by determining which Categories are relevant to a particular organization, sector, or other entity
- An organization’s risk management processes, legal / regulatory requirements, business / mission objectives, and organizational constraints guide the selection of activities during Profile development

**Table:**

<table>
<thead>
<tr>
<th>Category/Subcategory</th>
<th>Target Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Gap Identification:**

<table>
<thead>
<tr>
<th>Category/Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Framework Implementation Tiers

- Feedback indicated the need for the Framework to allow for flexibility in implementation.

- Responding to feedback, Framework Implementation Tiers were proposed to reflect how an organization manages its cybersecurity risk.

- The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is integrated into an organization’s overall risk management practices.

How to Use the Framework

The Framework can be used by organizations looking to:

• Establish or Improve a Cybersecurity Program
  Step 1: Identify
  Step 2: Establish a Current Profile
  Step 3: Conduct a Risk Assessment
  Step 4: Establish a Target Profile
  Step 5: Determine, Analyze, and Prioritize Gaps
  Step 6: Implement Action Plan

• Communicate Cybersecurity Requirements with Stakeholders

• Identify Gaps
Methodology to Protect Privacy and Civil Liberties

- The EO directs NIST to include a methodology to identify and mitigate impacts of the Framework and associated security measures to protect individual privacy and civil liberties.

- Appendix B presents a Privacy methodology that is coordinated with the Framework Core. This methodology provides organizations with flexibility in determining how to manage privacy risk.
  - Organized by Function and Category to correspond with the Framework Core.
  - Every Category may not be represented as not all Categories give rise to privacy and civil liberties risks.
  - Includes Informative References

- This methodology is based on the Fair Information Practice Principles (FIPPs) referenced in the EO, and is designed to complement existing processes organizations may have in place.
Areas for Improvement for the Cybersecurity Framework

Executive Order 13636 states that the Cybersecurity Framework will “identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations”. Based on stakeholder input, several high-priority areas for future development have been identified. Collaboration and cooperation must increase for these areas to further understanding and/or the development of new or revised standards.

- Authentication
- Automated Indicator Sharing
- Conformity Assessment
- Cybersecurity Workforce
- Data Analytics
- International Aspects, Impacts, and Alignment
- Privacy Standards
- Supply Chains and Interdependencies
Getting from the Preliminary Framework to the Final Framework and Beyond

- Prepare and Publish Preliminary Framework
  - Publish Preliminary Framework – October 29, 2013
  - Begin 45 day Public Comment Period

- Additional Ongoing Public Engagement
  - Stakeholder outreach discussion continue

- Public Comment Period
  - Public comment period closes – December 13, 2013

- Final Cybersecurity Framework
  - Complete comment resolution and disposition
  - Publish Cybersecurity Framework (v1.0) – February 2014

- Framework Evolution
  - Framework maintenance and transition to industry
  - Collaboration on Areas for Development

Ongoing Engagement:
Open public comment and review encouraged and promoted throughout the process
Thank You

The Preliminary Cybersecurity Framework and supporting material is available at http://www.nist.gov/itl/cyberframework.cfm

Comments on the Preliminary Cybersecurity Framework are due no later than 5pm EST on December 13, 2013.

Electronic comments concerning the preliminary Framework should be submitted to: csfcomments@nist.gov, with the Subject line: Preliminary Cybersecurity Framework Comments