The Framework for Improving Critical Infrastructure Cybersecurity

Matthew Barrett

September 2018

cyberframework@nist.gov
International Use
Framework for Improving Critical Infrastructure Cybersecurity
## Core

A Catalog of Cybersecurity Outcomes

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Understandable by everyone</td>
</tr>
<tr>
<td>Protect</td>
<td>Applies to any type of risk management</td>
</tr>
<tr>
<td>Detect</td>
<td>Defines the entire breadth of cybersecurity</td>
</tr>
<tr>
<td>Respond</td>
<td>Spans both prevention and reaction</td>
</tr>
<tr>
<td>Recover</td>
<td></td>
</tr>
</tbody>
</table>

- Understand risks
- Determine safeguards
- Identify events
- Address incidents
- Restore capabilities
## Core

A Catalog of Cybersecurity Outcomes

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
</table>
| **Identify** | Asset Management  
Business Environment  
Governance  
Risk Assessment  
Risk Management Strategy  
Supply Chain Risk Management |
| **Protect** | Identity Management, Authentication and Access Control  
Awareness and Training  
Data Security  
Information Protection Processes & Procedures  
Maintenance  
Protective Technology |
| **Detect** | Anomalies and Events  
Security Continuous Monitoring  
Detection Processes |
| **Respond** | Response Planning  
Communications  
Analysis  
Mitigation  
Improvements |
| **Recover** | Recovery Planning  
Improvements  
Communications |
# 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><strong>PROTECT</strong></td>
<td><strong>Data Security (PR.DS):</strong> Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</td>
<td><strong>PR.DS-1:</strong> Data-at-rest is protected</td>
<td><strong>CIS CSC</strong> 13, 14&lt;br&gt;<strong>COBIT 5</strong> APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06&lt;br&gt;<strong>ISA 62443-3-3:2013</strong> SR 3.4, SR 4.1&lt;br&gt;<strong>ISO/IEC 27001:2013</strong> A.8.2.3&lt;br&gt;<strong>NIST SP 800-53 Rev. 4</strong> MP-8, SC-12, SC-28</td>
</tr>
<tr>
<td><strong>PR.DS-2:</strong> Data-in-transit is protected</td>
<td><strong>CIS CSC</strong> 13, 14&lt;br&gt;<strong>COBIT 5</strong> APO01.06, DSS05.02, DSS06.06&lt;br&gt;<strong>ISA 62443-3-3:2013</strong> SR 3.1, SR 3.8, SR 4.1, SR 4.2&lt;br&gt;<strong>ISO/IEC 27001:2013</strong> A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3&lt;br&gt;<strong>NIST SP 800-53 Rev. 4</strong> SC-8, SC-11, SC-12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<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>
<td><strong>PR.AC-7:</strong> 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)</td>
<td><strong>CIS CSC</strong> 1, 12, 15, 16&lt;br&gt;<strong>COBIT 5</strong> DSS05.04, DSS05.10, DSS06.10&lt;br&gt;<strong>ISA 62443-2-1:2009</strong> 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</td>
<td></td>
</tr>
</tbody>
</table>
Sample Resources
www.nist.gov/cyberframework/industry-resources

Italy’s National Framework for Cybersecurity

American Water Works Association’s Process Control System Security Guidance for the Water Sector

The Cybersecurity Framework in Action: An Intel Use Case


Financial Services Sector Specific Cybersecurity “Profile”
Sample Resources
www.nist.gov/cyberframework/industry-resources

Manufacturing Profile
NIST Discrete Manufacturing Cybersecurity Framework Profile

Self-Assessment Criteria
Baldrige Cybersecurity Excellence Builder

Manufacturing Case Study
The Cybersecurity Framework in Action: An Intel Use Case
Learning More
Framework for Improving Critical Infrastructure Cybersecurity

News and information

www.nist.gov/cyberframework

Learn about the NIST Cybersecurity Risk Management Conference

Registration now open at

Additional cybersecurity resources through


National Cybersecurity Center of Excellence - http://nccoe.nist.gov/

Please direct questions, comments, ideas to cyberframework@nist.gov
"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

**Mailing Address:** NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

**Physical Address:** 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov