Framework for Improving Critical Infrastructure Cybersecurity

June 2018

cyberframework@nist.gov
Objective and Agenda

Objective: Convey Cybersecurity Framework use, explain the new version, and highlight some additional NIST resources

- NIST
- Healthcare Guidance
- Charter
- Users
- Component Overview
- Roadmap
- Resources
National Institute of Standards and Technology

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
Health Care Specific Guidance
Available at the Computer Security Resource Center

**Special Publication 800-66**: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

- An Overview of the Risk Management Framework (RMF)
- Using RMF to Apply Security Controls to Fulfill HIPAA Security Rule

**Special Publication 800-184**: Guide for Cybersecurity Event Recovery

- Sample Metrics
- Creating Recovery Plan: “Playbook”
  - Baselining Operations
  - Being Action Oriented
  - Testing Processes and Procedures
- Destructive Malware Example
  - Tactical Recovery
  - Strategic Recovery
Health Care Specific Guidance
Projects at the National Cybersecurity Center of Excellence

NIST Cybersecurity Practice Guide = cookbook
Multi-part, Multi-reader Document

**Special Publication 1800-1**: Securing Electronic Health Records on Mobile Devices
National Cybersecurity Center of Excellence

**Special Publication 1800-8**: Securing Wireless Infusion Pumps in Healthcare Delivery Organizations
National Cybersecurity Center of Excellence

Coming Soon: **Securing Picture Archiving and Communication System (PACS) Cybersecurity**
National Cybersecurity Center of Excellence
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 Use

Framework for Improving Critical Infrastructure Cybersecurity
Cybersecurity Framework Components

Cybersecurity outcomes and informative references

Ensures 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

Aligns industry standards and best practices to the Framework Core in an implementation scenario

Supports prioritization and measurement while factoring in business needs
Key Properties of Cyber Risk Management

Integrated Risk Management Program

Risk Management Process

External Participation
# 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 risk(^{1.1})</td>
</tr>
<tr>
<td></td>
<td>• benefits my sharing or receiving information from outside parties</td>
</tr>
</tbody>
</table>

\(^{1.1}\) This includes the consideration of supply chain risk as part of overall risk management practices.
Core
A Catalog of Cybersecurity Outcomes

What processes and assets need protection?
Identify

What safeguards are available?
Protect

What techniques can identify incidents?
Detect

What techniques can contain impacts of incidents?
Respond

What techniques can restore capabilities?
Recover

- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction
## 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 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 (ID)</td>
<td><strong>Supply Chain Risk Management (ID.SC):</strong> 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><strong>CIS CSC 4</strong>&lt;br&gt;<strong>COBIT 5</strong> APO10.01, APO10.04, APO12.04, APO12.07, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02&lt;br&gt;<strong>ISA 62443-2-1:2009</strong> 4.3.4.2&lt;br&gt;<strong>ISO/IEC 27001:2013</strong> A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2&lt;br&gt;<strong>NIST SP 800-53 Rev. 4</strong> SA-9, SA-12, PM-9</td>
</tr>
<tr>
<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></td>
<td><strong>COBIT 5</strong> APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03&lt;br&gt;<strong>ISA 62443-2-1:2009</strong> 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&lt;br&gt;<strong>ISO/IEC 27001:2013</strong> A.15.2.1, A.15.2.2&lt;br&gt;<strong>NIST SP 800-53 Rev. 4</strong> RA-2, RA-3, SA-12, SA-14, SA-15, PM-9</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>
| 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** |
### Core – Example

#### Cybersecurity Framework Component

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

Three Things All Cybersecurity Programs Must Do

• Support Mission/Business Objectives
• Fulfill Cybersecurity Requirements
• Manage Vulnerability and Threat Associated with the Technical Environment
Creating Target Profiles

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

<table>
<thead>
<tr>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>108</td>
</tr>
</tbody>
</table>
Framework Seven Step Process
Gap Analysis Using Framework Profiles

• **Step 1:** Prioritize and Scope
  • Implementation Tiers may be used to express varying risk tolerances\(^{1.1}\)

• **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\(^{1.1}\)

• **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>...</td>
<td>...</td>
<td>...</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>moderate</td>
<td>none</td>
<td>$$</td>
<td>reassess</td>
<td></td>
</tr>
</tbody>
</table>

Target Profile | Gap Analysis | Implementation
Operate
Use Cybersecurity Framework Profiles to Manage Cybersecurity

<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>
<tr>
<td>Reqs</td>
<td>Priorities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Organizing and monitoring work
- Distribution of authority and labor
- Empowering workforce
- Managing accountability
Supporting Risk Management with Framework
Framework for Improving Critical Infrastructure Cybersecurity

- Internal
- Supply Chain
Cyber SCRM Taxonomy\textsuperscript{1.1}

Framework for Improving Critical Infrastructure Cybersecurity

- 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

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
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\(^{1.1}\), lifecycle phases\(^{1.1}\), sectors and uses
• Meant to be customized

It’s risk-based
• A Catalog of cybersecurity outcomes
• Does 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
Roadmap Concepts

Roadmap for Improving Critical Infrastructure 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 9 topics</th>
<th>Proposed Roadmap 12 topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conformity Assessment</td>
<td>Confidence Mechanisms</td>
</tr>
<tr>
<td>Automated Indicator Sharing</td>
<td>Cyber-Attack Lifecycle</td>
</tr>
<tr>
<td>Data Analytics</td>
<td>Includes Coordinated Vulnerability Disclosure</td>
</tr>
<tr>
<td>Cybersecurity Workforce</td>
<td>Cybersecurity Workforce</td>
</tr>
<tr>
<td>Supply Chain Risk Management</td>
<td>Cyber Supply Chain Risk Management</td>
</tr>
<tr>
<td>Federal Agency Cybersecurity Alignment</td>
<td>Federal Agency Cybersecurity Alignment</td>
</tr>
<tr>
<td>Authentication</td>
<td>Identity Management</td>
</tr>
<tr>
<td>International Aspects, Impacts, and Alignment</td>
<td>International Aspects, Impacts, and Alignment</td>
</tr>
<tr>
<td>Technical Privacy Standards</td>
<td>Privacy Engineering</td>
</tr>
<tr>
<td></td>
<td>Referencing Techniques</td>
</tr>
<tr>
<td></td>
<td>Small Business Awareness and Resources</td>
</tr>
</tbody>
</table>
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.
There are many security frameworks, but we found that the Cybersecurity Framework was well-aligned with our main objective, which was to establish a common language for communicating cybersecurity risks across the Division,”
- Plamen Martinov, BSD CISO

Benefits Received from Implementing the Framework:
• **Aligned security risk expectations** across all 23 departments through a risk register aligned to the Cybersecurity Framework Subcategories
• Identified security requirements as a **common set of target outcomes**, while enabling departments to define the approach for achieving the outcome
• **Prioritized security goals** across the division within a resourced roadmap outlining gap closing activities
Resources
www.nist.gov/cyberframework/industry-resources

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
Examples of Framework Industry 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”
Recent NIST Work Products
www.nist.gov/cyberframework/industry-resources

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
Over 150 Unique Resources for Your Understanding and Use!

Resources

www.nist.gov/cyberframework/industry-resources

NIST Special Publications

Computer Security Resource Center
800 Series @ csirc.nist.gov

National Cybersecurity Center of Excellence
1800 Series @ ncceo.nist.gov
# NIST Special Publications by Category

www.nist.gov/cyberframework/industry-resources

<table>
<thead>
<tr>
<th>PROTECT (PR)</th>
<th>PROTECT (PR)</th>
<th>PROTECT (PR)</th>
<th>PROTECT (PR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>800-84</td>
<td>Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities <a href="#">↩</a></td>
<td>800-181</td>
</tr>
<tr>
<td></td>
<td>800-16</td>
<td>A Role-Based Model for Federal Information Technology/Cybersecurity Training <a href="#">↩</a></td>
<td>800-114</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. | 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 [↩](#) |
Small Business Guidance

- Understanding and Managing Risks
- Safeguarding Your Information
  - Provided According to Cybersecurity Framework “Functions”
- Working Safely and Securely
This document demonstrates how a cybersecurity framework can utilize current information security standards to achieve a well-controlled approach to cybersecurity management.

https://www.iso.org/standard/72437.html
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)
SP 800-37rev2 Discussion Draft Highlights

Special Publication 800-37 Revision 2 Discussion Draft

Security risks that arise from unauthorized system behavior

Privacy risks that arise from a by-product of authorized PII processing

SECURITY CONTROLS

PRIVACY CONTROLS
### Upcoming for Framework

<table>
<thead>
<tr>
<th>Summer 2018</th>
<th>Publication of <em>Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>Summer 2018</td>
<td>Spanish Language Translation of the <em>Framework for Improving Critical Infrastructure Cybersecurity Version 1.1</em></td>
</tr>
<tr>
<td>7-9 November 2018</td>
<td><a href="#">NIST Cybersecurity Risk Management Conference</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Registration</a> Now Open</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Call for Speakers</a> through 31 July 2018</td>
</tr>
<tr>
<td>Winter 2018-19</td>
<td>Small Business Starter Profiles</td>
</tr>
</tbody>
</table>
Resources & Next Steps

• Consider Using or Extending Your Use of Cybersecurity Framework
  • Perspectives to inform you decision to use
  • Online Learning to understand more
  • Resources and Success Stories to learn how others use
• Share your use via Resources or at the NIST Cybersecurity Risk Management conference
• Communicate with NIST via cyberframework@nist.gov
• Review other NIST health resources
  • Computer Security Resource Center
  • National Cybersecurity Center of Excellence
Thoughts and Questions?