NIST 101

Tools and Resources for Small Network Operators

May 8, 2019
www.ntca.org/cybersecurity

About Jesse

- Director of Industry & Policy Analysis for NTCA
- 14 years with the association
- Focused on cybersecurity policy
- Represent interests of small network providers
- Participate in working groups
  - NTCA’s Cybersecurity Working Group
  - FCC’s CSRIC advisory council
  - DHS ICT Supply Chain Risk Management (SCRM) Task Force
  - Communications Sector Coordinating Council (CSCC)
  - Communications Information Sharing and Analysis Center (ISAC)

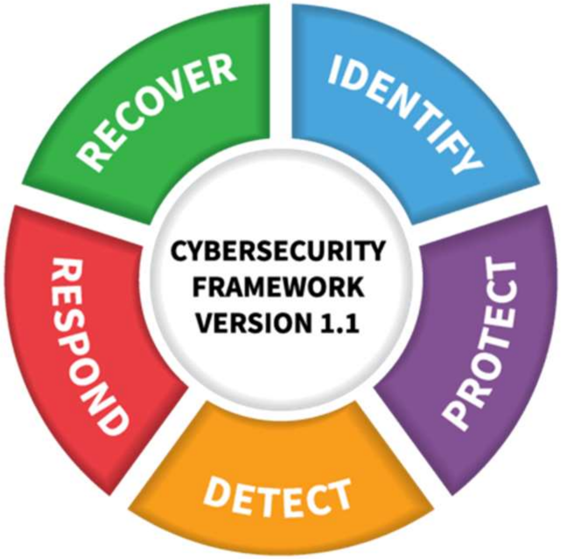
NIST 101

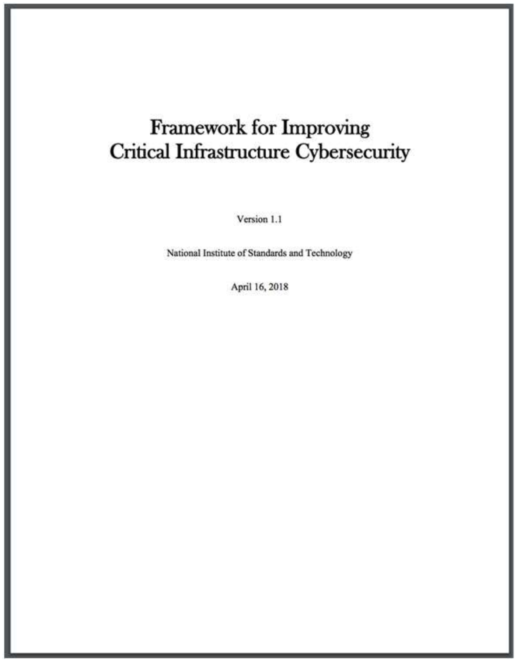
NTCA THE RURAL BROADBAND ASSOCIATION

NIST

National Institute of Standards and Technology
U.S. Department of Commerce

- To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology
- Non-partisan
- Maintains UTC, the U.S. national standard for time-of-day, time interval, and frequency
- Cybersecurity: Standards; Framework; Center of Excellence





Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

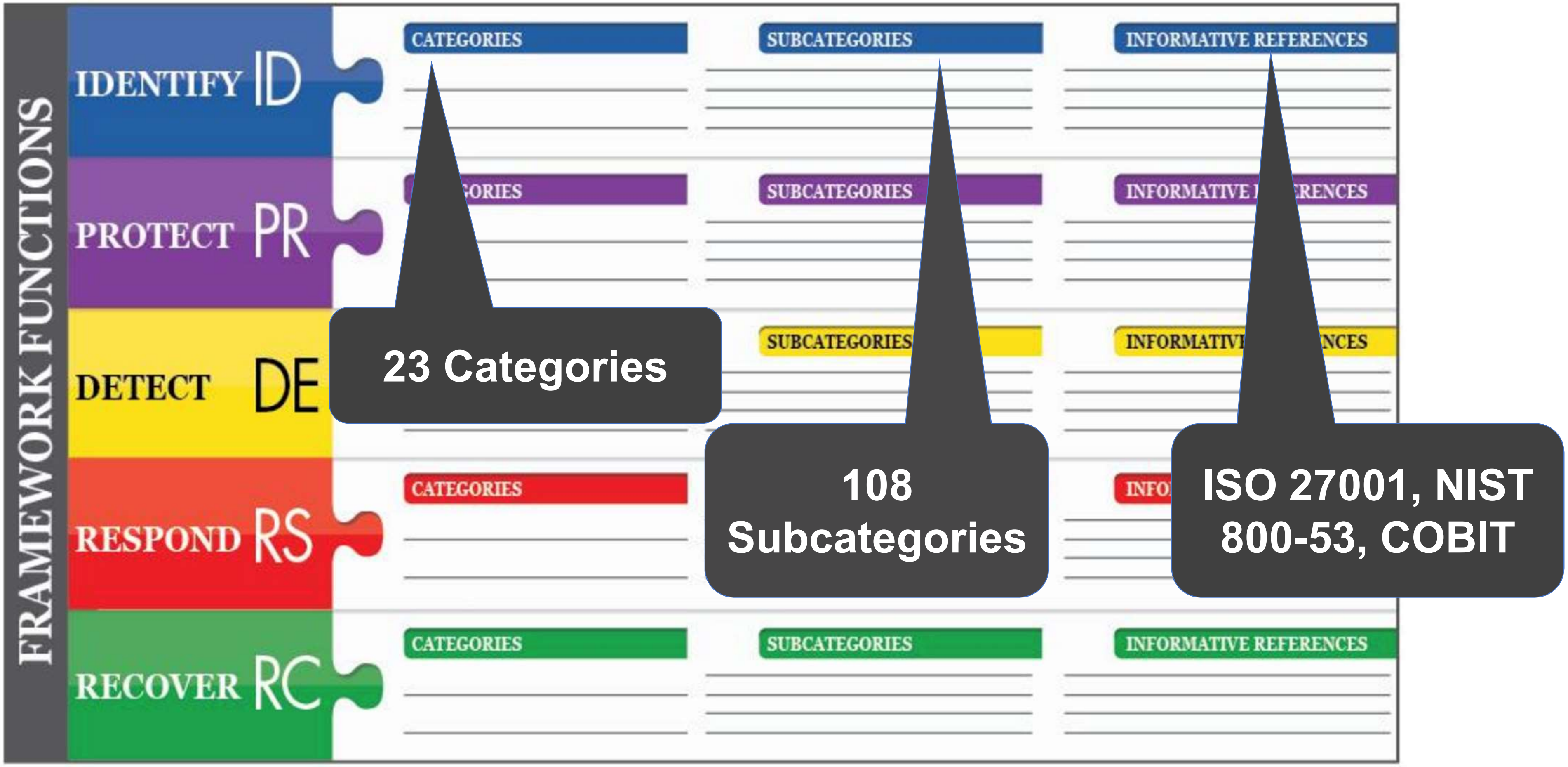
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Cybersecurity Framework 1.1

Evolution of the Framework

- Backwards compatible; Roadmap for future evolution
- Version 1.1:
  - authentication and identity;
  - supply chain;
  - vulnerability disclosure;
  - self-assessment
- Policymakers doubling down on Framework approach
- Focus on metrics

Framework 1.1 Core Structure

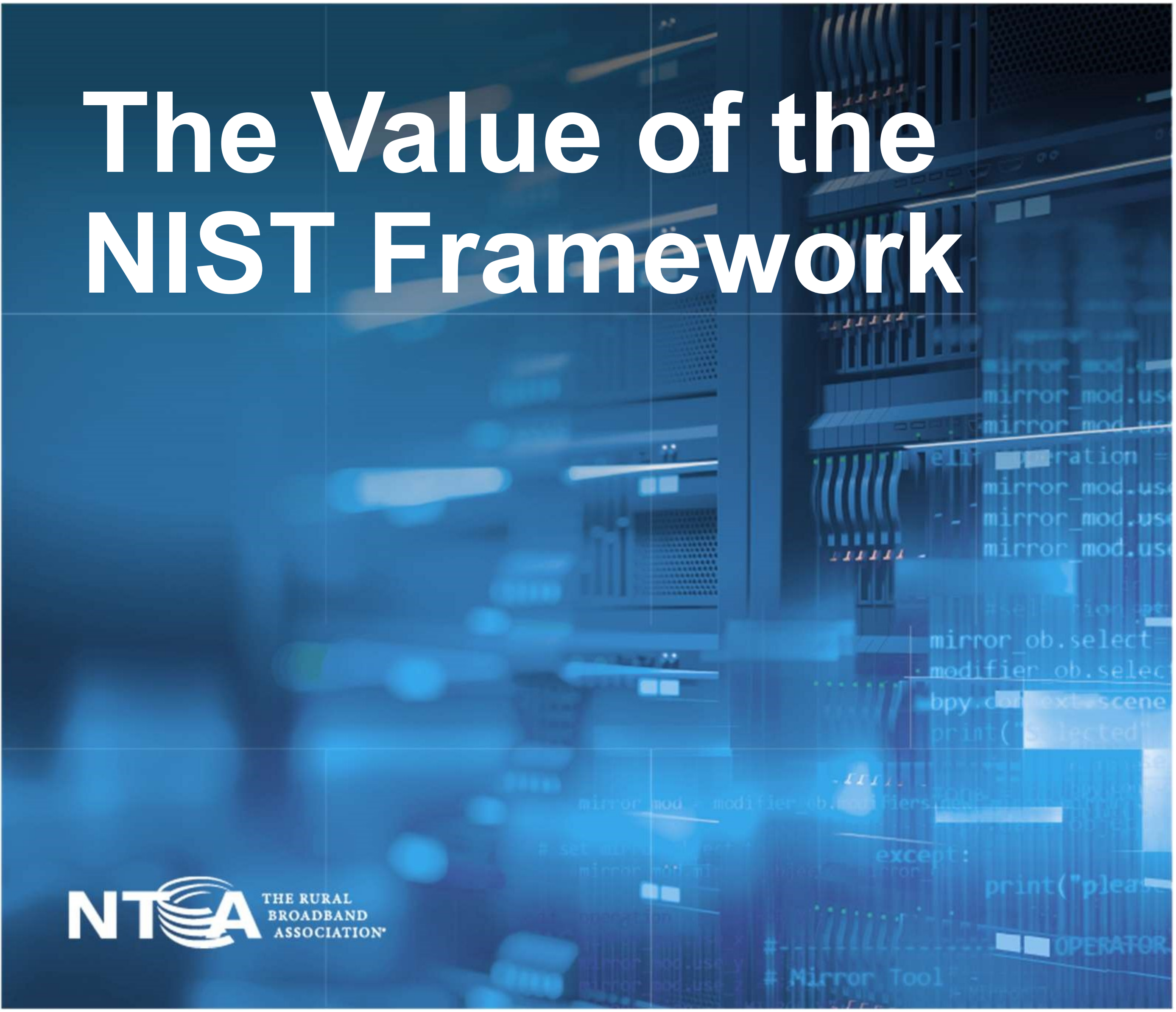


23 Categories

108 Subcategories

ISO 27001, NIST 800-53, COBIT

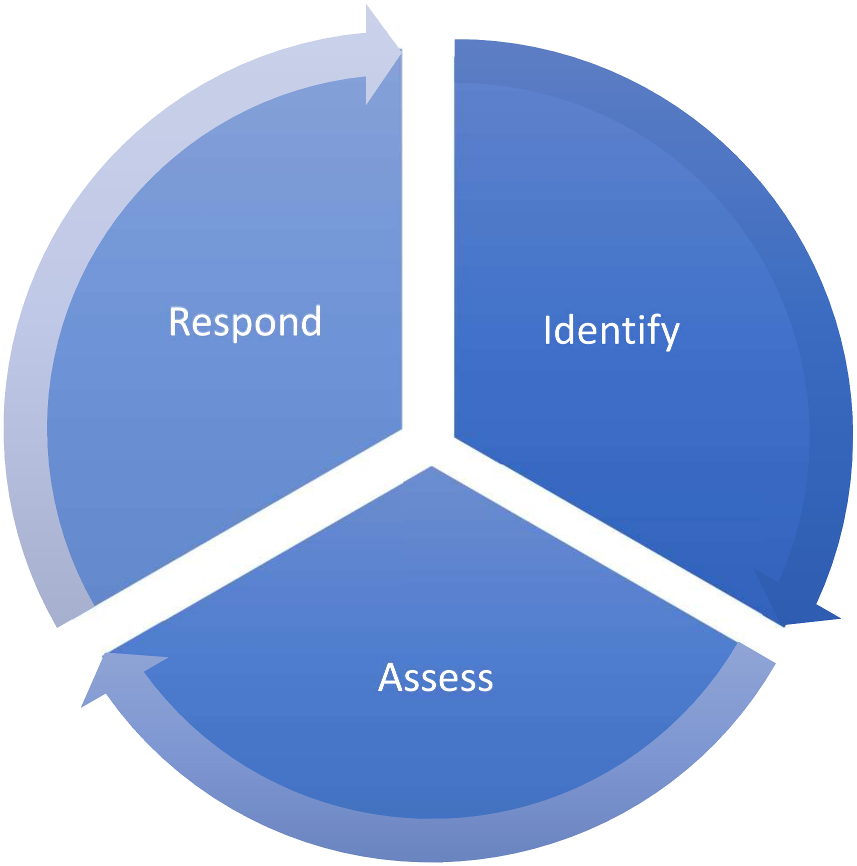
Figure 1: Framework Core Structure



The Value of the NIST Framework

NTCA THE RURAL BROADBAND ASSOCIATION

Risk-Management Process



You cannot eliminate all risk.

Rather, the goal is to understand security risks, and then reduce those risks to an acceptable level.

“Risk Tolerance”

Risk Management Approach

- Flexible & dynamic
- Company-wide approach
- Governed by senior execs
- Strives for ongoing improvement

NTCA THE RURAL BROADBAND ASSOCIATION®

THE GOOD THE BAD AND THE UGLY

Resources

THE RURAL BROADBAND ASSOCIATION

Sector-Specific Guide

NTCA Cybersecurity Bundle

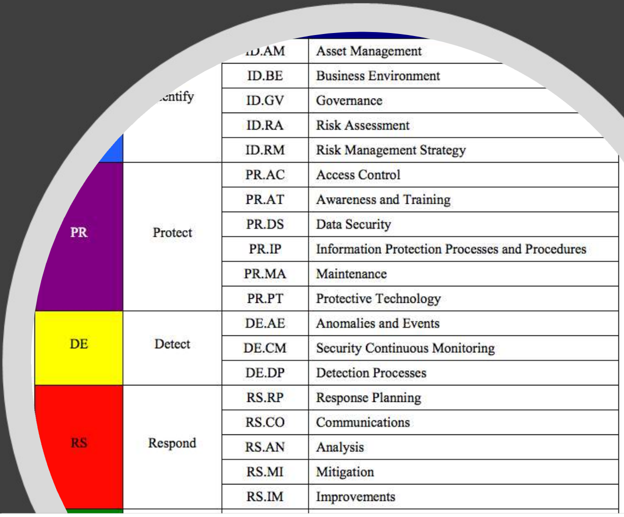
Sector-Specific Guide

“The magnitude of the framework can be both **intimidating** for a smaller business and, due to resource limitations, **functionally impossible** to implement **all at once**. As such, the **NTCA Member Advisory Group** offers the following **implementation guidance** for **small network operators**.”

- Operational guidance, drafted by NTCA members
- Illustrative and flexible; not a prescriptive checklist
- Focus on “core network” and “critical infrastructure and services”

Sector Guide: Framework Analysis

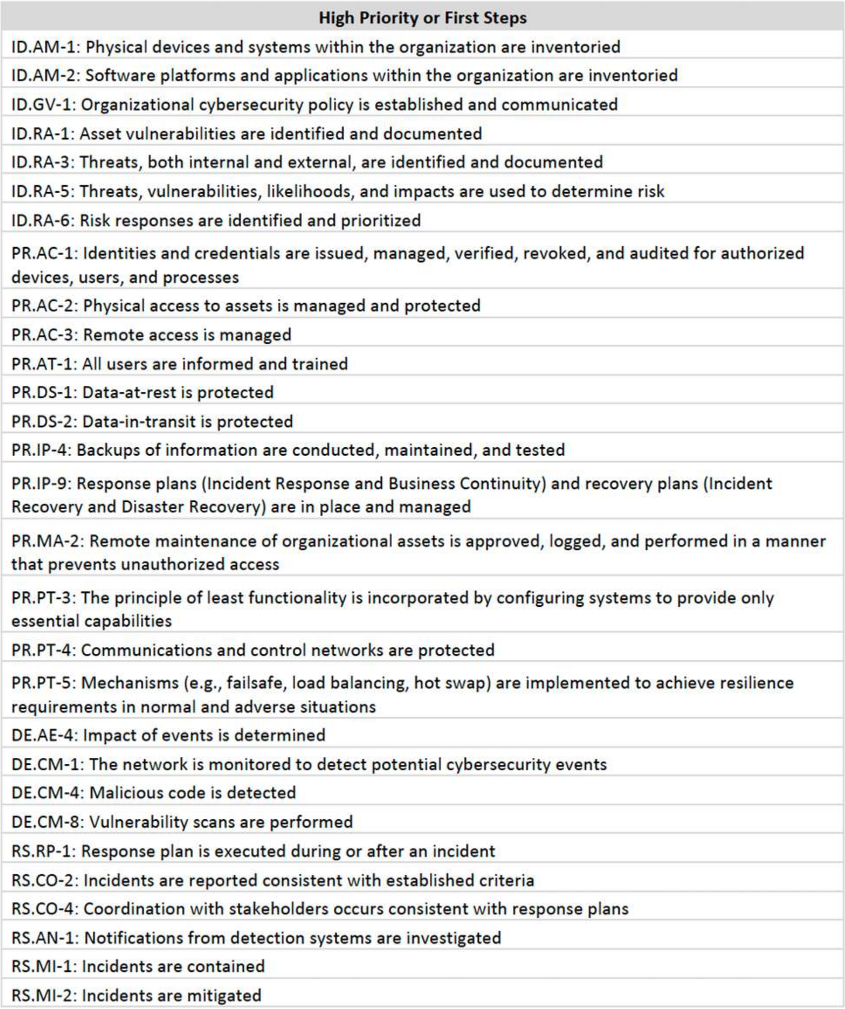
- In or Out of Scope
- Criticality (1-5)
- Application to Operating Environment
- Barriers to Implementation



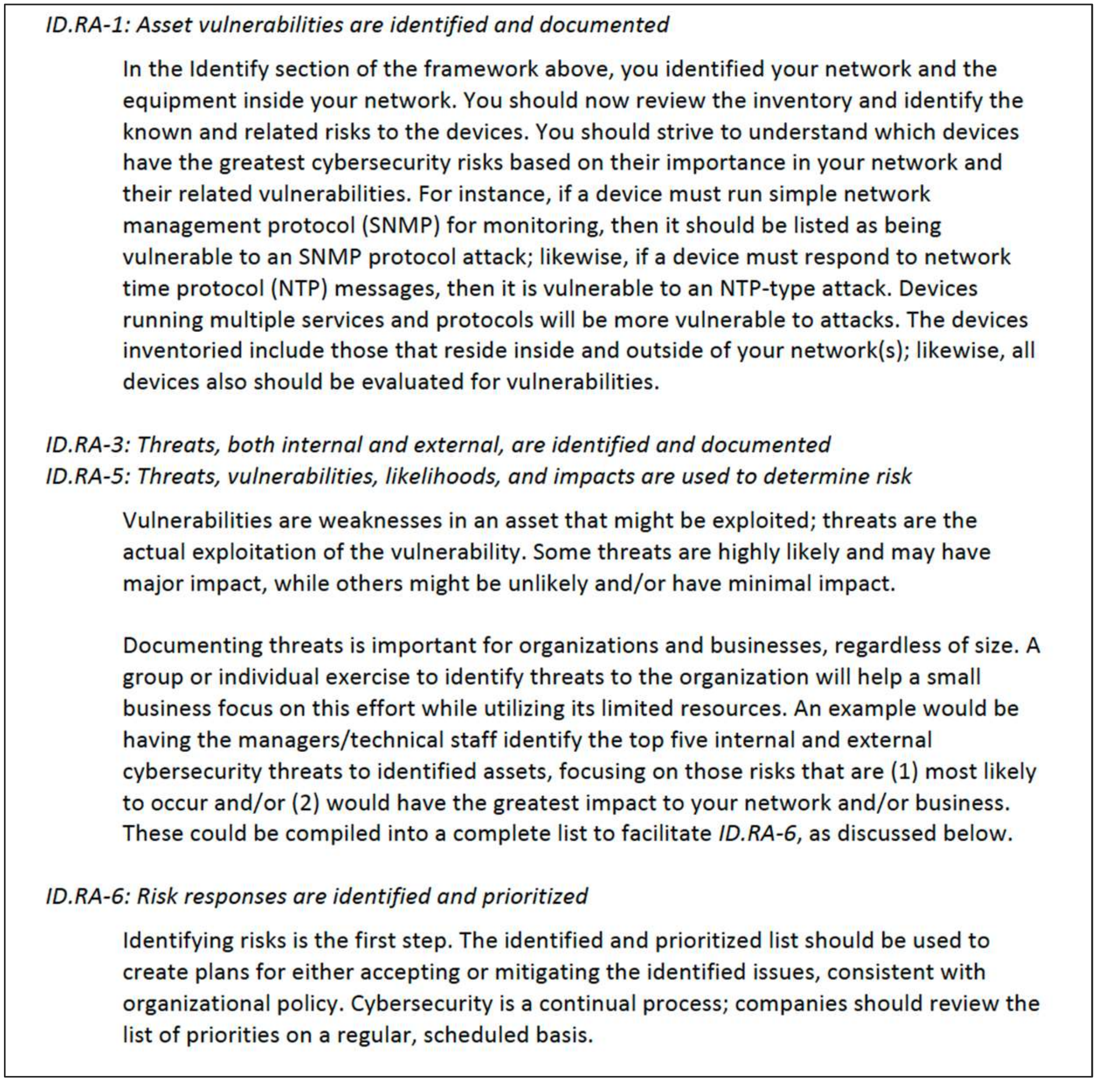
	entify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements

Sector Guide:

Priority Practices



High Priority or First Steps
ID.AM-1: Physical devices and systems within the organization are inventoried
ID.AM-2: Software platforms and applications within the organization are inventoried
ID.GV-1: Organizational cybersecurity policy is established and communicated
ID.RA-1: Asset vulnerabilities are identified and documented
ID.RA-3: Threats, both internal and external, are identified and documented
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
ID.RA-6: Risk responses are identified and prioritized
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes
PR.AC-2: Physical access to assets is managed and protected
PR.AC-3: Remote access is managed
PR.AT-1: All users are informed and trained
PR.DS-1: Data-at-rest is protected
PR.DS-2: Data-in-transit is protected
PR.IP-4: Backups of information are conducted, maintained, and tested
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
PR.PT-4: Communications and control networks are protected
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
DE.AE-4: Impact of events is determined
DE.CM-1: The network is monitored to detect potential cybersecurity events
DE.CM-4: Malicious code is detected
DE.CM-8: Vulnerability scans are performed
RS.RP-1: Response plan is executed during or after an incident
RS.CO-2: Incidents are reported consistent with established criteria
RS.CO-4: Coordination with stakeholders occurs consistent with response plans
RS.AN-1: Notifications from detection systems are investigated
RS.MI-1: Incidents are contained
RS.MI-2: Incidents are mitigated



ID.RA-1: Asset vulnerabilities are identified and documented

In the Identify section of the framework above, you identified your network and the equipment inside your network. You should now review the inventory and identify the known and related risks to the devices. You should strive to understand which devices have the greatest cybersecurity risks based on their importance in your network and their related vulnerabilities. For instance, if a device must run simple network management protocol (SNMP) for monitoring, then it should be listed as being vulnerable to an SNMP protocol attack; likewise, if a device must respond to network time protocol (NTP) messages, then it is vulnerable to an NTP-type attack. Devices running multiple services and protocols will be more vulnerable to attacks. The devices inventoried include those that reside inside and outside of your network(s); likewise, all devices also should be evaluated for vulnerabilities.

ID.RA-3: Threats, both internal and external, are identified and documented
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

Vulnerabilities are weaknesses in an asset that might be exploited; threats are the actual exploitation of the vulnerability. Some threats are highly likely and may have major impact, while others might be unlikely and/or have minimal impact.

Documenting threats is important for organizations and businesses, regardless of size. A group or individual exercise to identify threats to the organization will help a small business focus on this effort while utilizing its limited resources. An example would be having the managers/technical staff identify the top five internal and external cybersecurity threats to identified assets, focusing on those risks that are (1) most likely to occur and/or (2) would have the greatest impact to your network and/or business. These could be compiled into a complete list to facilitate *ID.RA-6*, as discussed below.

ID.RA-6: Risk responses are identified and prioritized

Identifying risks is the first step. The identified and prioritized list should be used to create plans for either accepting or mitigating the identified issues, consistent with organizational policy. Cybersecurity is a continual process; companies should review the list of priorities on a regular, scheduled basis.

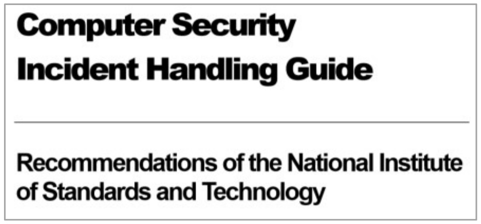
Sector Guide:

Case Study

Sector Guide:
Tools and Resources

- Best practices
- Planning guides/templates
- Tools
- Training
- Standards

SNORT®



Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

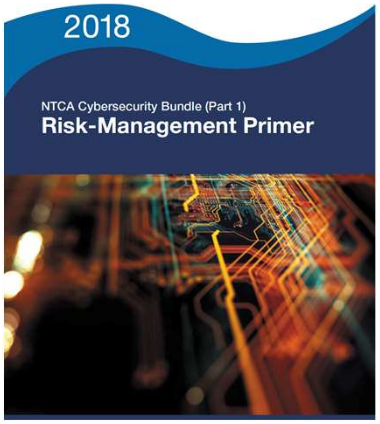
TEXAS A&M ENGINEERING TEEX EXTENSION SERVICE

NATIONAL EMERGENCY RESPONSE AND RESCUE TRAINING CENTER

CDI CYBERTERRORISM DEFENSE INITIATIVE FEMA

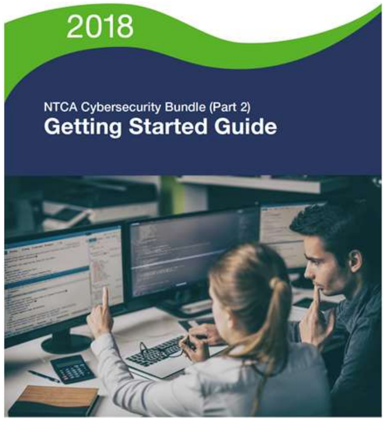
Free Cyberterrorism Training

2018 NTCA Cybersecurity Bundle


2018

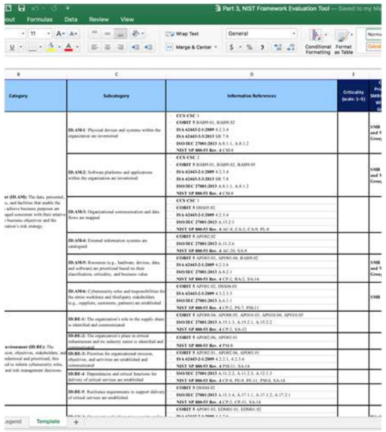
NTCA Cybersecurity Bundle (Part 1)

Risk-Management Primer

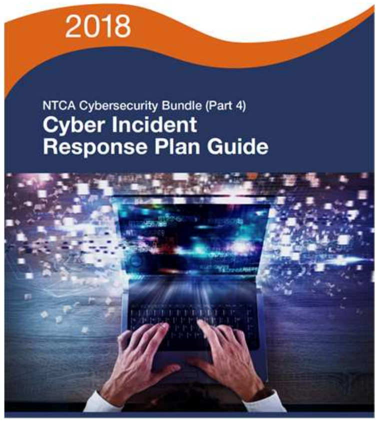

2018

NTCA Cybersecurity Bundle (Part 2)

Getting Started Guide

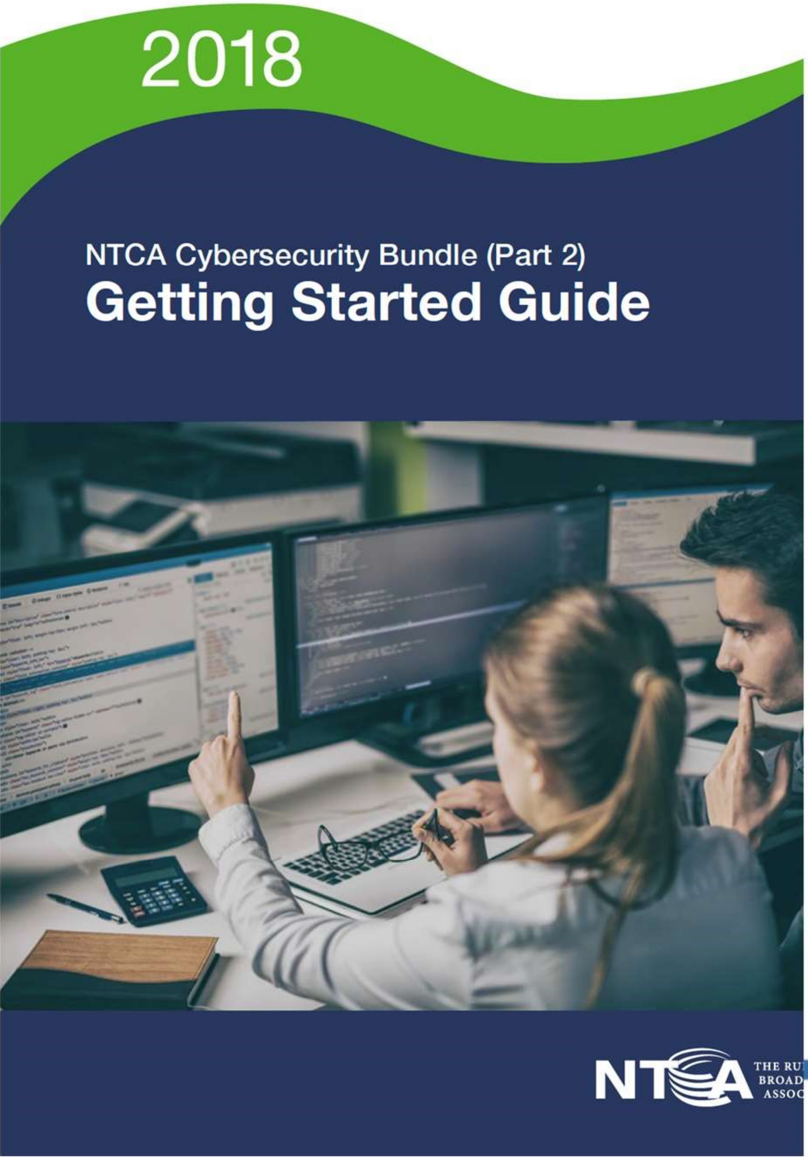


Category	Subcategory	Informative References	Criticality (scale: 1-5)	Pri SMB W G
t (ID.AM): The data, personnel, s, and facilities that enable the achieve business purposes are aged consistent with their relative business objectives and the ation's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8		SMB and V Grou
	ID.AM-2: Software platforms and applications within the organization are inventoried	CCS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8		SMB and V Grou
	ID.AM-3: Organizational communication and data flows are mapped	CCS CSC 1 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8		
	ID.AM-4: External information systems are catalogued	COBIT 5 APO02.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9		
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	COBIT 5 APO03.03, APO03.04, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14		SMB and V Grou
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	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		SMB
vironment (ID.BE): The sion, objectives, stakeholders, and nderstood and prioritized; this d to inform cybersecurity roles, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated	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		
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8		
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14		
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14		
	ID.BE-5: Resilience requirements to support delivery of critical services are established	COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14		
		COBIT 5 APO01.03, EDM01.01, EDM01.02		


2018

NTCA Cybersecurity Bundle (Part 4)

Cyber Incident Response Plan Guide



2018

NTCA Cybersecurity Bundle (Part 2)

Getting Started Guide

- “On-ramp” to using the NIST Framework
- Based upon NTCA member best practices
- Encourages robust internal discussion
- Define cyber risk-management team
- Meeting agendas, topics, and questions informed by 5 cybersecurity functions and most critical subcategories from Sector-Specific Guide

Questions?

Save-the-Date:
NTCA 2019 Cybersecurity Summit
Oct 27-29, Salt Lake City, UT

Jesse Ward
jward@ntca.org
703-351-2007