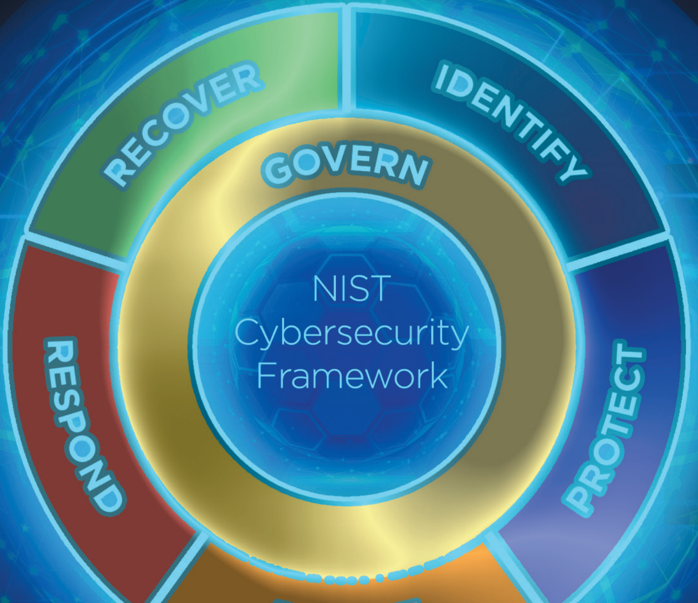
NTCA CYBERSECURITY SERIES

(Part 2)

Sector-Specific Guidance to the NIST Cybersecurity Framework



NTCA THE RURAL BROADBAND ASSOCIATION®

#BeCyberwise

NTCA CYBERSECURITY SERIES

(Part 2)

Sector-Specific Implementation Guidance for the NIST Cybersecurity Framework

Published March 2024

4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
703-351-2000
www.ntca.org

Disclaimer: The National Telecommunications Cooperative Association d/b/a NTCA–The Rural Broadband Association ("NTCA") is offering the NTCA Cybersecurity Series and/or its individual components for general information purposes only, and nothing contained herein constitutes legal advice or opinions of any kind. You use these documents at your own risk, and you should not use any of these documents without first seeking legal and other professional advice. NTCA makes no representations or warranties, express or implied, with respect to the Cybersecurity Series, including without limitation any warranties of fitness for a particular purpose. NTCA and its affiliates (and any of their respective directors, officers, agents, contractors, interns, suppliers and employees) are not responsible for, and expressly disclaim, all liability for, damages of any kind arising out of use, reference to or reliance of any information contained within the Cybersecurity Series. Although the Cybersecurity Series may include links providing direct access to internet resources, including websites, NTCA is not responsible for the accuracy or content of information contained in these sites.

Table of Contents

Introduction

In 2016, NTCA introduced its Cybersecurity Bundle, which consisted of educational components designed to help broadband executives, board officers and operational staff develop a risk-management approach to cybersecurity. Since its introduction, we've added and updated the resources to create the "NTCA Cybersecurity Series," which includes this "Sector-Specific Guidance to the National Institute of Standards and Technology (NIST) Cybersecurity Framework" as a resource for your cyber risk management team to consider. The NIST Cybersecurity Framework (CSF, or Framework), first released in 2014, updated in 2018 and again in 2024, is a voluntary framework based on existing standards, guidelines and practices for reducing cyber risks to critical infrastructure. Despite the voluntary nature of the Framework, some federal agencies have begun requiring companies to implement cybersecurity and supply chain risk management plans that incorporate the Framework as a condition to receiving federal funding.

Given the dynamic and evolving nature of cyberthreats, cybersecurity resilience is best approached from a risk/ benefit analysis. The CSF helps accommodate your environment, risk tolerance and unique needs while also helping you to identify, assess and prioritize the greatest risks to your business. The Framework then helps you determine where and how best to apply resources to minimize the probability and/or impact of cybersecurity events. In August 2023, NIST released a draft of CSF 2.0, a major refresh of the Framework, to reflect changes in technologies and cybersecurity risk management since 2018.

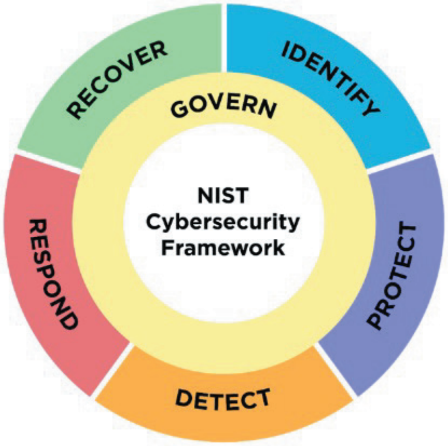


Fig. 2. Framework Functions

Most notably, CSF 2.0 adds a new Core Function, "Govern," that informs how organizations will implement each of the other five Core Functions that comprised Versions 1.0 and 1.1: Identify, Protect, Detect, Respond and Recover.

Additionally, the Recover Core Function was bolstered substantially, with a new subcategory that addresses recommendations for the effective execution of a recovery plan following an incident.

The Framework now provides six "functions" that all organizations, regardless of size, can use to evaluate and enhance the maturity of their cybersecurity programs:

- Govern: Establish and monitor the organization's cybersecurity risk management strategy, expectations and policy.
- Identify: Develop an organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
- Protect: Develop and implement appropriate safeguards to ensure the delivery of critical services.
- Detect: Develop and implement the capability to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber incident.

Within each function, the Framework provides more granular guidance via specific "categories" and "subcategories." The new Govern function includes a category focused on cyber supply chain risk management, recommending that processes be identified, established, managed, monitored and improved by organizational stakeholders.

The following report explains, in basic terms, how to interpret the NIST Cybersecurity Framework. It provides illustrative examples of how to apply the Framework to protect your core network and critical infrastructure. The guidance provided within this report is designed for a small network service provider that is seeking to undertake a more formalized and structured risk-management approach to address cybersecurity. However, each company should evaluate and apply the Framework based upon its unique needs and operational environment.

OBJECTIVE, SCOPE AND METHODOLOGY

OBJECTIVE

This report strives to provide overall guidance on how small network service providers can digest and apply Version 2.0 of the NIST Cybersecurity Framework to their operations, while simultaneously providing flexibility for individual companies to suit their unique needs, characteristics and risks (i.e., there is no one-size-fits-all approach to cybersecurity risk management).

SCOPE

For purposes of this document, a small network service provider is a facilities-based network service provider that operates a wireline, wireless and/or video network with fewer than 1,500 employees and/or fewer than 50,000 subscribers. However, this information is merely provided as a quantitative guide; whether a network service provider is defined as "small" is a nuanced decision, based upon multiple intricate factors and best left to the discretion of the individual business. Most importantly, the guidance offered within this report can be used by any telecommunications operator, or organization for that matter, that finds it useful.

As it looks to self-classify with respect to size, an individual business may consider the following:

- The resources and/or assets that a "small" business would have at its disposal to evaluate the recommended Framework best practices, including financial resources, the time required for the task and a company's access to internal and external expertise.
- The role of a "small" business in the supply chain, i.e., its purchasing power.
- Its dependencies on outside consultants, partners, vendors and systems, and the quantity/importance of those relationships.
- The total number of customers served.
- The business drivers for security, i.e., the unique needs of the company's or organization's customers.
- If a cyber incident should occur, its resultant impact upon the company's regional or local area.

Readers may also question how to apply the Framework to their companies, i.e., whether the Framework should be applied to corporate, IT or varied telecom access networks. Consistent with the spirit of the Framework, and the guidance provided by the Communications Security, Reliability and Interoperability Council IV Working Group 4 (CSRIC IV WG4) convened in April of 2014, small network service providers should start by applying the Framework to "core network" and "critical infrastructure and services." For example, a small network operator should maintain service to its core switch so that emergency services may maintain connectivity, including public safety answering points (PSAPs) or 911 call centers, police, fire, hospitals and other critical anchor institutions. In addition to core switches and routers, a small telecom operator should prioritize its transport network as a critical infrastructure component. For additional guidance on how to define "core network and critical infrastructure and services," see page 23.

METHODOLOGY

An NTCA Member Advisory Group consisting of individuals from small communications providers responsible for overseeing their company's cyber initiatives evaluated the subcategories included within the NIST Cybersecurity Framework. The group discussed whether each subcategory was in or out of scope; its criticality to protecting a small network operator's core network and/or critical infrastructure from cyber threats; how it should or could be applied within the operating environment of a small network provider; and potential barriers to implementation.

Based upon this qualitative analysis, NTCA prioritized the Framework subcategories into three phases:

PHASE ONE – Initial and Continuous Planning and Governance Priorities

PHASE TWO – Primary Operational Priorities

PHASE THREE – Longer Term Operational and Governance Priorities

These profiles offer a small network provider implementation guidance and strategy as it relates to Framework best practices. However, the NTCA Member Advisory Group urges caution as the terms "phase" and "priority" may be incorrectly viewed as prescriptive and restrictive; once again, the NIST Cybersecurity Framework, and the related guidance offered within this report, are designed to be flexible and dynamic to meet your company's unique security needs.

Phase One, Initial and Continuous Planning and Governance Priorities, included below, contains 35 subcategories or best practices from the Framework. This may be a useful starting point for a small network operator that is seeking to undertake a more formalized and structured risk management approach to protect its core network and critical infrastructure and services from cyber threats. Phase Two contains 48 subcategories, while Phase Three contains 23 best practices.

In addition to the profile listings, the NTCA Member Advisory Group developed a case study of practical implementation steps that offers additional "how-to" guidance for small network service providers with respect to implementation of the best practices contained within Phase One.

The guidance offered within this report should be taken as a whole and is for illustrative purposes only. The recommendations provided herein should not be boiled down to a prescriptive, inclusive list that predefines which Framework subcategories apply to all small network operators within the communications sector. Rather, consistent with the NIST Cybersecurity Framework, which provides for flexibility, each company should examine its network, core business objectives/ mission, risk tolerance and security needs to determine which subcategories included in Version 2.0 of the Framework are most applicable to its operational environment and security needs.

GUIDANCE TO IMPLEMENT THE NIST CYBERSECURITY FRAMEWORK

IMPLEMENTATION RECOMMENDATIONS

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, NTCA offers the following implementation guidance for small network operators.

Small network service providers should avoid a checklist approach to security. The cybersecurity risk landscape is constantly evolving. As attack methods change and new threats emerge, a static checklist methodology is not an effective defense as it confines the tactics by which an organization can prepare for and respond to imminent threats. Rather, a more fluid and dynamic risk-management approach is needed. Small network service providers should revise their cybersecurity practices with respect to a risk management maturity model, consistent with the Framework and the guidance provided in this document. In addition, small operators should remember to approach cybersecurity risk management as a process and strive for continual improvement.

Reevaluate your security needs, current status, target state and related priorities on a recurring basis with an eye toward process maturity.

The below chart cross-references to the subcategories in the previous version in the Framework and highlights the changes according to this chart.

Green	Entries remained substantively the same
Orange	Modified entries/significant consolidations or disassociations
Blue	New entries

PHASE 1- Initial and Continuous Planning and Governance Priorities

ID.AM-01: Inventories of hardware managed by the organization are maintained
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained
ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained (formerly ID.AM-03, DE.AE-01)
ID.AM-04: Inventories of services provided by suppliers are maintained
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission
ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained
ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded (Formerly ID.RA-01, PR.IP-12, DE.CM-08)
ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources
ID.RA-03: Internal and external threats to the organization are identified and recorded
ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization
ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated (formerly ID.RA-06, RS.MI-03)

ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established (formerly RS.AN-05)
ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)
ID.RA-10: Critical suppliers are assessed prior to acquisition
ID.RA-10: Critical suppliers are assessed prior to acquisition
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated (Formerly ID.BE-04, ID.BE-05)
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated (Formerly ID.BE-01, ID.BE-04)
GV.RM-01: Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (Formerly ID.RM-01)
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained (Formerly ID.RM-01, ID.RM-03)
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes (Formerly ID.GV-04)
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (Formerly ID.RM-01)
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally (Formerly ID.AM-06)
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (Formerly ID.SC-02)
GV.SC-04: Suppliers are known and prioritized by criticality
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (Formerly ID.SC-03)
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced (Formerly ID.AM-06, ID.GV-02, DE.DP-01)
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced (Formerly ID.GV-01)

PHASE 2 - Primary Operational Priorities

PR.AA-01: Identities and credentials for authorized users, services and hardware are managed by the organization (Formerly PR.AC-01)
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions (Formerly PR.AC-06)
PR.AA-03: Users, services and hardware are authenticated (Formerly PR.AC-03, PR.AC-07)
PR.AA-04: Identity assertions are protected, conveyed and verified
PR.AA-05: Access permissions, entitlements and authorizations are defined in a policy, managed, enforced and reviewed, and incorporate the principles of least privilege and separation of duties (Formerly PR.AC-01, PR.AC-03, PR.AC-04)
PR.AA-06: Physical access to assets is managed, monitored and enforced commensurate with risk (Formerly PR.AC-02, PR.PT-04)
PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind (Formerly PR.AT-01, PR.AT-03, RS.CO-01)
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind (Formerly PR.AT-02, PR.AT-03, PR.AT-03, PR.PT-02)
PR.DS-01: The confidentiality, integrity and availability of data-at-rest are protected (Formerly PR.DS-01, PR-DS.05, PR.DS-05, PR.AT-02)
PR.DS-02: The confidentiality, integrity and availability of data-in-transit are protected (FormerlyPR.DS-01, PR.DS-05, PR.DS-06, PR. PT-02)
PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected (Formerly PR. DS-05)
PR.DS-11: Backups of data are created, protected, maintained and tested (Formerly PR.IP-04)
PR.PS-04: Log records are generated and made available for continuous monitoring (Formerly PR.PT-01)
PR.PS-05: Installation and execution of unauthorized software are prevented
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage (Formerly PR.AC-03, PR.AC-05, PR.DS-07, PR.PT-04)
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (Formerl;y PR.PT-05)
DE.CM-01: Networks and network services are monitored to find potentially adverse events (Formerly DE.CM-01, DE.CM-04, DC.CM-05, DC.CM-07)
DE.CM-02: The physical environment is monitored to find potentially adverse events
DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events (Formerly DE.CM-03, DC.CM-07)
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events (Formerly DE.CM-01, DE.CM-04, DE.CM-05, DE.CM-07)
DE.CM-09: Computing hardware and software, runtime environments and their data are monitored to find potentially adverse events (Formerly PR.DS-06, PR.DS-08, DE.CM-04, DE.CM-05, DE.CM-07)
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities
DE.AE-03: Information is correlated from multiple sources
DE.AE-04: The estimated impact and scope of adverse events are understood

DE.AE-06: Information on adverse events is provided to authorized staff and tools (Formerly DE.DP-04)
DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria (Formerly DE.AE-05)
PR.IR-04: Adequate resource capacity to ensure availability is maintained (Formerly PR.DS-04)
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared (Formerly RS.RP-01, FS.CO-04)
RS.MA-02: Incident reports are triaged and validated (Formerly RS.AN-01, RS.AN-02)
RS.MA-03: Incidents are categorized and prioritized (Formerly RS.AN-04, RS.AN-02)
RS.MA-04: Incidents are escalated or elevated as needed (Formerly RS.AN-02, RS.CO-04)
RS.MA-05: The criteria for initiating incident recovery are applied
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident
RS.AN-06: Actions performed during an investigation are recorded and the records' integrity and provenance are preserved (Formerly part of RS.AN-03)
RS.AN-07: Incident data and metadata are collected and their integrity and provenance are preserved
RS.CO-02: Internal and external stakeholders are notified of incidents
RS.CO-03: Information is shared with designated internal and external stakeholders (Formerly RS.CO-03, RS.CO-05)
RS.MI-01: Incidents are contained
RS.MI-02: Incidents are eradicated
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process
RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed
RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms
RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed
RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed
RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders

PHASE 3 - Longer Term Operational and Governance Priorities

GV.OC-03: Legal, regulatory and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed (Formerly ID.GV-03)
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions
GV.SC-07: The risks posed by a supplier, their products and services and other third parties are understood, recorded, prioritized, assessed, responded to and monitored over the course of the relationship (Formerly ID.SC-02, ID.SC-04)
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response and recovery activities (Formerly ID.SC-05)
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
GV.RR-04: Cybersecurity is included in human resources practices (Formerly PR.IP-11)
GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated and enforced to reflect changes in requirements, threats, technology and organizational mission (Formerly ID.GV-01)
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed
ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles (Formerly PR.DS-03, PR.IP-02, PR.MA-01, PR.MA-02)
ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded and tracked (Formerly part of PR.IP-03)
ID.IM-01: Improvements are identified from evaluations
ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties (Formerly ID.SC-05, PR.IP-10, DE.DP-03)
ID.IM-03: Improvements are identified from execution of operational processes, procedures and activities (Formerly PR.IP-07, PR.IP-08, DE.DP-05, RS.IM-01, RS.IM-02, RC.IM-01, RC.IM-02)
ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained and improved (Formerly PR.IP-09)
PR.PS-01: Configuration management practices are established and applied (Formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk (Formerly PR.IP-12, PR.MA-02)
PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk (Formerly PR.MA-01)
PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle
PR.IR-02: The organization's technology assets are protected from environmental threats (Formerly PR.IP-05)
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement
RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging (Formerly RC.CO-01, RC.CO-02)

CASE STUDY: PRACTICAL IMPLEMENTATION STEPS

As a small or regional communications operator, your company has an important role in the regional or local community. In many instances, a small network provider is the only communications operator serving critical anchor institutions within the community. A targeted cybersecurity attack could reduce response time, eliminate communications connectivity and/or provide misleading information during a disaster.

The following case study provides additional implementation guidance with respect to Phase One outlined above. The case study focuses on the public-facing network that affects a small operator's customers. As a small network service provider, your company should secure its core network and critical infrastructure and services by adhering to regulatory requirements and industry best practices; the immediate steps of Phase One items identified above and described in greater detail below should be applied to harden your network against external and internal cyberattacks.

GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy and priorities and is communicated and enforced

A centralized cybersecurity policy should be in place to help you guard against cyberattacks. The policy should establish the company's goals regarding cybersecurity and may reference appropriate laws, regulations, or rules. This policy will be used to inform all operational policies and procedures to attain the stated goals. It should be simple and generalized (i.e., our company commits to following the best practice guidelines contained within Version 2.0 of the Framework). We recommend that you implement a policy that will establish your company's cybersecurity stance and provide guidance to build upon, including operational policies and procedures relating to cybersecurity.

GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders

Establishing risk management processes allows an organization to view risks within a common methodology across all aspects of the organization. While different organizations have different risk tolerances, the way that risks and potential risk mitigation measures are evaluated should be documented and approved by organizational stakeholders. Lists of stakeholders should include the board of directors, CEO and risk officer. Organizations need to engage employees of the organization to determine what risk applies to their business unit and the company overall. As an administrative control, there should be an overarching policy that provides the framework for the treatment of risk activity that all employees understand and clearly explains how they contribute to the overall risk management process. Organizations should place emphasis on areas that affect their strategy and performance within their marketplace. Risk management processes also need to allow some risk to be taken and for employees to understand the level of risk they can accept at each level within the organization.

GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies and processes are established and agreed to by organizational stakeholders

NIST's emphasis on supply chain security in Framework 2.0 is a recognition of the increased risk to organizations from hardware, firmware and software supply chain threats. Congress has prohibited federal government procurement from certain foreign telecommunications equipment manufacturers and required that the FCC pass rules prohibiting such equipment from being granted future authorizations to be used in U.S. networks. Experts have reported possible efforts by sophisticated nation-state cyber actors to exploit firmware vulnerabilities to gain persistent access. Further, a third-party file transfer tool was compromised, giving attackers access to proprietary business and customer data belonging to thousands of organizations. Supply chain threats require ongoing diligence on the part of network operators. Such diligence should begin during the vendor selection process and be maintained throughout the business relationship.

GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes

While this item is not always applicable to small and medium businesses, it is important that if there is a governance and/or risk management process in place, it needs to address cybersecurity. Also noteworthy is to ensure that cybersecurity measures are being implemented using those risk management and governance processes. Many times, security measures are implemented without consideration of their true value to the company. If your organization does have a governance or risk management team, be sure that the governing body or C-Suite includes a member that is well-versed in information security standards. Likewise, cybersecurity initiatives should flow through governance and risk management processes to ensure they support the organizational goals.

ID.AM-01: Inventories of hardware managed by the organization are maintained;

ID.AM-02: Inventories of software, services and systems managed by the organization are maintained;

ID.AM-04 Inventories of services provided by suppliers are maintained

You cannot protect what you do not know you have. Therefore, all companies, regardless of size, should maintain a list of equipment required for critical services. This list can be as simple as a Microsoft Excel spreadsheet or as complex as an automated, electronic database. An inventory system is invaluable. For instance, it can be used to verify that software patches identified by the manufacturer or third parties have been applied. We understand that small communications operators may not have access to the information for systems purchased from vendors, but you should attempt to maintain a list of hardware and software that can be checked for common vulnerabilities and exposures (CVEs) as they become available.

All devices must be inventoried, including those that reside inside and outside of your network as they are vulnerable to attack. Those devices that are directly addressed from the open internet will have the highest risk of exposure to a cybersecurity incident. However, devices inside your network are also vulnerable to attack. A properly maintained inventory of all devices and software is required to understand the full risks to the organization.

As you will see later in the process, it is beneficial to recognize and document the intended function of each network device. As such, your inventory should include the purpose the device serves within your network. For example, your voice switch might be an application appliance, which serves as a critical infrastructure function; LAN switches (and/ or routers) may serve multiple functions such as network operations, customer support and/or corporate operations; and your customer billing application serves a corporate operations function. Each device should be catalogued and tracked according to the highest function it enables within your network—in this case, the "critical infrastructure" function. Page 24 includes a sample device inventory listing with examples of devices and ideas for how to organize, classify and track them.

After you have completed the inventory functions in ID.AM-01 and ID.AM-02, it is time to fully catalogue external information systems in accordance with ID.AM-04. This is to ensure the organization knows where its external data resides and to identify the associated risks. While some consider the cloud to be insecure, it can become more secure than data housed in an on-premises data center due to additional security controls the hosting organization imposes. When entering external systems in a catalogue, consider how users authenticate to the platform (and therefore the data) and who is responsible for maintaining and auditing the process. When it comes to cloud applications, traditional IT is not always needed or consulted, which can introduce risk and bypass some of the safeguards that were previously in place. Particularly, be sure to have a plan in place to disable access to external systems when employment changes occur.

ID.RA-01: Vulnerabilities in assets are identified, validated and recorded

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.

Any hardware or software being considered for your operations should also be evaluated for vulnerabilities prior to purchase. Common tools to review vulnerabilities are the MITRE CVE, NIST's National Vulnerability Database, or automated tools such as Nessus or Windows Baseline Security Analyzer.

We recommend that companies perform regular vulnerability scans of the network to expose potential problems. Vulnerability scans should be performed on all equipment, inside and out of your network boundaries, to ensure vulnerabilities are exposed. New equipment could be added to the network and it is important to understand any inadvertent ramifications. All unnecessary ports and services should be disabled as they are discovered.

PRIORITIZE

ID.RA-05: Threats, vulnerabilities, likelihoods and impacts are used to determine risk and inform risk prioritization

After you have identified and documented vulnerabilities in step ID.RA-01, it is important to evaluate the overall risk of each vulnerability to your organization. A high common vulnerability scoring system (CVSS) score indicates that a vulnerability is serious if exploited; however, it does not indicate the risk it poses to you. To ensure you give the appropriate attention to the items that are most likely to impact your organization negatively, consider analyzing whether vulnerabilities are currently being exploited in the wild. Another item to consider is whether that asset is exposed to the internet. Likewise, some vulnerabilities take quite a bit of technical knowledge and maybe even knowledge of the environment that they are in, while others can be exploited by a novice. Be sure to pay close attention to those novice-level vulnerabilities, as they are likely to have automated exploits that are widely published.

PR.AA-01: Identities and credentials for authorized users, services and hardware are managed by the organization

Unauthorized access is a critical vulnerability. All devices should be configured, at a minimum, to require a complex password for access and any default credentials should be changed and/or disabled. Only authorized personnel should know the password and it should only be stored in an encrypted area. Procedures must be established for provisioning and de-provisioning users, determining appropriate access levels and a periodic review and change of all passwords. Processes should also be in place to change or remove access when key personnel change duties or employment status. We recommend installing a centralized authentication system, which allows for an authentication policy to be implemented on one device and provides the ability to monitor and log access. Consider installing a centralized solution, such as a RADIUS server or a Microsoft Windows domain controller with Network Policy Server enabled that performs authentication and authorization for network equipment. A centralized solution allows access to be provisioned and de-provisioned for individuals as needed without disclosing system-level passwords. When such a system is used in conjunction with a least privilege design, access to processes can be controlled and audited.

PR.AA-06: Physical access to assets is managed, monitored and enforced commensurate with risk

Physical security is the first line of defense against unauthorized access or modification. As such, physical access should be managed based on the least privilege principle. This could be as complicated as a physical card reader system with surveillance cameras at each location, or as simple as making sure the data center/ central office door is locked. An NTCA member has installed a systemwide proximity card system and surveillance cameras to control and monitor access from a central location. As a small business, the company felt that the centralized control and monitoring approach was the best use of capital to secure their network.

PR.AA-03: Users, services and hardware are authenticated

Remote access is very important to companies that operate 24/7. Employees need to have access to equipment and data to perform their jobs while away from the office. However, remote access is an open door to a cyberattack if improperly configured, secured or monitored. Therefore, remote access should be implemented with a multifactor authentication (MFA) process and encrypted using a virtual private network, secure shell (SSH) or similar secure protocols. For example, this could be accomplished by using two separate password authentication systems or a system that supports multifactor authentication for remote access devices.

Once remote access is gained through the system, users should only be provided with access to necessary devices to reduce risks from compromised users/ passwords. For example, your CFO does not need access to the network equipment, while your CTO does not need access to transfer bank funds. Roles should be defined in your cybersecurity policies and implemented on all systems.

PR.IR-01: Networks and environments are protected from unauthorized logical access and usage

Protecting the integrity of your network is vital to ensuring protection of your information. There are a few key items to consider regarding network integrity. These include network diagrams, network segmentation, understanding dataflow and securing configurations for network devices. As a first step to protecting network integrity, understanding network diagrams helps to recognize where your systems are located and how they are connected. This also assists with other key steps to protecting your network integrity, such as network segmentation. Network segmentation helps provide both integrity and regulatory compliance. By using your network diagram, you can logically and physically separate systems that handle regulated data such as health information or credit card data. By properly segmenting these from normal users, data or other designations of resources, you can apply the correct level of security resources to protect the data housed in that segment. The segmentation can also assist in minimizing damage in the event of a data breach. Part of helping to protect against a data breach is to have secure configurations on your network devices such as firewalls, routers and switches. Ensure that the version of the operating system is current and supports your business needs. Follow a "deny all" mentality where you only allow traffic that is required to perform a business function.

PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions.

Ensuring an account is verified and belongs to the person it is assigned to is vital to protecting access to systems and information. PR.AA-02 is focused on interactions and activities that focus on non-repudiation, which means the identity tied to an action such as a logon or logoff is the actual person who was assigned to the account. There are some simple ways to help proof and bound credentials to employees.

The first is to have a documented account creation and modification process require approval based on the access requested. Access to data should be set via group membership and accounts should have access to data verified by the data owner. Second, access needs to be audited on a regular basis as determined by the organization. Third, user accounts need to have a password associated with them that meets the organization password complexity and length requirements. Fourth, companies need to establish lockout parameters for accounts, including password, attempts threshold and lockout duration. Fifth, companies should require separate restrictive user and privileged accounts for employees who perform activities that require administrator or root-level permissions. The use of service accounts needs to be documented and each account needs to have an owner and understanding of the account's purpose.

PR.AA-03: Users, services and hardware are authenticated

Your authentication methods and layers should depend on the criticality of the asset and the organization's risk acceptance. One key to determining the level of risk for any transaction is to determine the value of the asset or data. For users, there are several different authentication models available. The oldest – and now outdated – model is the single factor, username and password. You should increase the authentication steps for users by adding a second authentication step such as a smart card, phone authenticator or biometric authentication (e.g., fingerprint or facial recognition). These can be added aftermarket or built into the computing device. There is an additional cost for this second level of protection, also called multi-factor authentication (MFA) but may be required based on risk or regulatory requirements. Single Sign On (SSO) makes authenticating to applications easier for the user and can be implemented either through Security Assertion Markup Language (SAML) or OAuth. The key is that the base account must be secured and follow PR.AA-02 guidelines. Authentication to devices can be done on an individual basis where the accounts are proofed and bound or you can use a centralized authentication system such as Terminal Access Controller Access Control System (TACACS) for console access to network devices. You can also utilize 802.11x for authenticating devices to the network and verifying their security posture or include sticky MAC on switch ports. Regardless, if the authentication is for users or devices, auditing needs to be integrated into the discussion.

You should audit all important events regarding logon, logoff, access to critical data folders and other items of importance for the organization. You also need to determine if you are concerned about success or failure on each audit activity. This will depend on your monitoring strategy. Additionally, log files should be sent to a central log server or security information and event management (SIEM) for archiving, analysis and reporting ability.

PR.DS-01: The confidentiality, integrity and availability of data-at-rest are protected

This best practice could translate into a variety of levels of protection. For a small operator, simple procedures should be followed to protect data, including not leaving data outside the isolated network. We recommend all companies include rules about removing data from the network in their cybersecurity policy and encryption on all company devices.

PR.DS-02: The confidentiality, integrity and availability of data-in-transit are protected

Data-in-transit should be protected when it leaves isolated and protected networks. Data-in-transit that is not protected could be viewed and used for a cyberattack. Consider using encrypted VPN connections, encrypted virtual desktop connections, Secure Shell (SSH) and SSH file transfer protocol (SFTP) for remote access. Use of any standard file transfer protocol (FTP) and Telnet protocols should be eliminated wherever possible, as they do not protect data-in-transit. When necessary, the Telnet protocol should be limited to private connections not accessed over the internet. Any device that must be public facing and only supports FTP or Telnet should be replaced.

PR.DS-11: Backups of data are created, protected, maintained and tested

All companies should maintain backups of the network and they should be tested and verified on a regular basis. A network can never be protected from all cybersecurity risks; however, backups allow a network to be fully restored to a previous configuration. Network backups help to reduce network restoration time.

They should be performed after significant changes at minimum and preferably on a regular schedule. Multiple free or commercial software packages are available for configuration or system backup. Offline and offsite copies of backups should be maintained and regularly tested to limit the impact of a cyber incident and ensure the continuity of operations.

ID.AM-08: Systems, hardware, software and services are managed throughout their life cycles

If keeping someone physically away from the equipment is important, then making sure they are approved to have remote access is just as important. In some areas, remote access is even more important because the threats will come from outside the area. Remote access to equipment should be limited to appropriate personnel and hardware/locations designed with high levels of security; the best solution is to keep all management systems behind a firewall or control access by IP address. An NTCA member built a separate network using virtual local area networks (VLANs) and L3VPNs to separate monitor/control networks for its equipment. This control network is only accessed from its internal network or through a two-level authenticated firewall (key + username/password). The outside equipment has access lists applied to only allow IP addresses from its internal network.

PR.IR-01: Networks and environments are protected from unauthorized logical access and usage

All small operators should deploy network segregation at some level; at a minimum, you should separate your public and private networks. We also recommend that private networks be separated by roles for integrity, such as by critical infrastructure, network operations, corporate operations, business systems, etc. One large local area network (LAN) for computers and equipment management puts both the equipment and LAN computers at risk. However, if the networks are separated, controls based on company policy can be applied to limit access to the network, including by source and/or type of traffic. A network separated by function will limit the ability of a hacker to move laterally within your network, thereby jumping from a comprised device such as a business system PC to a device in your critical infrastructure network, such as a multiplexer transporting supervisory control and data acquisition (SCADA) circuits to a power facility. As systems and networks are separated by roles, the service provider should move the control system protection by implementing controls on each device to limit access and traffic to the control plane of the equipment. This advanced configuration will ensure access to the devices are available during an attack and reduce denial of service (DoS) attacks on the management of the devices.

PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations

Small broadband providers should design and implement their networks to maximize availability and resiliency. Redundancy is a key component toward achieving this goal. For example, using redundant upstream providers is a recommended best practice. Similarly, core routing equipment should be purchased with redundant components and implemented with full mesh networking to accomplish real-time failover.

At a minimum, we recommend maintaining a spare inventory of backup components that can be placed into service when a primary component fails. Such network design and implementation will decrease downtime and restoration time. All services required to provide internet access should be designed for high availability and load sharing where practical, including dynamic host configuration protocol (DHCP) and DNS. All critical systems should be designed to achieve “5 9’s” or 99.999% uptime.

PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind

We recommend a regular and continuous cybersecurity training program for staff. Cyber threats are evolving and continually challenging your network and its users, so all staff must be trained and tested for cybersecurity readiness. A system of training videos along with sporadic control tests will help keep staff members informed of the ever-present threats. Hackers will try to penetrate the network through social engineering tactics, exploiting human nature. Small network service providers are known for being friendly and ready to serve, but this makes us an easy target for bad actors. Example: a hacker finds the address and phone number of a customer. They call customer support and explain that they cannot access a website. Without adequate training on how to spot a cyberattack, your support staff may be tempted to follow the hacker's instructions to verify this website does not work—leading your employee to a compromised website that introduces a virus into your internal protected network.

PR.AT-02: Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind

A “privileged user” is one that is authorized (and therefore, trusted) to perform security-related or relevant functions on a system, or any portion thereof. As such, these accounts have a level of access not available to other users. Such access, if compromised, could lead to severe consequences, including impaired operations, data exfiltration or complete system failure.

Privileged users are typically those who have access to configure one or more critical systems, including the ability to create and secure other accounts, enable/disable critical system features and functions and have access to highly sensitive information. All privileged accounts must be clearly defined according to the necessity for the creation of such roles. Any person assigned to a privileged role must understand the effects of operating with a high level of access, as well as the repercussions of improper use or compromise of the same. It is recommended that:

- Privileged roles should be limited to the minimum number of people possible:

  - Designed using least privilege/access principles

  - Designed using separation of duties, as appropriate

  - Require more stringent authentication methods— i.e., two-factor authentication at minimum, unique credentials for each system, geolocation rules and account lockout rules

- Configure specific monitoring and auditing where possible—i.e., login audit, file system audit and change management using two-man rule

All such roles should be incorporated into job descriptions and/or departmental policies, clearly defining the areas of responsibilities. Training and security awareness appropriate to these positions should be performed regularly.

Similar to the description and recommendations of a privileged user, physical and cybersecurity personnel must be made aware of the critical nature of their job functions and responsibilities. While such personnel may or may not have access to the most sensitive data or systems, the jobs performed by such personnel are part of the controls to prevent, detect and respond to incidents.

In smaller companies, physical and cybersecurity roles may be integrated into job functions held by personnel who have privileged access. As such, these job roles should follow the recommendations for privileged users.

DE.CM-01: Networks and network services are monitored to find potentially adverse events

Just as the Identify step of the Framework is necessary to understand what you have and what needs to receive priority attention and protections, the Detect function informs the company of what is occurring at any given time in the environment. The essence of both Identify and Detect come together in DE.CM-01, the need to determine when anomalous events occur when compared to a functional baseline. More importantly, continuous monitoring, when properly implemented, provides indications of compromise for forensic or immediate action.

The goals of DE.CM-01, while diverse, can be achieved by using a variety of different systems. Ideally, complete monitoring, auditing and alerting can be accomplished using a full-featured Security Information and Event Manager (SIEM) system, such as commercial products like LogRhythm or Splunk. The potential attack surface can only be monitored effectively once a baseline and event triggers have been established.

Monitoring network traffic for anomalies is essential to detecting and responding to cybersecurity incidents. Cyberattacks can come in various forms and some attacks can cause huge network spikes. Using monitoring tools on the network allows these attacks to be identified and corrected. For example, free tools like Snort, MRTG/Cat or Nagios can be deployed to monitor the network and develop a baseline of operations. At minimum, we recommend deploying an Intrusion Detection/Prevention System (IDS/IPS). Such systems can monitor and prevent unauthorized traffic from traversing the network. These are often integrated in next-generation firewalls or can be deployed as a standalone system. The results of all monitoring systems should be logged to facilitate incident response and forensics per DE.AE-04.

- Unauthorized personnel can be monitored at:
  - Point of authentication/authorization; e.g., Windows login, database login and access and firewall/VPN
  - Physical security/surveillance
  - File integrity monitoring
- Unauthorized connections and devices
  - Web applications
  - Switches/firewalls/routers
  - Wireless access points/controllers
- Unauthorized software
  - Asset management
  - Configuration change management

All audited events should, at minimum, be collected at a central point, such as a syslog or network management server, preferably with a component to send alerts via email or SMS. The events should be regularly reviewed and audited for anomalies.

Additionally, malware detection and antivirus software should be installed and maintained on all devices, in addition to the ingress/egress network point, to watch for anomalies.

DE.CM-02: The physical environment is monitored to find potentially adverse events

Physical security should be at the core of every system design, from the exterior of a building to the rack that houses system components or the PC sitting on a desk. Physical access to a system virtually guarantees a cybercriminal success, regardless of the relative importance of the system in question. This also includes remote access to physical environment controls.

To detect cybersecurity events, continuous monitoring must be part of the design of all systems. Simple locks might be an effective deterrent to the common person but pose no serious obstacle to a skilled cybercriminal with direct physical access; moreover, forcing open an unmonitored physical lock with even a modicum of care leaves no trace.

Even for small companies, a basic system for physical security is achievable at a reasonable cost. At a minimum, a company should control key disbursement for physical locks. However, this will not satisfy the need for continuous monitoring.

Access control to critical systems, sensitive data storage, building environmental systems or even just the perimeter can be achieved using a centralized security system that includes electronic locks with proximity or biometric sensors, surveillance cameras located in public and critical areas and door prop sensors on racks. Additionally, locking racks or face plates should be used on equipment that cannot be housed in controlled areas. Access to such areas or equipment should be limited to the personnel directly responsible for installation and maintenance and event logs should be audited on a regular basis.

Environmental controls should also be monitored and audited on a regular basis. Loss of power, temperatures, or humidity out of scope, or loss of air flow can also cause or be an indicator of a cybersecurity event.

ID.RA-01: Vulnerabilities in assets are identified, validated and recorded

We recommend that companies perform regular vulnerability scans of the network to expose potential problems. Vulnerability scans should be performed on all equipment, inside and out of your network boundaries, to ensure vulnerabilities are exposed. New equipment could be added to the network, and it is important to understand any inadvertent ramifications. All unnecessary ports and services should be disabled as they are discovered.

RS.MA-01: The incident response plan (IRP) is executed in coordination with relevant third parties once an incident is declared

Businesses (small or large) need to have a response plan to describe what a company should do during a cyber incident. This could be an informal plan (something agreed upon verbally), but it is better if the plan is formalized in writing and specifies how to handle a cybersecurity event. For example, it can include who needs to be contacted internally (C-level, legal, network manager, security) and who is authorized to approve mitigation efforts, including disabling remote access, internet traffic or a BGP session and/or installing an access list. By delineating roles, responsibilities and authorities within your prepared response plan, you can decrease the recovery/mitigation time frame.

During the creation of an IRP, stakeholders are identified, areas of responsibility are assigned and internal and external communication processes are defined. When possible, communications should be pre-scripted and reviewed by the stakeholders before an incident occurs. A response plan that is developed and shared with all stakeholders will allow quicker and more precise dissemination of information during a crisis. Then, during an incident, the plan should be executed accordingly. For example, during a significant cybersecurity incident, the incident response team lead, who is specified within your plan, will alert management as to the nature of the incident and provide regular updates. Depending upon the nature of the event, your legal representatives or insurance underwriter may need to be contacted, as specified within your plan. Should customers be affected, the response team would also engage the customer service representatives to tailor their responses to customer inquiries, the webmaster to update the website and the public relations team to engage with the public and the media, as necessary.

Items to include in your IIRP:

- Definitions of an incident
- Incident team members
- During- and post-incident responsibilities
- If/when legal counsel should be involved
- Information of law enforcement agency or agencies to be contacted
- Information of business partners to be contacted

The IRP should also be practiced, at least annually, through tabletop exercises that bring together stakeholders. This will help identify areas of improvement and ensure the document is updated regularly. Just like everything else, practice will help get it right when it is needed the most.

RS.CO-03: Information is shared with designated internal and external stakeholders

This should be defined in the IRP before an incident happens. Information that is shared needs to be vetted by appropriate personnel within the organization. You should strongly consider consulting legal counsel before the information is released. Each organization should have a designated official responsible for sharing information internally and externally.

RS.MA-02: Incident reports are triaged and validated

We understand that detection systems may not be part of all network plans due to their cost and complexity.

If detection systems are used within a network, these systems should be configured for remote alerting or active monitoring to ensure an immediate response to cybersecurity incidents. We recommend, at a minimum, setting up system logging on all devices and using free, off-the-shelf commercial software platforms to record data. Logging of the data will not be as robust as a dedicated detection system but will provide data that can be used for root-cause analysis.

ID.RA-09 Incidents are contained

Cybersecurity incidents should be contained within a network as soon as possible. This may include shutting down all affected equipment, shutting down a specific user's access to the network or device, or removing access to the device completely (both ingress and egress). This process should be automated in a large company but may require manual intervention in a small business.

RS.MI-02: Incidents are eradicated

Once an incident has been contained, the next step will be to find the root-cause and then correct the issue. If the original problem is not corrected, the incident could happen again.

ADDITIONAL RESOURCES AND REFERENCES

NIST FRAMEWORK EVALUATION TOOL

NTCA worked with the Member Advisory Group to create a "NIST Framework Evaluation Tool" for CSF version 2.0 to offer a more robust resource or a high-speed road map that references all of the subcategories contained within the NIST Cybersecurity Framework 2.0. This Evaluation Tool is intended to help your team evaluate your company's cybersecurity program at a more granular and sophisticated level.

This **"NIST Framework Evaluation Tool"** for Version 2.0 includes blue columns, which delineate the functions, categories, subcategories and informative references that are inherent components of the NIST Cybersecurity Framework. The green columns were added by NTCA and provide ideas for how to evaluate your company's cybersecurity posture relative to the listed best practices. (For more information as to the columns within the tool, refer to the "Legend" tab at the bottom of your screen.) However, just as the NIST Cybersecurity Framework is a flexible and scalable document, this "NIST Framework Evaluation Tool" should also be adjusted to meet your unique needs.

Once the evaluation process is complete, your company may desire to sort the resulting data to assist with prioritization efforts within your organization. For instance, the Framework best practices could be sorted by those that your company has deemed of "high criticality" and "low financial investment" in order to prioritize your security efforts. Once again, there are many ways to the use the Framework and this "NIST Framework Evaluation Tool," adapting the resources for your company's specific needs and analyzing the resultant data to prioritize your security efforts as you see fit.

SAMPLE INVENTORY LISTING

As previously discussed, the NIST Cybersecurity Framework was specifically developed to help organizations secure critical infrastructure. Indeed, given their limited resources, small network service providers should start by applying the Framework to "core network" and "critical infrastructure and services," as recommended by CSRIC IV WG4. However, the philosophy and techniques are equally applicable to your corporate operations, and as your company seeks to evolve and mature its holistic cybersecurity program, the Framework should be applied to secure your business and internal IT systems.

A sample inventory listing is included on page 24 In addition, included below are ideas for devices you may want to consider tracking as part of your critical infrastructure list:

- ✓ Voice switch
- ✓ Optical and/or metallic-based multiplexers that handle critical connections—for example, control circuits for power stations, community water systems, public safety or law enforcement
- ✓ Core router(s)
- ✓ Data switches and routers, depending on applications and devices served
- ✓ Physical and virtual servers
- ✓ Broadband remote access server (BRAS), if it serves a critical customer
- ✓ Digital subscriber line access multiplexer (DSLAM), if it serves a critical customer
- ✓ Reconfigurable optical add drop multiplexer (ROADM) that handles critical connections—for example, control circuits to power stations or community water systems, public safety and law enforcement circuits
- ✓ Network ops work stations
- ✓ Servers that back up critical infrastructure configuration files
- ✓ Network managed power systems (AC and DC) in central offices, remotes and data centers
- ✓ Remotely managed generators
- ✓ Network-managed HVAC systems in central offices, remotes and data centers
- ✓ Firewall(s)
- ✓ Intrusion detection system (IDS)/intrusion protection system (IPS)
- ✓ Element management system (ESM)
- ✓ Auto configuration system (ACS)
- ✓ Video system emergency alert system (EAS) receiver/generator

Additional “critical infrastructure” considerations:

- ✓ Critical infrastructure devices frequently have more than one network connection, so each needs to be consciously managed/protected;
- ✓ Look for connected server “maintenance” ports as well as network interface connectors (NICs); and
- ✓ If using virtual machines, remember to keep the HyperVisor patches current and ensure virtual NICs are properly isolated.

SAMPLE INVENTORY LISTING

Device Name	Make	Model	BIOS	OS Version	Location	Functional Group	Criticality	Last Update	Previous Update
Voice Switch	GenBand	C-15		13.2.27	CO Isle 2-5-23	Network Ops	Critical Infrastructure		
Optical Mux	Fuji	LS- 2000		17.2	MDF Room Isle 1-2-30	Network Ops	Critical Infrastructure		
Data Switch - 3	HP	5412		R-27.3	CO Isle 2-6-20	Network Ops	Critical Infrastructure		
Data Switch - 1	HP	5412		R-27.3	Data Center	Network Ops, Corporate Ops, Customer Support	Critical Infrastructure		
Server - 6	HP	G8	2.3	CENTOS 7.6	Data Center Isle 2-3-3	Network Ops - Mapping	NOT Critical Infrastructure		
Server - 10 PM	HP	G8	2.3	VMWare 3.1	Data Center Isle 2-3-10	VM Cluster Supports All Network, Corporate and Business Segments	Critical Infrastructure		
Server - 11 PM	HP	G8	2.3	VMWare 3.1	Data Center Isle 2-3-11	VM Cluster Supports All Network, Corporate and Business Segments	Critical Infrastructure		
Server - 12 PM	HP	G8	2.3	VMWare 3.1	Data Center Isle 2-3-12	VM Cluster Supports All Network, Corporate and Business Segments	Critical Infrastructure		
Server - 13 PM	HP	G8	2.3	VMWare 3.1	Date Center Isle 2-3-13	VM Cluster Supports All Network, Corporate and Business Segments	Critical Infrastructure		
Server - 14 PM	HP	G8	2.3	VMWare 3.1	Center Isle 2-3-14	VM Cluster Supports All Network, Corporate and Business Segments	Critical Infrastructure		
Server - 15 PM	HP	G8	2.3	VMWare 3.1	Data Center Isle 2-3-15	VM Cluster Supports All Network, Corporate and Business Segments	Critical Infrastructure		
Accounting	VM			Windows-10 Patched Date		Corporate Ops	NOT Critical Infrastructure		
Customer Billing	VM			Windows-10 Patched Date		Corporate Ops	NOT Critical Infrastructure		
Work Station 7	Dell	oti 6	11.1	Windows-10 Patched Date	Business Office	Customer Support	NOT Critical Infrastructure		
Router - 1	Cisco	9001		23.6.111-3	CO Isle 2-6-28	Network Ops - Core Router	Critical Infrastructure		

ANNOTATED LIST OF RESOURCES

Included below is an annotated list of tools, templates, reports, websites, etc., that you may find of assistance with your cybersecurity efforts.

RESOURCE TYPE	SOURCE	TITLE	LINK	DESCRIPTION
Best Practices	Cybersecurity and Infrastructure Security Agency (CISA)	Cybersecurity Best Practices	**https://www.cisa.gov/topics/cybersecurity-best-practices**	Information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks.
Best Practices	National Institute of Standards and Technology (NIST)	Cybersecurity for Small Business: The Fundamentals	**https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-fundamentals-presentation**	This report assists small business management with understanding how to provide basic security for their information, systems and networks.
Best Practices	NIST	Small Business Cybersecurity Case Study Series	**https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series**	The case study series prove useful in stimulating ongoing cybersecurity awareness learning for all business owners and their employees.
Resource	NIST	NIST 2.0 Resource Center	**https://www.nist.gov/cyberframework**	Last updates on CSF 2.0, including guides and resources.
Best Practices	Center for Internet Security (CIS)	The 18 CIS Controls & Resources	**https://www.cisecurity.org/controls/cis-controls-list/**	A prioritized set of best practices created to stop the most pervasive and dangerous threats of today.
Forums	NTCA – The Rural Broadband Association	CyberShare: The Small Broadband Provider Information Sharing and Analysis Center (ISAC)	**https://www.cyber-share.org/**	CyberShare provides immediate, actionable cyber threat information, and as an ISAC recognized by the National Council of ISACs, it is designed to maximize information flow across the small broadband provider sector and with government. CyberShare participants have access to daily and weekly reports and have the ability to communicate and collaborate in a trusted setting.
Network Protection Tool	Cybersecurity and Infrastructure Security Agency (CISA)	Known Exploited Vulnerabilities Catalog	**https://www.cisa.gov/known-exploited-vulnerabilities-catalog**	CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

RESOURCE TYPE	SOURCE	TITLE	LINK	DESCRIPTION
Forums	DHS	State and Regional Fusion Centers	https://www.dhs.gov/fusion-center-locations-and-contact-information	State and Regional Fusion Centers operate as state and major urban area focal points for the receipt, analysis, gathering and sharing of threat-related information among federal, state, local, tribal, territorial and private-sector partners.
Network Protection Tool	Open Source	Network Mapper (Nmap)	https://nmap.org/	Nmap ("Network Mapper) is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/ firewalls are in use and dozens of other characteristics.
Network Protection Tool	RAPID7	Penetration Testing Software	https://www.metasploit.com/	A collaboration of the open source community and Rapid7. Their penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments.
Network Protection Tool	SNORT	SNORT	https://www.snort.org/	Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS).
Planning Guide	CISA	Cybersecurity Resources Road Map	https://us-cert.cisa.gov/sites/default/files/c3vp/smb/DHS-SMB-Road-Map.pdf	A guide for identifying useful cybersecurity best practices and resources based on needs.
Planning Guide	CISA	Insider Threat Mitigation	https://www.cisa.gov/insider-threat-mitigation	The guide is designed to assist individuals, organizations, and communities in improving or establishing an insider threat mitigation program.
Planning Guide	DHS	Business Continuity Planning Suite	https://www.ready.gov/business-continuity-planning-suite	This software was created for any business with the need to create, improve or update its business continuity plan. The suite consists of business continuity plan (BCP) training, automated BCP and disaster recovery plan (DRP) generators and a self-directed exercise for testing an implemented BCP.
Planning Guide	NTCA	NTCA Cybersecurity Series	https://www.ntca.org/member-services/be-cyberwise	A 6-part series designed as a comprehensive guide to help telco executives, board officers and operational staff develop a risk-management approach to cybersecurity.

RESOURCE TYPE	SOURCE	TITLE	LINK	DESCRIPTION
Resource List	CISA	Stop Ransomware Guide	https://www.cisa.gov/resources-tools/resources/stopransomware-guide	A resource to help organizations reduce the risk of ransomware through best practices to detect, prevent, respond and recover.
Resource List	FCC	Cybersecurity for Small Businesses	https://www.fcc.gov/general/cybersecurity-small-business	The FCC offers a wide range of cybersecurity resources for small businesses under their Cybersecurity for Small Business website section. The resources include FCC, other government agency and private cybersecurity educational tools.
Resource List	Multi-State Information Sharing & Analysis Center (MS-ISAC)	MS-ISAC Cyber Security Toolkit	https://www.cisecurity.org/ms-isac/ms-isac-toolkit/	Near the bottom of this page are some documents created by the MS-ISAC to raise cybersecurity awareness through informative and practical means. There are also other cybersecurity resources and links on this page.
Resource List	NIST	Small Business Cybersecurity Corner	https://www.nist.gov/itl/smallbusinesscyber	NIST provides the small business community with their Small Business Cybersecurity Corner. It is a cybersecurity information and management tool that includes cybersecurity basics, guidance, solutions and training.
Resource List	US-CERT	Publications	https://us-cert.cisa.gov/security-publications	Various publications to help a user, from setting up a computer to emerging threats.
Network Protection Tool	US-CERT	Common Vulnerabilities and Exposures (CVE)	http://cve.mitre.org/cve	CVE is a dictionary of publicly disclosed cybersecurity vulnerabilities and exposures that is free to search, use and incorporate into products and services, per the terms of use.
Training	US-CERT	CERT Podcast Series	https://www.sei.cmu.edu/publications/podcasts/index.cfm	A series of podcasts that provides both general principles and specific starting points for business leaders who want to launch an enterprise-wide security effort or make sure their existing security program is as good as it can be.

NTCA Cybersecurity Series

(Part 2)

Sector-Specific Implementation Guidance for the NIST Cybersecurity Framework

#BeCyberwise

NTCA THE RURAL BROADBAND ASSOCIATION®

4121 Wilson Boulevard • Suite 1000 • Arlington, VA 22203-1801
703.351.2000 • www.ntca.org