Sector-Specific Guide for Small Network Service Providers

Using the NIST Cybersecurity Framework to Improve Your Cybersecurity Posture

September 2018

Table of Contents

1 Introduction

Within the last few years, cyber attacks have intensified in frequency, sophistication and severity. Corporations, networks and individuals are under constant attack from cyber threats originating within the United States and abroad. Bad actors are targeting all organizations, regardless of their size or business mission, and a cyber attack could adversely affect the continued viability of your company. Indeed, your corporate or business systems present an attractive financial target for bad actors. But as a small communications service provider, attacks against your core networking technology and critical infrastructure systems pose far greater consequences, threatening the availability, integrity and/or confidentiality of the communications network.

Given the dynamic and evolving nature of the threat, a static, prescriptive checklist approach to security is ill advised. Rather, cybersecurity resilience is best approached from a risk/benefit analysis. The central resource for this effort is the "Framework for Improving Critical Infrastructure Cybersecurity" (the NIST Cybersecurity Framework).[1] The framework's risk-management approach to cybersecurity is flexible and scalable in order to successfully accommodate your environment, risk tolerance and unique needs. It helps 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.

The framework provides five "functions" that all organizations, regardless of size, can use to evaluate their cybersecurity programs:

- Identify: Develop an understanding within an organization or operation to manage cybersecurity risks 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 methods to respond to cybersecurity events.
- Recover: Ensure the ability to restore normal operations and to learn from events.

Within each function, the framework provides more granular guidance via more specific "categories" and "subcategories."

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.

[1] For more information about the NIST Cybersecurity Framework, please visit: http://www.nist.gov/cyberframework/index.cfm.

2 Background

In response to evolving and increasing cyber threats, President Barack Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity,"[2] (EO) in February 2013. The EO directed the National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, to develop a voluntary framework for reducing cyber risks to critical infrastructure. Released in February 2014, the NIST Cybersecurity Framework[3] was created to assist all 16 critical infrastructure sectors,[4] including communications operators, with managing cyber risk.

The framework was designed to be technology-neutral, flexible and scalable, and applicable to a wide variety of industries and organizations. Indeed, "use" of the framework purposefully has not been defined; there are many ways for an organization to use the framework to install a new cyber risk-management program or enhance its existing program, applying only the practices enumerated within the framework that make sense for its needs.

In March 2014, the FCC convened an industry advisory council—the Communications Security, Reliability and Interoperability Council IV Working Group 4 (CSRIC IV WG4)—to analyze the NIST Cybersecurity Framework with respect to the specific needs of the communications sector and provide guidance as to how communications companies can apply the framework within their organizations. Within WG4, a Small and Medium Business (SMB) Feeder Group focused on helping small and medium communications companies understand how the framework could be applied to their operations to secure critical infrastructure and services while also respecting challenges related to their size and limited resources.

Taken together, Version 1.0 of the NIST Cybersecurity Framework and the sector-specific report provided by CSRIC IV WG4[5] provide communications companies with substantive guidance on how to use the framework to mitigate cyber-based threats to their communications networks, infrastructure and sensitive data.

[2] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," rel. Feb. 12, 2013, available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[3] For more information on the NIST Cybersecurity Framework, see https://www.nist.gov/cyberframework. For historical reference, Version 1.0 of the framework is available online at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[4] To learn about the federally recognized 16 critical infrastructure sectors, see https://www.dhs.gov/critical-infrastructure-sectors.

[5] See CSRIC IV, "Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report," rel. March 2015, at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

Subsequent to the release of the EO, the Cybersecurity Enhancement Act of 2014[6] reinforced NIST's role and the nation's continued commitment to the ongoing development of the framework. As such, in April 2018, NIST released Version 1.1 of the framework,[7] which includes additional best practices beyond the original Version 1.0 release.

In the summer of 2018, NTCA–The Rural Broadband Association (NTCA) convened a Member Advisory Group to evaluate Version 1.1 of the NIST Cybersecurity Framework and update the initial 2014 guidance provided by the CSRIC IV WG4 SMB Feeder Group. Therefore, the guidance provided to small network operators within these pages draws heavily from the initial leadership and direction offered in the CSRIC IV WG4 SMB Report,[8] but has been updated to reflect Version 1.1 of the framework and the evolving cybersecurity needs of small network service providers.

3 Objective, Scope & Methodology

3.1 Objective

This report strives to provide overall guidance on how small network service providers can digest and apply Version 1.1 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).

3.2 Scope

The NTCA Member Advisory Group offers the following guidance on its target reader: a facilities-based network service provider that operates a wireline, wireless and/or video network with fewer than 1,500 employees[9] 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.

[6] The Cybersecurity Enhancement Act of 2014, S. 1353, https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[7] For more on the NIST Cybersecurity Framework, see https://www.nist.gov/cyberframework. Version 1.1 of the framework is available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[8] See CSRIC IV, "Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report," rel. March 2015, available at: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf. Note: The entirety of the WG4 report is more than 400 pages; the guidance specifically applicable to small and mid-sized businesses is located via section 9.9.

[9] The Small Business Administration (SBA) has established a numerical definition of small businesses, or size standards, for all for-profit industries, which are helpful as a general guide: https://www.sba.gov/content/summary-size-standards-industry-sector. According to the SBA, a wired and/or wireless telecommunications provider is defined as "small" if it has fewer than 1,500 employees.

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 organizations, i.e., should the framework be applied to your corporate, IT or varied telecom access networks. Consistent with the spirit of the framework and the guidance provided by the April 2014 convened CSRIC IV WG4, small network service providers should start by applying the framework to "core network" and "critical infrastructure and services," as recommended by CSRIC IV WG4. For example, a small network operator should maintain service to its core switch so that emergency services are able to 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," please see Section 6.1 on page 19.

3.3 Methodology

The NTCA Member Advisory Group evaluated the 108 subcategories included within Version 1.1 of 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, the NTCA Member Advisory Group grouped the framework subcategories into high-priority, mid-priority and low-priority listings or "profiles."[10] These profiles offer a small network provider implementation guidance and strategy as it relates to the framework best practices. However, the NTCA Member Advisory Group urges caution as the term "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.

[10] See the NIST Cybersecurity Framework, Version 1.1, page 4. The term "profile" is used by NIST to describe "the outcomes based on business needs that an organization has selected from the framework Categories and Subcategories." For instance, an organization's "Current Profile" may contain those framework subcategories it has already implemented, while its "Target Profile" would contain additional subcategories the organization has identified as important to improving its cybersecurity posture.

The high priority/first-step profile included below contains 29 subcategories or best practices from the framework. This culled list 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. The mid-priority or second-step profile contains 33 subcategories, while the low-priority or third-step profile contains 35 best practices. Also of note, the group identified 11 framework subcategories as not applicable (N/A) or out-of-scope for small network service providers, as they were far beyond the practical and operational capabilities of a small company and/or did not serve to protect core network or critical infrastructure.

In addition to the profile listings, the NTCA Member Advisory Group developed a case study that offers additional practical guidance for small network service providers with respect to implementation of the best practices contained within the high-priority or first-step profile.

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—of the 108 included in Version 1.1 of the framework—are most applicable to its operational environment and security needs.

4 Guidance for Small Network Service Providers

4.1 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, the NTCA Member Advisory Group 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 no longer an effective defense as it confines the tactics by which an organization can prepare for and respond to eminent 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. Re-evaluate your security needs, current status, target state and related priorities on a recurring basis, with an eye toward process maturity.

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

Mid Priority or Second Step
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
PR.AT-2: Privileged users understand their roles and responsibilities
PR.AT-4: Senior executives understand their roles and responsibilities
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
PR.DS-4: Adequate capacity to ensure availability is maintained
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
PR.IP-3: Configuration change control processes are in place
PR.IP-10: Response and recovery plans are tested
PR.IP-12: A vulnerability management plan is developed and implemented
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
PR.PT-2: Removable media is protected and its use restricted according to policy
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats
DE.CM-5: Unauthorized mobile code is detected
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
DE.DP-3: Detection processes are tested
DE.DP-4: Event detection information is communicated
DE.DP-5: Detection processes are continuously improved
RS.CO-1: Personnel know their roles and order of operations when a response is needed
RS.CO-3: Information is shared consistent with response plans
RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
RC.CO-1: Public relations are managed

RC.CO-2: Reputation is repaired after an incident
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Low Priority or Third Step
ID.AM-3: Organizational communication and data flows are mapped
ID.AM-4: External information systems are catalogued
ID.GV-4: Governance and risk management processes address cybersecurity risks
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
ID.RM-2: Organizational risk tolerance is determined and clearly expressed
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
PR.IP-6: Data is destroyed according to policy
PR.IP-7: Protection processes are improved
PR.IP-8: Effectiveness of protection technologies is shared
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
DE.AE-2: Detected events are analyzed to understand attack targets and methods
DE.AE-3: Event data are collected and correlated from multiple sources and sensors
DE.AE-5: Incident alert thresholds are established

DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
DE.DP-2: Detection activities comply with all applicable requirements
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
RS.AN-2: The impact of the incident is understood
RS.AN-3: Forensics are performed
RS.AN-4: Incidents are categorized consistent with response plans
RS.IM-1: Response plans incorporate lessons learned
RS.IM-2: Response strategies are updated
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident
RC.IM-1: Recovery plans incorporate lessons learned
RC.IM-2: Recovery strategies are updated
N/A – Out of Scope
ID.BE-1: The organization's role in the supply chain is identified and communicated
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
ID.BE-4: Dependencies and critical functions for delivery of critical services are established
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.RA-4: Potential business impacts and likelihoods are identified
PR.DS-5: Protections against data leaks are implemented
PR.DS-7: The development and testing environment(s) are separate from the production environment
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
PR.IP-2: A System Development Life Cycle to manage systems is implemented

4.2 Case Study

As a small or regional communications operator, your company does not have a national presence, however it 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 the high-priority profile 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 high-priority items identified above should be applied to harden your network against external and internal cyber attacks.

ID.AM-1: Physical devices and systems within the organization are inventoried
ID.AM-2: Software platforms and applications within the organization are inventoried

You can't protect what you don't 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. We recommend tools that can gather this information and produce some type of report(s). 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 addressable 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 (i.e., *PR.PT-3* and *PR.PT-4*), 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, in the network operations group, which services a critical infrastructure function; LAN switches (and/or routers) may serve multiple functions such as network operations, customer support and/or corporate operations; while 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. Section 6.1, which starts on page 19, includes a sample device inventory listing with examples of devices and ideas for how to organize, classify and track them.

ID.GV-1: Organizational cybersecurity policy is established and communicated

A centralized cybersecurity policy should be in place to help you guard against cyber attacks. 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 1.1 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.

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.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes

Unauthorized access is a critical vulnerability. All devices should be configured to require a complex password for access, and any default user names and passwords should be changed and/or disabled. Only authorized personal 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 accounts and/or 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 access, logging it as it occurs. 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/access design, access to processes can be controlled and audited.

PR.AC-2: Physical access to assets is managed and protected

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 (see *PR.PT-3* below). This could be as complicated as a physical card reader system with surveillance cameras at each location, or as simple as making sure the database center/central office door is locked. In our use case, we installed a systemwide proxy card system and surveillance cameras to control and monitor access from a central location. As a small business, we felt that the centralized control and monitoring approach was the best use of capital to secure our network.

PR.AC-3: Remote access is managed

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 cyber attack if improperly configured, secured or unmonitored. Therefore, remote access should be implemented with a multifactor authentication 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.AT-1: All users are informed and trained

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 random 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 cyber attack, 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.DS-1: Data-at-rest is 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 in their cybersecurity policy rules about removing data from the network and encryption on all company devices. For example, Microsoft includes BitLocker on all Windows10 Pro operating systems, which is a free feature that can be used to encrypt the data on a PC.

PR.DS-2: Data-in-transit is 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 cyber attack. Consider using encrypted VPN connections, encrypted virtual desktop connections, SSH and SSH file transfer protocol (SFTP) for remote access. Use of any standard file transfer protocol (FTP) and Telnet protocols should be limited because 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.IP-4: Backups of information are conducted, 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 an original configuration. Having backups available helps to reduce network restoration time. Network backups should be performed after significant changes and/or on a schedule. Multiple free or commercial software packages are available for configuration or system backup. Offline copies of backups should be maintained and regularly tested to limit the impact of a cyber incident and ensure the continuity of operations.

PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

A response plan should define roles and responsibilities for various team members. We recommend, at a minimum, to create a flow chart showing who to notify for what type of incident. For instance, you may not need to contact your CFO for a denial of service (DNS)/network time protocol (NTP) attack, but your CFO should be notified of an attack designed to compromise company financial data. It is also important to include in the plan any legal or regulatory requirements.

PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

If keeping someone physically away from the equipment is important, then making sure they do not 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 controlled; the best solution is to keep all management systems behind a firewall or control access by IP address. In our case, we built a separate network using virtual local areas networks (VLANs) and L3VPNs to separate monitor/control networks for our equipment. This control network is only accessed from our 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 our internal network.

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

We recommend that you configure your devices with only essential capabilities to perform the required task. Similarly, users should be assigned privileges based on the least privilege required to perform their assigned duties. For example, least functionality of devices includes disabling or removing unnecessary services on servers or limiting traffic to only required ports. We recommend a policy to define which users and groups are authorized to access the network, as well as installing a centralized system that enables you to configure each device and thereby control access consistent with your company policy.

PR.PT-4: Communications and control networks are protected

All small operators should be deploying 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 LAN for computers and equipment management puts both the equipment and local area network (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 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.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) 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. By way of 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.

DE.AE-4: Impact of events is determined

Depending upon the type of event, the impact can be difficult to assess. Small carriers should deploy some type of external logging to assist in determining the source and impact of events. A good log server will accept syslog and other logs, which can be correlated and analyzed. As the provider becomes more advanced in cyber defense, this system should accept logs from firewall/intrusion detection systems to watch for malicious traffic. After every event, your Incident Response Team should use these logs as a tool to build a root cause analysis, incorporate findings into improved responses, and determining what, if any, further controls need to be put in place.

DE.CM-1: The network is monitored to detect potential cybersecurity events

Monitoring network traffic for anomalies is essential to detecting and responding to cybersecurity incidents. Cybersecurity attacks 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 IPS/IDS (Intrusion Prevention/Detection System). 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-4*.

DE.CM-4: Malicious code is detected

Malicious code is a way to gain access to a network to cause problems. As such, 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-8: Vulnerability scans are performed

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.RP-1: Response plan is executed during or after an incident

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 and specifies how to handle a cybersecurity event. Our plan includes who needs to be contacted internally (C-level, legal and/or network manager); and who is authorized to speed up mitigation efforts, including disabling remote access, internet traffic or a BGP session, and/or installing an access list. By providing direct authorized items within your prepared response plan, you can decrease the recovery/mitigation time frame.

RS.CO-2: Incidents are reported consistent with established criteria

Most likely small businesses will not have staff dedicated to cybersecurity risk management. These roles will be filled by multiple personnel and completed as part-time work. Part-time roles enforce the need for response plans and reporting systems. If you employ full-time security personal, they likely understand the flow to resolve a problem. In a small business, part-time roles require information and procedures to ensure polices are followed. By themselves, policy and procedures never make a network secure, but they allow conformity to ensure all parties are aware of their roles and responsibilities and that information is documented.

RS.CO-4: Coordination with stakeholders occurs consistent with response plans

During the creation of an incident response plan (*PR.IP-9*), 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.

By way of 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 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 reports, the webmaster to update the website, the marketing team to update social media with relevant information, and the public relations team to engage with media as necessary.

RS.AN-1: Notifications from detection systems are investigated

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.

RS.MI-1: Incidents are contained

Cybersecurity incidents should be contained within a network. This may include shutting down the effected 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-2: Incidents are mitigated

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 attack or incident could happen again.

5 NTCA Member Advisory Group

The following NTCA members assisted with the creation of this report. NTCA and the community thanks them for their participation, engagement and support of this effort.

Name	Company
Jerry Horton	Blue Valley Tele-Communications (Home, Kan.)
Chad Kliewer	Pioneer Telephone Cooperative (Kingfisher, Okla.)
Jeremy Larson	USConnect (Colorado City, Colo.)
Rob Leonard	Hamilton Telecommunications (Aurora, Neb.)
Rhonda Lively	Shentel (Edinburg, Va.)
Bill Trelease	Delhi Telephone Company (Delhi, N.Y.)
Jeff Walker	Pioneer Communications (Ulysses, Kan.)
Jesse Ward	NTCA–The Rural Broadband Association
Kathleen Whitbeck	Nsight (Greenbay, Wis.)

6 Additional Resources and References

6.1 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 21. 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).
- 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	Today's Date	End of last month
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	Data 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	Data 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		

6.2 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.[11]

RESOURCE TYPE	SOURCE	TITLE	LINK	DESCRIPTION
Best Practices	Microsoft	Tips for Creating Strong Passwords	http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password	Provides tips for creating and maintaining strong passwords.
Best Practices	NIST	Small Business Information Security: The Fundamentals	https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final	This report assists small business management to understand how to provide basic security for their information, systems and networks.
Best Practices	Pennsylvania Public Utility Commission	Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities	http://www.puc.pa.gov/general/pdf/Cybersecurity_Best_Practices_Booklet.pdf	The guide outlines red flags to look for and ways to prevent identity or property theft; how to manage vendors and contractors who may have access to a company's data; what to know about antivirus software, firewalls and network infrastructure; how to protect physical assets, such as a computer in a remote location or a misplaced employee device; how to respond to a cyber attack and preserve forensic information after the fact; and how to report incidents.

[11] This resource listing was originally created by the CSRIC IV WG4 Small and Mid-Size Business Feeder Group. The listings, including the hyperlinks, were updated when this guide was published in September 2018.

Best Practices	Center for Internet Security (CIS)	CIS	https://www.cisecurity.org/	Cybersecurity tools and best practices, including the CIS Top 20 Controls.
Network Protection Tool	Open Source	Network Mapper (Nmap)	http://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	http://www.metasploit.com/	World's most used penetration testing software; Put your network's defenses to the test – A collaboration of the open source community and Rapid7. Our penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments
Network Protection Tool	Sourcefire	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	NIST	Contingency Planning Guide for Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf	Provides instructions, recommendations, and considerations for creating a contingency plan that is used by government agencies, but can be applied to any company/industry.
Planning Guide	NIST	Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf	This document assists organizations in establishing computer security incident response capabilities and handling incidents.
Planning Guide	DHS	Business Continuity Planning Suite	https://www.ready.gov/business-continuity-planning-suite	Developed by DHS' National Protection and Programs Directorate and FEMA, 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.
Resource List	U.S. Department of Homeland Security (DHS)	Stop. Think. Connect. Tips and Resources	http://www.dhs.gov/stopthinkconnect-get-informed	Materials that can be used to increase cybersecurity awareness.
Resource List	Multi-State Information Sharing & Analysis Center (MS-ISAC)	MS-ISAC Cyber Security Toolkit	http://msisac.cisecurity.org/resources/toolkit/oct14/	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	United States Computer Emergency Readiness Team (US-CERT)	Resources for Small and Midsize Businesses	https://www.us-cert.gov/ccubedvp/smb	Resources provided by the DHS Critical Infrastructure Cyber Community (C^3) to help small and midsize businesses recognize and address their cybersecurity risks.
Resource List	US-CERT	Publications	https://www.us-cert.gov/security-publications/	Various publications to help a user, from setting up a computer to emerging threats.
Self-Service Tool	FCC	FCC Cybersecurity Planning Guide	http://transition.fcc.gov/cyber/cyberplanner.pdf	A tool for small businesses to create customized cybersecurity planning guides.
Self-Service Tool	FCC	FCC Small Biz Cyber Planner 2.0	http://www.fcc.gov/cyberplanner	Online resource to help small businesses create customized cybersecurity plans.
Self-Service Tool	U.S. Small Business Administration (SBA)	Cybersecurity for Small Businesses	http://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses	This self-paced training exercise provides an introduction to securing information in a small business.
Self-Service Tool	(US-CERT)	Cyber Resilience Review (CRR)	https://www.us-cert.gov/ccubedvp/self-service-crr	The CRR is a no-cost, voluntary, nontechnical assessment to evaluate an organization's operational resilience and cybersecurity practices. This site also provides a link to self-assessment tool.
Self-Service 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.

Standards	Payment Card Industry (PCI) Security Standards Council	PCI Security Standards	https://www.pcisecuritystandards.org/security_standards/getting_started.php	PCI security for merchants and payment card processors are the vital result of applying the information security best practices in the Payment Card Industry Data Security Standard (PCI DSS). The standard includes 12 requirements for any business that stores, processes or transmits payment cardholder data.
Training	Federal Emergency Management Agency (FEMA)	Cyberterrorism Defense Initiative	http://cyberterrorismcenter.org/	The Cyberterrorism Defense Initiative (CDI) is a national counter-cyberterrorism training program, developed for technical personnel and managers who monitor and protect our nation's critical cyber infrastructures. Classes are held in easily accessible and centralized locations throughout the United States.
Training	InfraGard	The Center for Information Security Awareness	https://www.infragard.org/	Infragard provides free online security awareness and PCI employee training for individuals and companies. In addition, InfraGard provides a forum for public-private partnership and information sharing regarding physical and cyber threats and best practices.
Training	MS-ISAC	Cybersecurity Awareness Free Training and Webcasts	http://msisac.cisecurity.org/resources/videos/free-training.cfm	A collection of cybersecurity training websites and podcasts links.
Training	SANS	Webcasts	https://www.sans.org/webcasts/	SANS Information Security Webcasts are live web broadcasts combining knowledgeable speakers with presentation slides. SANS offers several types of webcasts designed to provide valuable information and enhance your security education.

Training	Texas A&M Engineering	Web-based Training	https://teex.org/Pages/Program.aspx?catID=667&courseTitle=Online+Training	The TEEX/NERRTC Cybersecurity web-based courses are designed to ensure that the privacy, reliability and integrity of the information systems that power our global economy remain intact and secure. These DHS/FEMA-certified courses are offered through three discipline-specific tracks targeting general, nontechnical computer users, technical IT professionals, and business managers and professionals.
Training	US-CERT	CERT Podcast Series	http://cert.org/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.