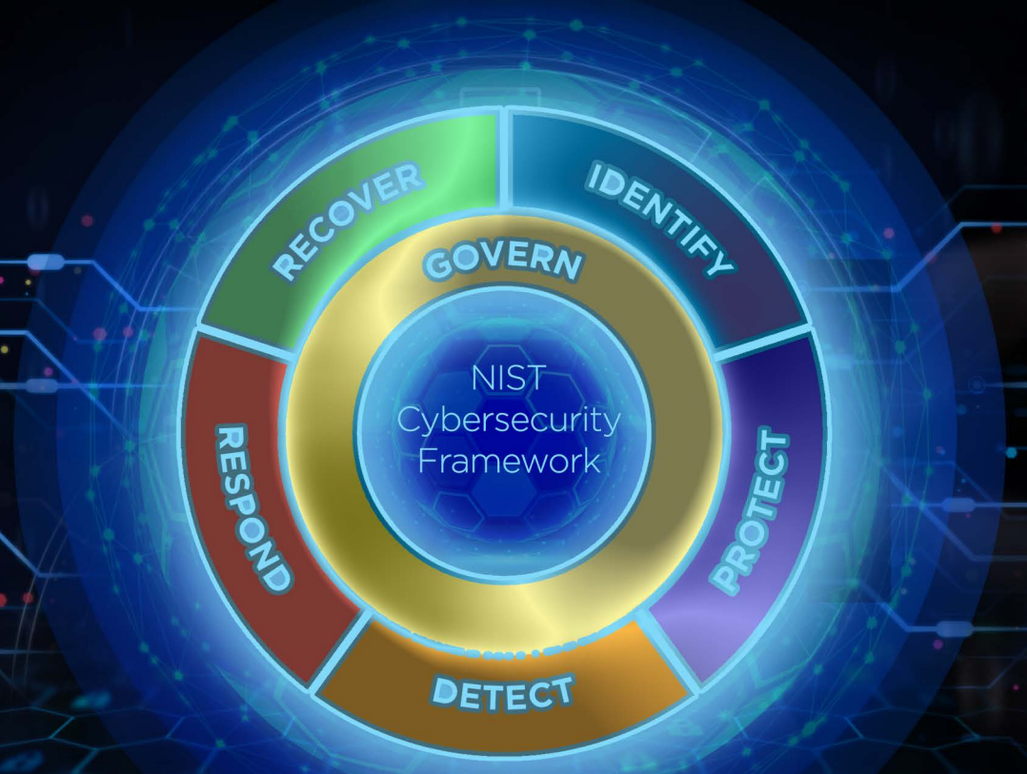
NTCA CYBERSECURITY SERIES

(Part 2)

Sector-Specific Guidance to the NIST Cybersecurity Framework



NTCA THE RURAL BROADBAND ASSOCIATION®

#BeCyberwise

TABLE OF CONTENTS

INTRODUCTION

The 2021 NTCA Cybersecurity Series includes the "Sector-Specific Guidance to the NIST Cybersecurity Framework" as a resource for your cyber risk management team to consider as they review Version 1.1 of the National Institute of Standards and Technology (NIST) Cybersecurity Framework—a voluntary framework based on existing standards, guidelines and practices for reducing cyber risks to critical infrastructure.

Given the dynamic and evolving nature of cyberthreats, cybersecurity resilience is best approached from a risk/benefit analysis. The "Framework for Improving Critical Infrastructure Cybersecurity" (the NIST Cybersecurity Framework) helps successfully accommodate your environment, risk tolerance and unique needs.[1] 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 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 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.

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 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 was created to assist all 16 critical infrastructure sectors,[3] 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. 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[4] provide communications companies with substantive guidance on how to use the framework to mitigate cyber threats to their communications networks, infrastructure and sensitive data.

Subsequent to the release of the EO, the Cybersecurity Enhancement Act of 2014[5] 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,[6] which includes additional best practices beyond the original Version 1.0 release.

In the winter of 2020, NTCA–The Rural Broadband Association (NTCA) convened a Member Advisory Group to reevaluate Version 1.1 of the NIST Cybersecurity Framework and update our previous guidance. This update reflects the evolving cybersecurity needs of small network service providers and the experience of our members with the NIST Framework.

OBJECTIVE, SCOPE AND METHODOLOGY

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).

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[7] 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., should the framework be applied to 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," see page 19.

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 prioritized the framework subcategories into high-priority, mid-priority and low-priority listings or "profiles."[8] 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.

The high priority/first-step profile included below contains 36 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 67 subcategories, while the low-priority or third-step profile contains five best practices.

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.

GUIDANCE TO 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, 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 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.

HIGH PRIORITIES 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.AM-4: External information systems are catalogued
ID.GV-1: Organizational cybersecurity policy is established and communicated
ID.GV-4: Governance and risk management processes address cybersecurity risks
ID.RA-1: Asset vulnerabilities are identified and documented
ID.RA-5: Threats, vulnerabilities, likelihoods and impacts are used to determine risk
ID.RM-1: Risk management processes are established, managed and agreed to by organizational stakeholders
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.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
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-1: All users are informed and trained
PR.AT-2: Privileged users understand their roles and responsibilities
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities

HIGH PRIORITIES OR FIRST STEPS
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.MA-2: Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access
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.CM-1: The network is monitored to detect potential cybersecurity events
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
DE.CM-4: Malicious code is detected
DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed
DE.CM-8: Vulnerability scans are performed
DE.DP-2: Detection activities comply with all applicable requirements
RS.RP-1: Response plan is executed during or after an incident
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.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 PRIORITIES OR SECOND STEPS
ID.AM-3: Organizational communication and data flows are mapped
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.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-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources
ID.RA-3: Threats, both internal and external, are identified and documented
ID.RA-4: Potential business impacts and likelihoods are identified

MID PRIORITIES OR SECOND STEPS
ID.RA-6: Risk responses are identified and prioritized
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.
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.AT-4: Senior executives understand their roles and responsibilities
PR.DS-3: Assets are formally managed throughout removal, transfers and disposition
PR.DS-4: Adequate capacity to ensure availability is maintained
PR.DS-5: Protections against data leaks are implemented
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware and information integrity
PR.DS-7: The development and testing environment(s) are separate from the production environment
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-2: A System Development Life Cycle to manage systems is implemented
PR.IP-3: Configuration change control processes are in place
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-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
PR.IP-10: Response and recovery plans are tested
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
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
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
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

MID PRIORITIES OR SECOND STEPS
DE.AE-4: Impact of events is determined
DE.AE-5: Incident alert thresholds are established
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
DE.CM-5: Unauthorized mobile code is detected
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
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-2: Incidents are reported consistent with established criteria
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.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
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
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 PRIORITIES OR THIRD STEPS
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.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

CASE STUDY

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 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 cyberattacks.

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 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. We recommend tools that can gather this type of 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 addressed from the open internet will have the highest risk of exposure to a cybersecurity incident (more information can be found in ID.AM-4). 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-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, 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 20 includes a sample device inventory listing with examples of devices and ideas for how to organize, classify and track them.

ID.AM-4: External information systems are catalogued

After you have completed the inventory functions in ID.AM-1 and ID.AM-2, it is time to fully catalogue external information systems. This is to ensure the organization knows where its external data resides and to identify the associated risks. This is where the cloud portion of the Identify function comes into play. 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.GV-1: Organizational cybersecurity policy is established and communicated

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 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.GV-4: Governance and risk management processes address cybersecurity risks

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 it 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.

D.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. 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.

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

After you have identified and documented vulnerabilities in step ID.RA-1, 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 doesn't indicate the risk it poses to you. To ensure you give the appropriate attention to the items that are most likely to cause you headaches, consider analyzing whether vulnerabilities are currently being used 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 vulnerabilities, as they are likely to have automated exploits that are widely published.

ID.RM-1: Risk management processes are established, managed 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 tolerance, the way that risks and potential risk prevention 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 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.

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, 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 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. 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.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 a cyberattack if improperly configured, secured or monitored. 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.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)

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.

PR.AC-6: Identities are proofed and bound to credentials and asserted in 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.AC-6 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.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)

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 is the single factor, username and password both of which are something you know. You can increase the authentication steps for users by adding a smart card or fingerprint. These can both 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.AC-6 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.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 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-2: Privileged users understand their roles and responsibilities

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.

PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities

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.

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 rules about removing data from the network in their cybersecurity policy 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 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.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 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.

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 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.PT-4: Communications and control networks are protected

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.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. 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.

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. 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-4.

DE.CM-2: The physical environment is monitored to detect potential cybersecurity 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 man 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.

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-7: Monitoring for unauthorized personnel, connections, devices and software is performed

Just as the Identify step of the framework is necessary in order 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 CM-7, 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 CM-7, 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. However, each of the CM-7 goals can be monitored directly at the potential attack surface once a baseline and event triggers have been established.

- 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.

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.

DE.DP-2: Detection activities comply with all applicable requirements

The core of this subcategory is to understand required legal obligations. These obligations could originate from any combination of federal, state, contractual and/or any other regulatory entity. Sometimes these will spell out what is required, sometimes not. Considerations should be given to PCI, DoD contracts, CPNI, etc. You will find many of these have overlapping requirements.

You will also have specific requirements in your business. Identify your most valuable sources of data and critical infrastructure and plan to protect it.

Once the requirements have been determined, a plan can be developed. This plan can include log monitoring, IDS/IPS logs, DNS query analysis, results from antivirus scans, etc. Depending on the size and budget of the business, outsourcing security services may be the most effective use of resources.

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. For example, it can include 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-1: Personnel know their roles and order of operations when a response is needed

Items to include in your Incident Response Plan (IRP):

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

The IRP should also be practiced with tabletop exercises. 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-3: Information is shared consistent with response plans

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 may want to consider consulting legal counsel before the information is released. Each organization should have a designated person responsible for sharing information internally and externally.

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

During the creation of an IRP (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. 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 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 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-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.

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.)
Jeff Walker	Pioneer Communications (Ulysses, Kan.)
Eric Wilkens	Arvig (Perham, Minn.)
Roxanna Barboza	NTCA–The Rural Broadband Association

ADDITIONAL RESOURCES AND REFERENCES

NIST FRAMEWORK EVALUATION TOOL

The "NIST Framework Evaluation Tool" is a more robust resource or a high-speed road map that references all 108 of the subcategories contained within the NIST Cybersecurity Framework to help your team evaluate your company's cybersecurity program at a more granular and sophisticated level.

This "NIST Framework Evaluation Tool" includes light blue columns, which delineate the functions, categories, subcategories and informative references that are inherent components of the NIST Cybersecurity Framework. The dark blue 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.

Download the NIST Framework Evaluation Tool

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 20 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)	Choosing and Protecting Passwords	https://us-cert.cisa.gov/ncas/tips/ST04-002#:~:text=Use%20different%20passwords%20on%20different,keep%20track%20of%20your%20passwords	Provides tips for creating and protecting strong passwords.
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.
Best Practices	Pennsylvania Public Utility Commission	Cyber Best Practices for Small and Medium Pennsylvania Utilities	https://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 cyberattack and preserve forensic information after the fact; and how to report incidents.
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.ntca.org/member-services/cybershare	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.
Forums	DHS	U.S. Computer Readiness Team (US-Cert)	https://us-cert.cisa.gov/	US-Cert distributes cyber vulnerability and threat information on a regular basis, often several times per week, for free to subscribers.

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	NIST	Telework Security Overview & Tip Guide	**https://www.nist.gov/system/files/documents/2020/03/18/Telework%20Overview%20and%20Tips.pdf**	Basic tips to improve your telework security.

RESOURCE TYPE	SOURCE	TITLE	LINK	DESCRIPTION
Resource List	NTCA	Cybersecurity Information and Resources	**https://www.ntca.org/advocacy/issues/consumer-protection-network-reliability/cybersecurity**	In response to members' needs, NTCA's cybersecurity webpage provides resources to combat cybersecurity threats.
Resource List	CISA	Stop. Think. Connect. Toolkit	**https://www.cisa.gov/publication/stop-think-connect-toolkit**	Materials that can be used to increase cybersecurity awareness.
Resource List	FCC	Cybersecurity for Small Business	**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	United States Computer Emergency Readiness Team (US-CERT)	Resources for Small and Midsize Businesses	**https://us-cert.cisa.gov/resources/smb**	Resources provided by the DHS Critical Infrastructure Cyber Community (C3) to help small and midsize businesses recognize and address their cybersecurity risks.
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.
Self-Service Tool	CISA	Assessments: Cyber Resilience Review (CRR)	**https://us-cert.cisa.gov/resources/assessments**	The CRR downloadable resources are a no-cost, voluntary, nontechnical way to evaluate an organization's operational resilience and cybersecurity practices.
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.

RESOURCE TYPE	SOURCE	TITLE	LINK	DESCRIPTION
Standards	Payment Card Industry (PCI) Security Standards Council	Maintaining Payment Security	**https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security**	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	CISA	Cybersecurity Training & Exercises	**https://www.cisa.gov/cybersecurity-training-exercises**	A collection of cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation.
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/program/nerrtc-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	**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.

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

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

[4] 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**.

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

[6] 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**.

[7] 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.

[8] 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.