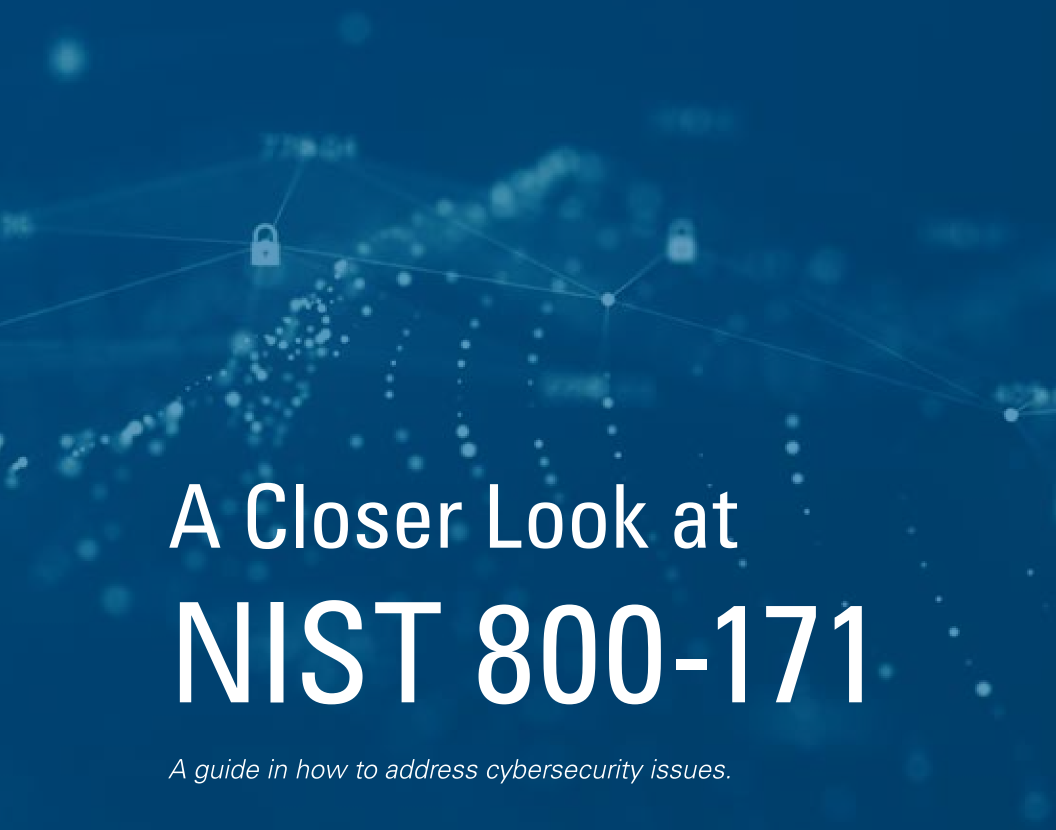
NCMEP



A Closer Look at NIST 800-171

A guide in how to address cybersecurity issues.

A Closer Look at

NIST 800-171

A guide in how to address cybersecurity issues.

This e-book is a compilation of 14 blog posts by Katherine Bennett, Manager, Instructional Design at NC State Industry Expansion Solutions.

NCMEP™
North Carolina
Manufacturing Extension Partnership

The North Carolina Manufacturing Extension Partnership (NCMEP) provides manufacturing extension services that enhance the productivity, innovative capacity and technological performance of North Carolina based manufacturing firms. We also work to strengthen the global competitiveness of small- and medium-sized manufacturers.

Published November 2019; BR-1119-0015.00

Contents

RESOURCES

What is NIST 800-171?

NIST 800-171 defines how to protect data, information and materials. NIST 800-171 was originally adopted as the minimum standards required to meet for compliance to the Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity clause. The DFARS cybersecurity clause impacts all Department of Defense (DoD) contractors, both prime and subcontractors. Though NIST 800-171 is the standard adopted by the DoD, its use goes far beyond DoD contractors—to all federal contractors and even to all businesses and manufacturers.

The set of standards is officially named the National Institute of Standards and Technology Special Publication 800-171. It targets the protection of Controlled Unclassified Information in Non-Federal Information Systems and Organizations. So, what does that mean?

Controlled Unclassified Information (CUI) is any information that is not deemed “classified” but used while working on a federally funded project. This can be any data or information that you research, discover, or otherwise put to use while working on a federally funded project. Even though this information may not be classified, it is still an asset to be protected.

The standards within NIST 800-171 provide guidance to all businesses and manufacturers who are seeking guidance and direction in how to address cybersecurity issues. The protections that these standards put in place help protect all assets not just CUI.

The standards contained in NIST 800-171 are divided into 14 families. These families are:

1. Access Control: This area addresses who you authorize to view/access to your assets.
2. Awareness and Training: This area looks into how employees, contractors or others on your site/network, are educated on your cybersecurity policy and procedures.
3. Audit and Accountability: This area goes into your

record keeping of access to your systems and ability to identify violations.

4. Configuration Management: This area covers your existing network protocols and safety procedures.

5. Identification and Authentication: This area goes beyond Access Control to look in detail at how authorized users are verified before gaining access to the systems.

6. Incident Response: This area addresses your processes that are triggered when a cybersecurity threat or breach occurs.

7. Maintenance: This area looks at your maintenance turnaround time and responsible staff.

8. Media Protection: This area goes over how you backup and store information as well as who has access to backups.

9. Physical Protection: This area delves into who has physical access to your equipment and storage.

10. Personnel Security: This area addresses any screening process you have in place for employees, contractors, and others who access your systems.

11. Risk Assessment: This area goes over your proactive testing of systems and processes.

12. Security Assessment: This area addressed the effectiveness of your processes and procedures.

13. System and Communications Protection: This area looks at your ability to monitor the exchange of information within your systems.

14. System and Information Integrity: This area looks at how fast your turnaround time is for detected threats.

NIST 800-171 compliance can help you showcase your cybersecurity preparedness for working within your supply chain or on a federal contract. The DoD has already made NIST 800-171 compliance a requirement. Other federal agencies are expected to follow. Even if you are not a federal contractor or sub-contractor, use NIST 800-171 to help get ahead of the competition and solidify your spot in the supply chain!

[FAMILY 1]

A Closer Look at NIST 800-171:

The Access Control Family

The first of the fourteen families within the NIST 800-171 standard is Access Control. This family is all about who you authorize to view or access your assets and controlling how they are allowed to access your system.

WHY IS ACCESS CONTROL IMPORTANT?

All of us have assets that, if compromised, would result in a loss to our businesses. We also have information that we share publicly and freely. On websites and social media we share information about our mission, our staff, our products or services, and even some of our clients. But, we would never share our staff members' social security numbers, our intellectual property, our detailed operating procedures, or our schematics in a public area where anyone and everyone can access it. Instead, we control who within our organization is authorized to view such information.

WHAT IS ACCESS CONTROL ABOUT IN NIST 800-171?

There are 22 requirements within Access Control family, making it the densest family within the standard. The main focus of this family is to limit system access to only trusted users and devices. Some key points addressed within this family are:

1. Limit access to systems to authorized users–authorized users (employees, contractors, etc.) are assigned system accounts and system role. No users without assigned account login credentials are allowed to access the system.
2. Tailor access to job role and duties–assigned system roles or permissions should mirror the job requirements for the individual. For example, perhaps only financial personnel should be able to access budget workbooks and therefore access to these files would be denied for other job roles.
3. Restrict access to admin functions–assign edit or modify permissions only to those authorized users who actually make the changes. View permission can

be shared with others as needed.

4. Control remote access to your systems–establish requirements and restrictions for remote access including the levels of access that are permitted to authorized users while they are using remote access.

5. Control wireless and mobile device access to your systems–establish wireless and mobile device guidelines and restrictions. Verify and permit only trusted devices operated by authorized users.

[FAMILY 2]

A Closer Look at NIST 800-171:

The Awareness and Training Family

The Awareness and Training family is the second family of requirements in the NIST 800-171 standard. This family covers the requirements that address how employees, contractors, or others on your IT system are educated on your cybersecurity policy and procedures.

WHY IS AWARENESS AND TRAINING IMPORTANT?

Cyber attackers are always looking to exploit any weakness in our networks and systems. And, when it comes to cybersecurity, it is us humans who are the greatest weakness. We are the ones who will click on an infected link in a phishing email; we are the ones who will find a USB memory stick in the parking lot and plug it into our computers; we are the ones who will use the sticky note on the monitor system to remember our passwords. So, we are the ones who can unintentionally let an attack through. However, with upfront and regular training, we can also learn and adapt to become cyber-aware vigilants!

WHAT IS AWARENESS AND TRAINING ABOUT IN NIST 800-171?

There are only three requirements in the Awareness and Training family but, don’t let that number distract you from the importance of this family. The main focus of this family is to keep employee cybersecurity education a priority. Key points addressed within this family are:

1. Make all employees aware of the security risks of their actions–provide training during onboarding to introduce your company cybersecurity policy and provide an overview of good cybersecurity habits.

2. Keep all employees aware of your cybersecurity policies and procedures–hold refresher training or share materials throughout the year.

3. Include cybersecurity training as an ongoing part of your strategic planning–cybersecurity risks grow each year and so your employee education will need to be updated, too.

[FAMILY 3]

A Closer Look at NIST 800-171:

The Audit and Accountability Family

The third family addressed in the NIST 800-171 standard is Audit and Accountability. This family focuses on your record keeping of access to your IT systems and your ability to identify any unauthorized access.

WHY IS AUDIT AND ACCOUNTABILITY IMPORTANT?

We all have to create, store, and maintain data. But, we have to do this securely and protect the data that is kept in our system. Much of our data is valuable and if it fell into the wrong hands, could lead to a serious cybersecurity breach that could compromise our business, our employees, our clients and others in our supply chain. So, we have to have the ability to protect information from unauthorized access and hold those with authorized access accountable for their actions when working with our data.

WHAT IS AUDIT AND ACCOUNTABILITY ABOUT IN NIST 800-171?

There are nine security requirements in the Audit and Accountability family. The primary purpose of this family is to address your record keeping of access to your systems and your ability to identify violations. A few key points addressed in this family are:

1. Create and store records to document any unauthorized activity–any attempt made to access protected information by users who do not have authorized credentials should be documented.
2. Maintain the ability to trace actions on the network to identified users–authorized user actions in protected areas should be able to be tracked with the ability to identify which users performed specific actions.
3. Analyze records that may be kept by varied departments to build organization-wide awareness–individual departments should not act in silos but should share record analyses so that the entire organization can benefit and adjust policy or procedures accordingly.

4. Protect audit information from unauthorized access–restrict access to audit information to a specific subset of authorized users and limit actions such as the ability to edit or delete to an even smaller subset of authorized users.

[FAMILY 4]

A Closer Look at NIST 800-171:

The Configuration Management Family

The Configuration Management family is the fourth family in the NIST 800-171 standard. This family focuses on the requirements that surround your existing network protocols and safety procedures.

WHY IS CONFIGURATION MANAGEMENT IMPORTANT?

In order for us to best protect our IT systems and network, we have to know what is included in our system. What servers do we have? How many computers are connected?

Do we have printers, copiers, webcams, or other hardware connected? Do we allow mobile devices to connect to our system? We need to identify and control the hardware and software that is installed and maintained on our system. If we do not know what is on our system then we cannot control what or who may be able to access it and the data we store. Knowing our system configuration keeps us aware of the different points of access to our system and helps us to better be able to protect these points of access from becoming points of vulnerability that would expose us to higher cybersecurity risk.

WHAT IS CONFIGURATION MANAGEMENT ABOUT IN NIST 800-171?

The Configuration Management family contains nine security requirements. Some of the main points that are addressed by these requirements include:

1. Establish, document, and maintain baseline configurations for your systems–identify your current system configuration and establish baseline security settings for devices and authorized access to modify these settings. Make sure that your configuration and settings are documented and trackable.

2. Keep your technology device inventory up to date–Update your inventory to document any added or removed devices. Devices that are added to your system should have your baseline security settings in place. Devices that are removed from your system

should be properly disposed of such that they are no longer able to access your system.

3. Keep your software and firmware updated and patched–Regularly check for and apply software updates and firmware (hardware) patches. Out-of-date or unpatched software or firmware create vulnerabilities in your system.

4. Track, review, and document changes to the configuration of your system–Update your system configuration when any new device or software is added, when any devices or software are retired, and when any modification to settings or documentation is made. Make sure that each change is documented.

5. Monitor and control software installed by employees–Protect the integrity of your system by controlling who is allowed to install software. Software that installed without your knowledge results in a change to your IT system. And, that will lead to unknown threats that you may be unable to detect.

[FAMILY 5]

A Closer Look at NIST 800-171:

The Identification and Authentication Family

The fifth family of requirements in the NIST 800-171 standard is Identification and Authentication. This family covers how your authorized users are verified before they gain access to your system.

WHY IS IDENTIFICATION AND AUTHENTICATION IMPORTANT?

It is not enough for us to control who can access our data and systems. We also have to put in cybersecurity safeguards to ensure the people we allow in are indeed who they say they are. I may have a policy in place that allows only current employees within my organization to access a staff portal that contains restricted data. But, how can I know that the people entering the staff portal are indeed current employees? For that, we need to be able to verify identities and establish policies and procedures around how people are verified before they can get into our systems.

WHAT IS IDENTIFICATION AND AUTHENTICATION ABOUT IN NIST 800-171?

The Identification and Authentication family contains eleven security requirements. The main focus of this family is verifying that the people who are accessing your systems are the ones authorized to do so. Some of the key points within this family include:

1. Verify the identity of any person or device accessing your system—ensure that the system login information matches a known authorized user and that any devices that access your system can be traced to an assigned and authorized user.

2. Enforce minimum complexity protocols for passwords—help your authorized users keep their passwords secure by including a password policy. Password complexity protocols establish how long passwords should be and if numerals, uppercase letters, or special characters (!, @, *, etc.) are required.

3. Use multifactor authentication for network access—

enable at least a two-factor authentication which requires another authentication tool in addition to the login and password. This may either be through a numeric code sent to a user's mobile device or a fingerprint scanner.

4. Set access time-out to disable access after a period of account inactivity—set a session time-out that will automatically close a network connection after a specified time. This will prevent a user from keeping an open connection to your data unless they are actively working in the system.

[FAMILY 6]

A Closer Look at NIST 800-171:

The Incident Response Family

Incident Response is the sixth family in the NIST 800-171 standard. This family is all about the processes that are triggered when a cybersecurity threat or breach occurs.

WHY IS INCIDENT RESPONSE IMPORTANT?

An incident response plan is a guide you develop so your management team and employees, at all levels, will know what steps to take when managing a potential cybersecurity breach. This plan is equally important to having cybersecurity protections in place. While we need to protect data we also need to be prepared with a plan for what to do if that data is breached.

WHAT IS INCIDENT RESPONSE ABOUT IN NIST 800-171?

There are only three controls in the Incident Response family. Although there are only three controls, remember that the incident response plan is a critical element in your cybersecurity preparedness. The controls within the Incident Response family focus on the development, implementation and testing of your incident response plan.

1. Develop an incident response plan—Include the maximum allowed turnaround time for responding to threats. Assign roles to members of your organization: who will report the breach and to whom? Who will confirm and analyze the breach? Who will fix the problem? Who will record the breach?

2. Track, document and report incidents both internally and externally to appropriate officials—Identify the appropriate internal and external contacts in your incident response plan. Maintain records of all detected breaches included the initial date of breach, date of reporting the breach, analysis and date of recovery.

3. Test incident response procedures—As part of your emergency planning, include a test of your incident response procedures. Define the frequency of testing in your incident response plan. Keep a record of these tests.

[FAMILY 7]

A Closer Look at NIST 800-171:

The Maintenance Family

The seventh family in the NIST 800-171 standard is the Maintenance family. This family addresses your maintenance turnaround time and responsible staff.

WHY IS MAINTENANCE IMPORTANT?

Maintenance is a crucial part in protecting your systems from a cybersecurity threat. Without regularly scheduled maintenance, your systems' protections are neglected and quickly become outdated. This can lead to exposed weaknesses in the systems that will allow a threat through. Depending on the state of neglect, that threat may even go undetected while causing irreparable damage and loss of data. Regular maintenance performed by authorized personnel following proper procedures can greatly improve your cybersecurity preparedness.

WHAT IS MAINTENANCE ABOUT IN NIST 800-171?

The Maintenance family contains six controls. The primary focus of this area is to ensure that you have a systems' maintenance plan that includes identified personnel and procedures for maintenance. Some of the main focus areas include:

1. Schedule, perform and document maintenance and repairs—Develop a maintenance plan that covers the maintenance tools, techniques, mechanisms, and personnel allowed. Keep a regular maintenance schedule and make sure it is followed. Also, keep a record of both regularly scheduled maintenance and emergency repairs.
2. Maintain a list of authorized maintenance personnel—Document who is allowed to serve in a maintenance capacity. These individuals should also have authorized access on your systems.
3. Supervise maintenance activities performed by third parties—Make sure that the list of authorized maintenance personnel is available to your staff and identify employees who are responsible for escorting any third party service providers who are supervised throughout the times of service.

[FAMILY 8]

A Closer Look at NIST 800-171:

The Media Protection Family

The eighth family in the NIST 800-171 standard is the Media Protection family. This family is about how you backup and store information as well as who has access to your backups.

WHY IS MEDIA PROTECTION IMPORTANT?

Media protection includes print and digital content. You want to know that your media content and communications are secure at all times. Portable flash drives, remote access and even email can make it a challenge to track the transportation of media. Having media protection written into your cybersecurity policy will clearly outline who has the authority to access and share media, which devices are allowed to store and transport media, and how to properly destroy media when it has expired. Media will also include Controlled Unclassified Information (CUI) for those working with government contracts. Controlled Unclassified Information "requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies." (U.S. National Archives and Records Administration) CUI Policy and Guidance can be found on the National Archives website.

WHAT IS MEDIA PROTECTION ABOUT IN NIST 800-171?

The Media Protection family contains nine controls. These controls are primarily focused on the security of media storage including who can access the stored content, how transportation is controlledand the safe use of storage devices. Some of the key points addressed in this family are:

1. Securely store paper and digital content—Store print and digital media content in a restricted and protected area. This may a physical locked cabinet or secure server.

2. Limit access to protected information to authorized users—Restrict access to only authorized users on your system. For physical storage areas, keys, key cards or other locks should be in place. For digital storage areas, two-factor authentication should be

implemented.

3. Mark content with CUI markings as needed—All Controlled Unclassified Information should follow the CUI marking guidelines.

4. Control the transport and sharing of protected information—Only authorized personnel using authorized devices should be allowed to transport or share protected content. Any media that has expired the storage date requirements must be properly destroyed.

5. Prohibit the use of portable storage devices unless assigned to an authorized user—Only devices with known and identifiable authorized users should be permitted to access your system, store data or transport data.

[FAMILY 9]

A Closer Look at NIST 800-171:

The Physical Protection Family

The Physical Protection family is the ninth family in the NIST 800-171 standard. This family focuses on who has physical access to your equipment and storage.

WHY IS PHYSICAL PROTECTION IMPORTANT?

A true cybersecurity plan must also include a physical element. Firewalls, anti-virus programs, password protections, two-factor authentication and other policies and procedures are entirely ineffective if someone can just walk into your server room and access your controls. A person who can gain direct access to either your server or a connected device, can use keyloggers, encryption devices, malicious code on a flash drive, and more to get access to your data or lock you out. If they can get into the server room, they can even take your drives right out the door with them. So, it is not enough to block attackers on the digital front, you must also be prepared with a physical protection plan.

WHAT IS PHYSICAL PROTECTION ABOUT IN NIST 800-171?

The Physical Protection family contains six controls. The primary focus of this family is on controlling access to the physical locations of your equipment and storage. Some of the areas addressed include:

1. Limit access to IT equipment and backups to authorized personnel—Maintain a list of personnel who are authorized to access your equipment and make sure that list is accessible to anyone is able to grant access.

2. Monitor physical access to servers and network controls—Anyone working in the server area should have authorization. In the case of third party contractors, authorization and direct supervision by an authorized employee is needed.

3. Escort visitors and monitor visitor activity—All guests and visitors should be escorted while on site. Ensure

that their movements are monitored and known.

4. Secure keys, combinations, badges and other methods of physical access—Make sure to keep access points secure by also securing access to keys, employee badges, and passcodes. Make all employees aware of their responsibilities in securing their badges and keys as a part of your physical security plan.

[FAMILY 10]

A Closer Look at NIST 800-171:

The Personnel Security Family

The Personnel Security family is the tenth family in the NIST 800-171 standard. This family addresses your screening processes that are in place for employees, contractors and others who access your systems.

WHY IS PERSONNEL SECURITY IMPORTANT?

Much of our ability to build and maintain a secure system is based on the people that we choose to trust. Employees, contractors, third-party vendors and others in our supply chain are trusted with access to our systems. We must make sure that people are trustworthy and aware of our cybersecurity policies and procedures. We also need to ensure that each person who has access to our system has the correct level of access to perform their necessary job functions. If an individual has a higher level of access than is required, they may be able to harm the system with or without intention. We also need to remove access during the off-boarding process. A terminated or disgruntled employee who maintains access to our system can destroy, steal or block access to our assets.

WHAT IS PERSONNEL SECURITY ABOUT IN NIST 800-171?

The Personnel Security family consists of only two controls. The focus of this family is on screening and access authorization policies for employees, contractors and others who should have access to your systems. The key points in this family are:

1. Screening prior to authorizing access—Include a background check and other standard screening processes before granting anyone access to your systems. This is typically done pre-hire, during onboarding or prior to a contract award. Screening should also be ongoing.

2. Terminating access during off-boarding processes—terminate access or authorization immediately upon an employee exit or contract end.

3. Modifying access authorizations based on need—regularly assess access authorizations needs for employees and contractors. Make necessary modifications that may arise due to any change in assignment or transfer.

[FAMILY 11]

A Closer Look at NIST 800-171:

The Risk Assessment Family

The Risk Assessment family is the eleventh family in the NIST 800-171 standard. This family addresses the proactive testing of systems and processes.

WHY IS RISK ASSESSMENT IMPORTANT?

Sure, cybersecurity is important to our business. But, what is it that we need to protect? What controls do we put in place to protect it? Where might a threat come from? What is the worse case scenario for our businesses and bottom lines? What happens if our risk factors change?

Risk assessments help answer these questions and more. Performing risk assessments allow us to identify the proper controls to put in place to protect our assets from likely threats. Through risk assessments, we can determine how best to strengthen our areas of vulnerability. By scheduling regular recurring risk assessments, we can also be more agile in our ability to adapt as system vulnerabilities and threats change.

WHAT IS RISK ASSESSMENT ABOUT IN NIST 800-171?

There are three controls in the Risk Assessment family. The main focus of this family is on your ability to perform regular, recurring risk assessments. Risk assessment in the NIST 800-171 standard includes:

1. Regularly conducting a risk assessment—Perform regularly scheduled risk assessments for your operations and individuals, protected assets, backup and storage, and communication procedures. Include the likelihood of threat in these areas and the extent of harm that could be caused if an attack or loss of data were to occur.

2. Documenting risk assessment results—Review the results of your risk assessments. Document and share the results with key personnel across your organization. Results should not be 'siloed' by division.

3. Updating risk assessments for significant changes to your systems and operations—Whenever there is a

significant change in your operations or IT system, a new threat is identified, or your security is otherwise impacted, make sure to update your risk assessment. Updates should be timely, documented and shared with key personnel.

[FAMILY 12]

A Closer Look at NIST 800-171:

The Security Assessment Family

The twelfth family in the NIST 800-171 standard is Security Assessment. This family addresses the effectiveness of your cybersecurity processes and procedures.

WHY IS SECURITY ASSESSMENT IMPORTANT?

Cybersecurity threats change over time. We must be ready to adapt and update our security processes and procedures. A security plan that works for us today will not be the final solution for all time. It is important to test the effectiveness of our security plan through security assessments. Security assessments should be regularly performed to test our security controls, how well threats are identified and how quickly we are able to respond to threats. Through these assessments, we can identify weaknesses in our process and procedures and take the steps necessary to improve our security plan.

WHAT IS SECURITY ASSESSMENT ABOUT IN NIST 800-171?

The main focus of this family is on continuous improvement of your security plan. The key points within the Security Assessment family are:

1. Develop a security assessment plan—define how security controls will be assessed and by whom. Ensure that testing is done to meet the most up-to-date security requirements. Maintain documentation of the testing parameters, dates and results.

2. Develop a plan of action for correcting any weaknesses found— a plan of action to correct weaknesses should include milestones to document progress. Update the plan of action regularly to reflect completion of outcomes.

3. Continuously monitor security controls—the process of security assessment is ongoing; to ensure the greatest level of effectiveness of security controls, monitor them on an ongoing basis.

[FAMILY 13]

A Closer Look at NIST 800-171:

The System and Communication Protection Family

System and Communication Protection is the thirteenth family in the NIST 800-171 standard. This family focuses on your ability to monitor the exchange of information in your systems.

WHY IS SYSTEM AND COMMUNICATION PROTECTION IMPORTANT?

Cybersecurity protection has many layers. One of the first layers involves identifying the boundaries of your system and putting defenses in place. When we have assets or valuable information to protect, we want to deter anyone from trying to get to that data. So, just as we lock our doors and use home monitoring and alarm systems, we use firewalls, restricted access protocols, and monitoring systems for our networks. To protect our assets and data, we need to be able to block or restrict access to our network to anyone without authorization.

WHAT IS SYSTEM AND COMMUNICATION PROTECTION ABOUT IN NIST 800-171?

The System and Communication Protection family is one of the larger families in the NIST 800-171 standard. The main areas of focus within the System and Communication Protection family are:

1. Utilizing hardware and software firewalls to protect the boundaries of your system—firewalls are often the first line of defense to block unauthorized access to your IT system. Always keep the software and/or firmware updated.
2. Providing levels of access across your IT system—keep protected information separated from publicly accessible information. Design your network to allow for varying degrees of access and protection. Keep your assets and most sensitive data in the areas with the greatest level of restrictions and protections.

3. Implementing deny-all protocols for firewalls—set your firewall protection protocols to deny-all network traffic. You can then add in permit-by-exception protocols to allow designated network traffic through.

4. Controlling and monitoring mobile and remote access to your system—Establish restrictions of use for mobile and remote access to your system. Only authorized devices assigned to authorized users should be able to access the system.

[FAMILY 14]

A Closer Look at NIST 800-171:

The System and Information Integrity Family

The final family in the NIST 800-171 standard is the System and Information Integrity Family. This family focuses on your turnaround time for detected threats.

WHY IS SYSTEM AND INFORMATION INTEGRITY IMPORTANT?

A cybersecurity threat is not often announced. No phishing emails are sent with the subject line "This Phishing Email is

Targeting You." Websites with malicious code do not contain warnings in their URLs or google search results. It would be great if all the threats came with warning labels! Since that is not the case, we have to be diligent and regularly monitor our systems, scanning for threats and identifying any unauthorized access. Failure to identify a threat quickly will result in our systems being compromised and left open to attack.

WHAT IS SYSTEM AND INFORMATION INTEGRITY ABOUT IN NIST 800-171?

The controls in the System and Information Integrity family are focused on your ability to detect threats and protect your system against malicious code. The key points addressed in this family are:

1. Regularly scanning for threats—ensure you have anti-virus and anti-malware programs that scan your system for any existing infected or compromised files. Make sure that these programs and virus definitions are updated regularly. Set these programs to alert an administrator upon discovery of malicious code.

2. Scanning for real-time threats—employ real-time virus and malware scans on any devices that access external websites, receive emails or otherwise receive files from external sources. Real-time scans should be set to scan for malicious code from external sources as the files are downloaded, opened or run.

3. Monitoring network traffic for threats—monitor all incoming and outgoing communication within your network to detect unauthorized access and any intrusion. Activity monitoring should be done in accordance with any applicable state and federal laws and regulations.

4. Being able to identify unauthorized use of the system—monitor, and identify any intrusions to your systems through local, network and remote access. Any device that is permitted to access your systems should be monitored even if that device is accessing the system remotely.

NIST 800-171 Recommended Top 5 Controls

The NIST 800-171 standards may seem a bit overwhelming to those who are just starting to venture out into the world of cybersecurity planning. There are a total of 109 controls or requirements divided among the 14 families within NIST 800-171. Understanding and implementing changes to address each will take some time— typically six months or longer.

Getting started is the first hurdle. Especially since the first family, Access Control starts off with a list of 22 controls! I'd recommend you go through NIST 800-171 with a "choose your own adventure" style. Rather than starting on page one and sequentially addressing each family or control in order, review each family and skim the controls within to find those that are easiest for your business to address first.

Customizing your sequence of addressing the controls will make the process more meaningful and more efficient for you. Plus, you'll gain familiarity with the standards as you work through the easiest-for-you controls which will make the more complicated controls more understandable.

I even have five recommended controls to start you out in your adventure:

1. User awareness—phishing
2. Two-factor authentication
3. Patching
4. Firewalling
5. Antivirus/antimalware

User awareness/phishing is part of the awareness and training family. Education and training are very important to any cybersecurity program! Even with the best technology protections in place, one human error can open your systems up to a threat. Keeping everyone aware of cybersecurity risks and how their actions and activities impact those risks is the backbone of any cybersecurity plan. I recommend starting out with awareness training on phishing because phishing remains the number one way for outsiders to gain access to your system. People continue to fall victim to phishing scams and click links and even provide usernames and passwords to imposters.

To get an idea of how a phishing attack works check out the Cybersecurity Incident Response video featuring Deb Crawford, Internet of Things (IoT) Research Lead at the Laboratory for Analytic Sciences at North Carolina State University.

Two-factor authentication is part of the identification and authentication family. Implementing two-factor (or multi-factor) authentication protects your system by adding a layer of security around access point to your systems. This can prevent unauthorized access to your system using a stolen or compromised username and password.

With two-factor authentication, a person attempting to log in to your system would need to go through two steps to verify that they are allowed on the system. First, they would need a username and password. Second, they may need to enter an access code they retrieve from their smartphone. Or, perhaps they need to scan their fingerprint. It is often described as "something you know and something you have." The password is something that the person knows and the smartphone or finger is something that they have.

Patching is part of the configuration management family. Keeping your software programs and hardware patched closes another popular vulnerability that exposes your assets. Many successful hacks are made possible through the exploitation of outdated or unpatched software. Make sure to update your operating system, antivirus program and definitions, malware detection software, firewall and any software applications and hardware devices that run on or are connected to your systems. Apply patches as soon as possible and regularly check for upcoming updates that can be scheduled to run in advance.

Firewalling is part of the system and communication protection family. A firewall is your boundary protection keeping your systems separated from the outside world. It monitors inbound and outbound communication happening in your network. The firewall is the first line of defense that can block unauthorized access to your system while still allowing your system to communicate with designated parts of the outside world. Your firewall should be set to deny all network communications and allow only authorized communications using permit by exception.

Antivirus/Antimalware is part of the system and information integrity family. Viruses, worms, hijackers, Trojans, Spyware, Adware, Ransomware and more are abundant. These attacks are looking for any vulnerability to get into your system. An early line of defense is having antivirus and antimalware programs running on your systems. Run scans of your system regularly. Set these program to alert an administrator of any malicious code detection while also blocking off the code from your system. And, always keep the programs and definitions updated!

NCMEP