National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

Manageable Network Plan

Networks often become unmanageable and rapidly get out of control. An unmanageable network is not secure. The Manageable Network Plan is a series of milestones to take an unmanageable and insecure network and make it manageable, more defensible, and more secure. This plan provides overall direction, offers suggestions, calls out crucial security tips, and gives references to books, Web resources, and tools.

Version 4.0
December 2015
MTR U/OO/813640-15

Manageable Network Plan

Comments or feedback? manageable@nsa.gov

Disclaimer of Endorsement:
Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

Manageable Network Plan

Contents

The Manageable Network Plan

Have you discovered that your network is insecure? Are your network administrators always running around putting out fires? Does it seem to be impossible to get anything implemented or fixed on your network? If so, your network may be unmanageable.

An unmanageable network is insecure!

The Manageable Network Plan is a series of milestones to take an unmanageable and insecure network and make it manageable, more defensible, and more secure. The Plan is intended to be a long term solution; implementing the milestones may take a significant amount of resources and time (possibly months or even years). But consider: If your network is not manageable, or only barely manageable, it will be very difficult for you to fully implement *any* security measures. Once your network is manageable, you will be able to consider and implement security measures—and verify their implementation—much more efficiently and effectively.

Administrators may start shouting, "We have no free time! How can we do all this?" Having a manageable network *increases* your free time; it allows you to be *proactive* instead of *reactive*. And if you do have a huge network, do not take on the whole network at once: consider starting with individual subnets.

Each of the Plan's milestones contains a "To Do" list, and may also contain documentation requirements, points to consider, and ongoing tasks. Ideally, each milestone should be fully implemented before moving on to the next one, although some milestones can be implemented in parallel. If the earlier milestones are already implemented on your network, skip ahead to the first one that is not yet fully implemented. To determine this, each milestone has a checklist. For each question in a milestone's checklist, answer Yes or No; if No or only partially implemented, provide an explanation. If you consider the explanation acceptable from a risk management standpoint, check Accepts Risk.[1] If all the questions can be answered Yes or Accepts Risk, the milestone is complete. Document and date your answers to these milestone checklists. If a future network evaluation finds problems on your network, it may indicate that you should no longer accept the risks that you did in some areas, and that changes are needed. Some checklist questions have suggested metrics that can be used to track progress.

The Plan provides overall direction, offers suggestions, calls out crucial security tips,[2] and gives references to books, Web resources, and tools.[3] Every network is different, so use the Plan milestone "To Do" lists, documentation requirements, and ongoing tasks as a guide, and generate specific tasking for your network. The points to consider under each milestone may suggest additional tasks for your network. When developing these tasks, be mindful of

Note to Management

In order for this Plan to work, it will require—as with any strategic plan—a persistent organizational commitment. We understand that this may be difficult when balancing resources for your many mission priorities.

The risk of an unmanageable network is that, although it may be *available*, it is most likely not *secure*. It may be available to those who should *not* have access! This Plan helps your organization begin the step-by-step process of securing your network (see Appendix C). The Plan is consistent with the NSA Community Gold Standard and the Center for Internet Security (CIS) Critical Security Controls (formerly the SANS Twenty Critical Security Controls) (see Appendix B), and it will enable you to more easily implement any regulatory requirements you may have. This Plan also briefly describes the Risk Management Framework (see Appendix F) which, along with the rest of this Plan, will help you improve your network's security posture. Much of this Plan is applicable to Industrial Control System (ICS) / Supervisory Control and Data Acquisition (SCADA) networks as well. Some of the unique characteristics of ICS/SCADA networks are described throughout this document.

Familiarize yourself with the Plan and consult with your technical people to help you identify the resources and personnel skill sets that will be needed to execute this Plan. Keep in mind that hiring and retaining competent technical people is key to securing your network; turnover of personnel greatly contributes to making a network unmanageable.

With a strong organizational commitment, we are confident that this Plan will help you make your network manageable and more secure!

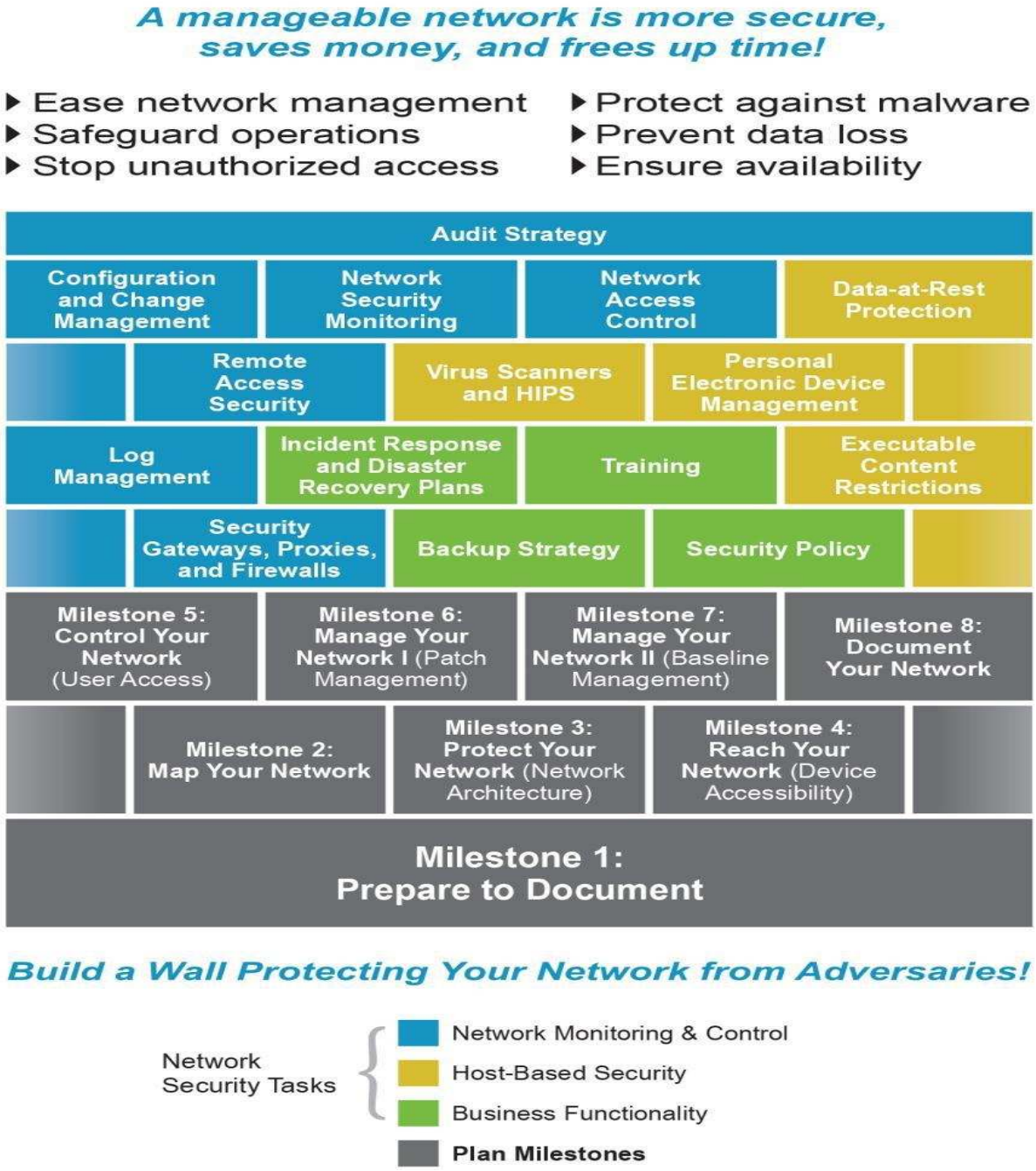
[1] For information on risk management, see NIST Special Publication 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View" (Available at http://csrc.nist.gov/publications/).

[2] These crucial security tips are consistent with the top mitigations noted in the Australian Signals Directorate's "Strategies to Mitigate Targeted Cyber Intrusions" (http://www.asd.gov.au/infosec/mitigationstrategies.htm).

[3] Note that the tools mentioned have not been evaluated by the NSA and might not be approved for use in your organization.

any security assessment and authorization authorities that you must comply with. Use relevant standards (such as SCAP standards[4]) and community-vetted data models so that you can benefit from others' work, both immediately and in the long term. Be sure each task states *what* is to be done, *who* is to do it, and *when* the task must be completed. Also be sure that your specific tasking does not water down or miss the point of the Plan milestones—that will not help your network become more manageable!

Manageable Network Plan Defensive Wall



[4] For information on using SCAP, see NIST Special Publication 800-117: "Guide to Adopting and Using the Security Content Automation Protocol (SCAP)" (Available at http://csrc.nist.gov/publications/).

Manageable Network Plan

Milestone 1: Prepare to Document

Documentation will be a necessary part of every milestone.

To Do

- Set up a way to begin documenting information about your network. (This does not mean *do* all the documentation here—just set up a way to do it.)
  - Suggestion: Use a blog or bulletin board to notify administrators of changes, and a wiki to document information. A common issue occurs when multiple administrators administer the same devices: one of them goes on vacation and wants to know who picked up the slack (or not) while he was out. A blog of tasks the administrators performed lets the administrator who was on leave quickly catch up.
  - Consider: Any documentation that you already have should be collected and organized. Your documentation approach should support this existing documentation as well.
  - Consider: A more formal documentation approach may be necessary, to include a central documentation authority, document tracking, and enforcement of documentation consistency.
  - Consider: Because of the nature of Industrial Control System (ICS) / Supervisory Control and Data Acquisition (SCADA) devices, these systems and their networks are often overlooked. Be sure to include your ICS/SCADA networks in your documentation planning.

Consider

- **Ease of use.** Doing documentation should be quick and painless; otherwise it will never get done. Make sure your documentation approach is easy to use.
- **Purpose.** The two purposes of documentation are to share information and to retain information. Does your documentation approach address these points?
  - Suggestion: If you do use a blog to document administrator changes, consider using RSS feeds to keep other administrators apprised of the changes.
  - Consider: Having good documentation allows managers to track and reward progress. It may also allow users to understand and solve their own problems, instead of going to the administrators for every little thing. Can management and users easily read your documentation?
- **Sufficient level of detail.** Someday you will need to consult your documentation to rollback an unwanted change to a device, or to rebuild a device that had a catastrophic failure. Does your documentation approach support recording information at this level of detail? Do your administrators realize that they need to document to this level of detail, and include not only the *what* but also the *why* of changes?
  - Suggestion: Before making changes to a device's configuration, save off the current configuration file. Then if the changes do not work properly, it is easier to roll back to a working version.
  - Consider: Most important to document are the trouble spots, unique fixes, chain reactions due to unexpected dependencies, command line parameters, installation procedures, etc. However, it is also important to document the mundane, day-to-day things so that someone unfamiliar with the usual processes can take over in an emergency, and so new personnel can get up to speed quickly.
- **Timestamps.** Does your documentation approach ensure that everything has a timestamp so you know when it was last valid? (Yes, this includes even the sticky notes!)
- **Backing up.** Having good documentation assists in disaster recovery. Is your documentation repository backed up on a regular basis?
- **Protection.** If a network intruder obtains access to your documentation, they may discover additional information about your network. Is your documentation protected (e.g., password or PKI) and encrypted?
  - Suggestion: Never store non-temporary passwords on the network or send them in an e-mail. A network intruder can find them and use them to further compromise your network.
- **Hard copy.** It is hard to read on-line docs when the power goes out! Is a hard copy version of relevant sections of your documentation readily available?

- Suggestion: Hard copy documentation should at least include start-up information and sequence, and emergency procedures.
- Consider: Besides protecting your on-line documentation, it is also important to protect the hard copy version (limit number of copies, keep in secure area, shred old versions, etc.).

Ongoing

- From now on, whenever a change is made to your network or to devices on your network, document it. Even if you have no current documentation, just documenting from this point forward will be beneficial.
- Update paperwork for newly hired system administrators to reflect the location of documentation as well as requirements and expectations for documentation.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 1: Prepare to Document
				Do you have a way to document information about your network?
				Are you currently documenting all changes to your network?
				Have you gone over the points to consider for this Milestone?

Checklist date:

Milestone 2: Map Your Network

In order to have any sort of control over your network, you first need to know where everything is. This milestone and the next focus primarily on gathering information about your network (although the points to consider may prompt you to investigate making network changes). Note that, depending on your network, it may be easier to implement Milestones 2 through 5 first for the infrastructure and then for the endpoint devices, instead of trying to do everything at once.

To Do

- Create an accurate map of your current network (network topology). Be sure this network map is stored in a way that is secure, but yet still allows easy updates as network changes occur. Now before you can create an accurate map of your network, you must first identify the boundaries of your network.
  - Consider: Typically your network consists of all of the equipment and communications channels under your control.
  - Suggestion: If you have any devices connected by wireless, they should be included on the map. Connections to any clouds, external networks, and the Internet should also be included on the map.
- Create an accurate list of ALL devices on your network. For each device, record host name, role (its purpose on your network), MAC address (and IP address if static), service tag/serial number, physical location, and operating system or firmware. Note that your organization may require recording additional information. Also, for each device, record a specific person or group who is responsible for it, so that if there is a problem you know exactly whom to contact.
  - Suggestion: All workstations, servers, supporting devices (such as printers and scanners), and infrastructure devices (such as routers, firewalls, and IDSs) should be included in this list. In addition, all mobile devices (such as laptops and smartphones) and removable media (such as USB drives) that ever connect to your network should be included in this list.
  - Suggestion: Store this information in a central database. Applications can be written to query this database and automate many tasks. Be sure to properly secure this database!
  - Consider: Make use of tools such as Nmap, arpwatch, and/or a commercial enterprise network mapping solution to discover your network devices, but do not rely on them to discover ALL your devices. A room-to-room walkthrough of your organization will probably be required so that no devices are overlooked. Be cautious about scanning ICS/SCADA devices or networks. ICS/SCADA devices are designed to communicate in a simple, well-structured manner. Any communications outside of prescribed protocols could adversely affect these devices. Problems ranging from hang-ups to a total "bricking" of a device are possible. Therefore, active scanning (such as using Nmap) of an ICS/SCADA device or network should be avoided. The safest way to identify ICS/SCADA devices is by utilizing passive data collection techniques such as using Wireshark (https://www.wireshark.org) followed up by a room-to-room walkthrough.
    - For more information on the network security scanner Nmap, see http://nmap.org.
    - For more information on arpwatch, for tracking MAC-IP address pairings, see http://ee.lbl.gov.
  - Consider: An additional way to gather this information is to require users to register their devices in order to obtain an IP address on your network. Consider using an application like NetReg (http://netreg.sourceforge.net) or a commercial IP Address Management (IPAM) solution.

Crucial Security Tip

- Create a list of ALL protocols that are running on your network.
  - Suggestion: Three possible ways to do this are: 1) Use Wireshark, tcpdump, and/or WinDump to figure out what is currently running on your network (you may also be able to get this information directly from your routers); 2) Allow traffic with only specific protocols and ports through your firewalls and see what breaks; or 3) Read the documentation on all your network applications to determine what *should* be running on your network.
    - For more information on the network protocol analyzer Wireshark, see https://www.wireshark.org.
    - For more information on the network packet analyzer tcpdump, see http://www.tcpdump.org.
    - For more information on the Windows port of tcpdump, WinDump, see http://www.winpcap.org/windump.

Manageable Network Plan

Consider

- **Physical routes.** If you are using a Virtual Local Area Network (VLAN), have you recorded the possible *physical* routes that your VLAN traffic traverses? This is important to know so that if, for example, you take a router down for maintenance, you can be sure that it will not accidentally bring down your virtual network.
- **Removing unapproved devices and protocols.** Any devices on your network that you have not approved should be removed. Any protocols that you have not approved should be blocked.
- **Asset management.** The ideal way to keep track of all the devices on your network is to implement a formal IT inventory (or asset) management process. Such a process can help you keep track of devices all the way from request and procurement to disposal. Consider also keeping track of device suppliers and maintenance providers here.
- **Network Map Distribution.** Consider providing the Network Map to team members for review on a periodic basis. However, the Network Map should only be given to members with a need-to-know.

Ongoing

- Update the network map and list of devices any time a device is added to or removed from your network. As your procedure for this becomes more standardized, consider automating it.
- Update the list of protocols any time a new protocol is added to your network, or an old protocol is no longer used. As your procedure for this becomes more standardized, consider automating it.
- Periodically use the tools mentioned above to check your network map and your lists of devices and protocols for accuracy. Remember, the tools will not find everything, but they may find things that were added to the network without your knowledge.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 2: Map Your Network
				Do you have a current, accurate network map?
				Do you have a current, accurate list of ALL devices on your network (or that ever connect to your network), that records host name, role, MAC address, service tag, physical location, OS/firmware, and responsible person/group? - Total number of devices on your network, broken down by category (workstation/server/supporting/infrastructure/mobile/ removable media)? - How often is this list checked for accuracy by using discovery tools?
				Do you have a current, accurate list of ALL protocols that are running on your network?
				Are you updating your network map and lists of devices and protocols whenever a change is made to your network? - When there is a change, how long before this documentation is updated?
				Have you gone over the points to consider for this Milestone?

Checklist date:

Milestone 3: Protect Your Network (Network Architecture)

Sound network architecture protects your high-value assets by limiting access to them, provides important functionality consistent with your business model, and ensures business continuity in the event of a disaster.

To Do

- Identify your current network enclaves: which groups of users on your network have access to what types of information. For example, the Engineering enclave has access to the CAD drawings, the HR enclave has access to the personnel files, etc.
- Identify your current high-value network assets. Note that "high-value asset" does NOT mean "the machine cost a lot of money." Identify what you are trying to protect from a *business* standpoint: What *data* is most critical to you? What *functionality* is absolutely required? The machines where this data resides (for example, your servers) and where this functionality is implemented (for example, your domain controllers) are your high-value assets—your "crown jewels".
  - Consider: Also identify anything on which your high-value assets depend (other systems, certificate authorities, specific vendors, the air conditioning, etc.). This will help you understand how a problem at that level might affect your high-value assets and what mitigation strategies might be needed.

How to Identify Your High-Value Network Assets

1. Identify the products your organization produces.
2. Understand your production process.
3. Identify your high-value network assets:
   - **Any machine** involved in your production process that cannot be easily replaced in a timely manner.
   - **Any machine** that holds data important to your production process, where that data cannot be easily restored in a timely manner from a *recent* backup.
   - **Any machine** that EVER comes in contact with sensitive data, i.e., data that would cause your organization (or other people or organizations that rely on you) grave damage if a competitor or someone with malicious intent got access to it.

- Identify the choke points on your network. A choke point is a location which allows access between different "sections" of your network, such as sections with different trust levels, your different enclaves, or even your ICS/SCADA network. Ideally, all traffic between these sections should flow over a relatively small number of choke points. Especially be sure to identify the choke points on the "edge," i.e., the points of access into your network.

Documentation

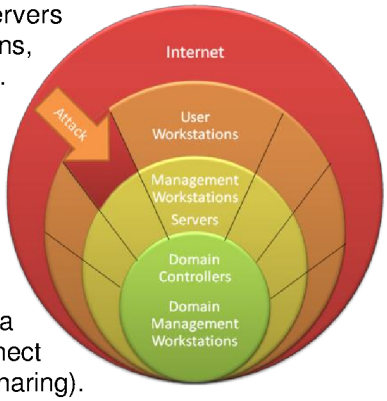
- Document your network enclaves.
- Document the high-value assets and choke points on your network.

Consider

- **Damage containment.** Your network should be designed to keep any damage to it contained, reducing the impact of a potential compromise. An intruder who penetrates your boundary defenses should not have open access to everything on your network. An insider desiring to steal sensitive data should not have access to information that he does not have a genuine need-to-know.
  - Suggestion: Be sure the choke points on your network are positioned to most effectively protect your high-value assets. Place security gateways, proxies, or firewalls at these choke points so that traffic over them can be monitored and controlled (see the *Security Gateways, Proxies, and Firewalls* and *Network Security Monitoring* Network Security Tasks).
  - Suggestion: Your network enclaves should be separated so that valuable data is only available to those who need it. For example, Engineering should have access to the CAD drawings, but not the personnel files; and HR should have the opposite access. Ideally, network assets should be physically isolated, but VLANs can also be used to logically enforce separation.
    - At a minimum, there should be separation between your organization's internal network, the extended enterprise, and the Internet. This is the idea behind, for example, putting all your publicly-accessible assets into DMZs (demilitarized zones). There should also be separation

between your internal network and your remote access users. Consider noting all these separations on your network map from Milestone 2.

- Consider additional separations: wired vs. wireless, voice vs. data, separation of network assets with different sensitivities of information, and isolation of servers with highly sensitive data. Keep internal administrative functions, internal user functions, and external user functions separate. Physically separate server functions onto different servers—for example, a domain controller should not also be running a customer database. In addition, never use your servers as workstations.



Crucial Security Tip

- To decrease your attack surface, limit the number of Internet gateways/access points into your network. Ensure that wireless devices on your network cannot be used to bypass firewalls or other boundary defenses by acting as a conduit through which other or unauthorized devices can connect to your network (for example, Windows Internet Connection Sharing). This is especially significant if your ICS/SCADA network is connected to your corporate network.
- If assets on your network are not sufficiently separated, consider redesigning your network architecture and migrating to that new design. For guidance, see *Top-Down Network Design, Third Edition* by Priscilla Oppenheimer (Cisco Press, 2010). For guidance on isolating assets based on security dependencies (specific to a Windows network, but the general principles apply to any network), see *Windows Server 2008 Security Resource Kit* by Jesper Johansson (Microsoft Press, 2008), Chapter 13 ("Securing the Network").
- For more information on using VLANs for logical separation, see "VLAN Provisioning for Logical Separation" (http://iase.disa.mil/stigs/Documents/vlan_provisioning_security_guidance_at-a-glance_v8r1.pdf). Keep in mind that VLANs segregate traffic at OSI Layer 2, but a Layer 3 device such as a router could still allow separate VLANs to talk to each other. Be sure that any Layer 3 device that bridges your VLANs has appropriate access controls in place.

Crucial Security Tip

- Suggestion: Examine your network trust relationships—those within your internal network and also those you have with external networks—to determine whether they are really necessary for your organization's mission. Trust relationships can be exploited by malicious intruders to gain access, and traditional network defenses (e.g., firewalls, malware scanners, etc.) *cannot defend* your network against exploited trust relationships! Eliminate all trust relationships that are not needed. Make trust relationships one-way instead of two-way whenever possible. Limit who is trusted, what privileges they are allowed, and what access to resources they have.
- Suggestion: Limit workstation-to-workstation communication to severely restrict attackers' freedom of movement via techniques such as Pass-the-Hash (see Milestone 7) . In general, limiting the number and type of communication flows between systems also aids in the detection of potentially malicious network activity. For more information on limiting workstation-to-workstation communication, see the "Limiting Workstation-to-Workstation Communication" NSA Fact Sheet (Available at https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_LimitingWtWCommunication_Web.pdf).
- Suggestion: Consider restricting the access of mobile devices such as laptops to only the devices on your network with which they actually need to communicate.
- Suggestion: Block peer-to-peer services.
- Suggestion: Use penetration tests and Red Team exercises to test your damage containment.
- Consider: For additional considerations related to protecting data and keeping damage contained, see the *Personal Electronic Device Management, Data-at-Rest Protection,* and *Remote Access Security* Network Security Tasks. Also see Least Privilege Administrative Model under the Milestone 5 points to consider (discusses limiting damage from credential theft) and Same Password Problem under the Milestone 7 points to consider (discusses mitigating pass-the-hash attacks).

- **Data-in-transit protection.** Data traversing your network or moving between networks is at risk from eavesdropping and malicious redirection. Your data transport mechanisms must protect this data.
  - Suggestion: Use IPsec to protect the confidentiality and integrity of data in transit/motion. IPsec can also be used for peer authentication, replay protection, traffic analysis protection, and access control. For recommendations on using IPsec, see NIST Special Publications 800-77: "Guide to IPsec VPNs" (Available at http://csrc.nist.gov/publications/). A more flexible option to protect the confidentiality and integrity of data in transit may be Transport Layer Security (TLS, the successor to SSL).

- Consider: Many ICS/SCADA systems do not use any encryption on data in transit. Lack of encryption enables unauthorized persons to monitor ICS/SCADA communications as well as inject false data or harmful commands onto the ICS/SCADA network which could result in shutdowns, damage, or product tampering. To protect ICS/SCADA data in transit, consider using VPN tunnels for data that must transit a corporate network or the Internet. Radio links such as Wi-Fi, WirelessHART or 900 MHz SCADA radios should be built with hardware that support radio frequency link data encryption and this encryption should be used.
- Suggestion: A man-in-the-middle (MITM) attack occurs when communicating parties believe they are talking with each other over a private connection, but where in reality an adversary is eavesdropping on their communication by making independent connections with the parties and relaying messages between them. This might allow the adversary to intercept sensitive data. A MITM attack is successful only if the adversary can impersonate each party in the communication to the satisfaction of the other. Use robust end-to-end mutual authentication techniques based on public key infrastructure (PKI) to reduce the chance of successful MITM attacks.
- Suggestion: The Domain Name System (DNS) is a sort of "phone book" for the Internet, translating human-readable domain names into IP addresses. The original DNS was designed with no security controls, allowing critical attacks that could result in network compromise and loss of sensitive data. DNS Security Extensions (DNSSEC) was introduced to provide a layer of integrity to the DNS; it does not offer protection from all DNS attacks, but it does give greater assurance that users and their data are not being redirected to malicious sites. For recommendations on securing DNS and using DNSSEC, see NIST Special Publication 800-81: "Secure Domain Name System (DNS) Deployment Guide" (Available at http://csrc.nist.gov/publications/).

- **Cloud computing.** If all or part of your network is integrated with "the cloud"—or you are considering such integration—be sure that you understand the benefits and risks involved.
  - Suggestion: For more information on the benefits and risks of cloud computing, see the following:
    - NIST Special Publication 800-146: "Cloud Computing Synopsis and Recommendations" (Available at http://csrc.nist.gov/publications/)
    - The Cloud Security Alliance's "Security Guidance for Critical Areas of Focus in Cloud Computing" (Available at https://cloudsecurityalliance.org/research/security-guidance)
  - Suggestion: The U.S. Government has established the Federal Risk and Authorization Management Program (FedRAMP), a standard set of basic security requirements that cloud service providers must meet before being authorized for U.S. Government use. FedRAMP is mandatory for U.S. Government cloud systems; other organizations should also consider using the FedRAMP criteria when selecting cloud service providers. For more information, including a list of third party assessment organizations, see http://www.fedramp.gov.

- **Virtualization security.** If your network includes virtual servers and/or desktops—or you are considering using these—be sure that you understand the security implications. For more information, see NIST Special Publication 800-125: "Guide to Security for Full Virtualization Technologies" (Available at http://csrc.nist.gov/publications/).
  - Suggestion: Be sure to follow the configuration and hardening guidance from the vendor of your virtualization solution.
  - Consider: Virtualization approaches (such as thin clients, desktop virtualization, or application virtualization) and cloud computing may improve your organization's network resiliency, by enabling rapid reconstitution of assets and data. Again, consider the benefits and risks involved.

- **Physical security.** Physical security of your network assets is extremely important! If an adversary can *physically* touch your boxes, it will not matter how well you secure your data.
  - Suggestion: At the very least, implement some kind of monitored physical access control so that unauthorized individuals are not allowed near your high-value assets. Also consider how you will authorize and monitor maintenance personnel, janitorial staff, and other persons who need physical access to your facilities.

- **No single points of failure.** Are there any single points of failure for critical systems on your network? These should be eliminated. Think end-to-end when considering this. For example, is all of your critical outgoing network traffic routed through only one physical cable? Even if you have multiple cables out, do they ever run together, such as through a single conduit under a river? Are both the main and backup power supplies on a critical server plugged into the same UPS or into electrical outlets on the same

breaker switch? Are your primary and backup e-mail (or other application) servers located in the same rack or sharing power sources or sharing the same network switch? Are your primary e-mail (or other application) server and the network switch for your backup e-mail (or other application) server sharing power resources such that if power goes out to your primary server it also goes out to the switch for your backup server resulting in both servers being unreachable? Look for other instances where space (e.g. rack), power, or cooling resources are shared and consider the impacts of a failure of any of the resources.

- Suggestion: Regularly test your failover equipment and scenarios. If a critical system fails, ensure that it can be fixed or replaced in a timely manner.

- **Custom Web applications.** Do you have custom Web applications facing the Internet? If so, are they protected and/or are your developers trained in writing secure, robust, and fault-tolerant code?
  - Suggestion: Use the Open Web Application Security Project (OWASP) resources for secure Web application development:
    - Secure Web application development guide (https://www.owasp.org/index.php/Category:OWASP_Guide_Project)
    - Web application testing guide (https://www.owasp.org/index.php/Category:OWASP_Testing_Project)
    - Developing your own security controls can lead to wasted time and security holes. Use the OWASP Enterprise Security API (ESAPI) toolkits (https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API).
    - The best place to defend a Web application from malicious activity may be within the application itself. Consider using the OWASP AppSensor framework (https://www.owasp.org/index.php/Category:OWASP_AppSensor_Project).

- **Legacy systems.** Do you have legacy systems and software (including operating systems) that your organization depends on? If so, are they protected from more modern attacks and other misuse? If they ever get compromised, is the rest of your network protected from *them?*
  - Suggestion: Put your legacy systems on a separate network and access them through a custom Web service that appropriately sanitizes all input and output.
  - Suggestion: For guidance on migrating legacy systems, see "DoD Legacy System Migration Guidelines" (http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=13311).

- **ISC/SCADA vulnerability.** Field level controllers and devices used on ICS/SCADA networks are special purpose systems designed to operate in a trusted environment. Therefore, they have limited built-in security or protection measures.

- **Risk assessment.** If you want to go more in-depth than just "what is a high-value asset and what is not" on your network, consider doing a complete risk assessment.
  - Suggestion: For guidance on conducting risk assessments, see the following:
    - NIST Special Publication 800-30: "Guide for Conducting Risk Assessments" (Available at http://csrc.nist.gov/publications/)
    - ISO/IEC 31010, *Risk management – Risk assessment techniques* (Available at http://www.iso.org)
  - Consider: Risk assessment is only part of the larger risk management process. For more information, see Risk Management under the *Configuration and Change Management* Network Security Task.

Ongoing

- Update your documentation whenever your network enclaves, high-value assets, or choke points change (added, removed, or relocated). Consider that your enclaves and which of your assets are identified as high-value might change periodically, based on your mission.

- Re-evaluate your network architecture periodically. Your security and manageability requirements may change, especially as your organization grows.

Manageable Network Plan

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 3: Protect Your Network (Network Architecture)
				Have you identified and documented your current network enclaves?
				Have you identified and documented the current high-value assets and choke points on your network?
				Are you updating your documentation whenever your network enclaves, high-value assets, or choke points change? - When there is a change, how long before this documentation is updated?
				Are you periodically re-evaluating your network architecture to make sure it most effectively protects your high-value assets, limits access to sensitive information, and keeps damage contained? - How often are these re-evaluations done? - How often do you review your network trust relationships? - If a trust relationship is found that can be eliminated or limited, how long before this elimination/limiting is actually done?
				Have you gone over the points to consider for this Milestone?

Checklist date:

Milestone 4: Reach Your Network (Device Accessibility)

Hard-to-administer devices on your network will be looked at less often and thus are more likely to have vulnerabilities.

To Do

- Establish a process to properly, easily, and securely access (either remotely or physically) and administer EVERY device on your network (workstations, servers, supporting devices such as printers, infrastructure devices such as routers and firewalls, and mobile devices such as laptops and smartphones).
  - Suggestion: For Windows machines, implement Active Directory.
  - Suggestion: Windows Group Policy is a powerful way to securely configure and administer the machines in a Windows network domain. For more information on Windows Group Policy, see *Group Policy: Fundamentals, Security, and Troubleshooting* by Jeremy Moskowitz (Wiley, 2008).
  - Suggestion: To configure and administer non-Windows machines on your network, consider using Puppet. For more information on Puppet, see https://puppetlabs.com.
  - Suggestion: To administer devices that cannot be accessed on a regular basis, such as laptops and other mobile devices, consider using a network access control solution to update these devices when they are next connected to the network (see the *Network Access Control* section under Network Security Tasks). Note that if a user is allowed full administrative control of such a device, the device should be wiped and reimaged before it is allowed back on the network.

Documentation

- Document your process to administer ALL your devices, especially those that cannot be accessed on a regular basis.

Consider

- **No clear-text administration protocols.** Do not use protocols that transmit information in the clear (HTTP, Telnet, rsh, FTP, TFTP, etc.) to administer your devices. Instead use encrypted protocols (HTTPS, SSH, SCP, SFTP). If using SNMP, use SNMPv3 (versions 1 and 2 are clear-text protocols) and ensure that the integrity and authentication features are properly enabled.
  - Suggestion: On Windows machines, use utilities such as the PuTTY SSH client, the WinSCP SFTP client or FileZilla SFTP. SSH and SFTP capabilities are included natively on Linux/Unix.
    - For more information on PuTTY, see http://www.chiark.greenend.org.uk/~sgtatham/putty.
    - For more information on WinSCP, see http://winscp.net.
    - For more information on FileZilla, see https://filezilla-project.org.
  - Suggestion: Block or proxy the clear-text protocols mentioned above on your network, in order to prevent malware from misusing them.
- **No unacceptable security dependencies.** A critical device should never be administered from a less critical device, because this makes the security of the critical device dependent on the security of the less critical device. For example, a domain controller should never be administered from an Internet-connected workstation. Consider using dedicated management stations for administering critical devices.
- **Remote administration.** Are your administrators able to administer your network from home or from outside your network? If so, make sure that all remote administration hosts and credentials are extremely secure (see the *No unacceptable security dependencies* point to consider above). Also make sure that the remote connection is secure (see the *Remote Access Security* Network Security Task). If you allow remote administration, a compromise in any of these areas might allow an intruder access to your entire network!
- **Physical security.** Not just anyone should be able to walk up and access your network devices in an administrative mode. Do you have some sort of physical access control in place to prevent this? Do your administrators know to close a device's administrative interface when they walk away from it?
- **Automating administration.** Automating administrative tasks frees up network administrator time. Is as much administration as possible done in an automated way?

- **Same administrative tools.** The way the devices on your network are administered should be standardized. Do all your network administrators use the same tools?
- **Administrator teaming.** If you have an ICS/SCADA network, it is probably maintained by a team of administrators that typically is separate from the administrators for your other network. It is important that they communicate with each other as the two groups often do not understand the complexities and issues with each other's networks.
- **Outsourcing administration.** If you outsource your network administration and maintenance, use trustworthy vendors in whom you have complete confidence, because these vendors will have full access to your network. Remember that all expectations you have of these vendors must be explicitly codified in contract language with appropriate performance metrics. Also consider the following:
  - Vendors must be required to maintain not only an acceptable level of performance for your network, but also an acceptable level of security. You—not the vendors—must predefine what you consider "acceptable levels" (i.e., goals) and how these will be measured. Also consider how you will resolve disagreements between you and your vendors over how these acceptable levels are maintained.
  - All processes, procedures, and configurations under vendor control for your network must be properly documented. This documentation must be owned by you—not the vendors—so that it remains available to you if you change vendors or take over administrator duties yourself.
  - Vendors must allow independent assessments as you—not the vendors—deem necessary.
  - There must be agreement between you and the vendors on how to recognize, handle, and report network incidents.

Ongoing

- As necessary, update your device access/administration process and documentation.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 4: Reach Your Network (Device Accessibility)
				Have you established and documented a process to properly, easily, and securely access and administer EVERY device on your network (workstations, servers, supporting devices, infrastructure devices, and mobile devices)?
				Are you updating your device access/administration process and documentation as necessary?
				Have you gone over the points to consider for this Milestone?

Checklist date:

Milestone 5: Control Your Network

Users on your network should be limited to the least privilege that they require to perform their duties.

To Do

- Establish non-privileged user accounts for all users on your network. Regular users should *only* be allowed to use non-privileged accounts. Administrators should only use their privileged accounts when performing administrative tasks and should use their non-privileged accounts for everything else.
  - Suggestion: Some users may still require some elevated privileges; limit the number of these users and their allowed privileges to an absolute minimum.
    - If a user only requires privileged access to certain directories or applications, use Windows Group Policy to grant that access instead of giving the user local administrator privilege. If a user does require full local administrator privilege, consider only allowing that privilege for a limited time or isolating any system on which that privilege is given.
    - Consider using Windows Delegation to give some domain administrator privileges to those users that require it, without giving them full access. For operating systems other than Windows, use sudo or Role-Based Access Control (RBAC). Alternatively, consider using Attribute-Based Access Control (ABAC) or an application to granularly elevate user privileges: access control should be as granular as possible.
      - For more information on ABAC, see NIST Special Publication 800-162: "Guide to Attribute Based Access Control (ABAC) Definition and Considerations" (Available at http://csrc.nist.gov/publications/).
  - Consider: For additional considerations related to user access and preventing credential misuse, see User Authentication under the *Network Access Control* Network Security Task. Also see Same Password Problem under the Milestone 7 points to consider (discusses mitigating pass-the-hash attacks) and Data Loss Prevention under the *Data-at-Rest Protection* Network Security Task (discusses insider threat).
  - Consider: Periodically analyze, survey, and assess vulnerabilities to further evaluate user activity and mishandling of privileged accounts. If you outsource this service, use trustworthy vendors in whom you have complete confidence because these vendors will have full access to your network. Remember that all expectations you have of these vendors must be explicitly codified in contract language with appropriate performance metrics. Also consider the following:
    - Vendors must be required to maintain not only an acceptable level of performance for your network, but also an acceptable level of security. You—not the vendors—must predefine what you consider "acceptable levels" (i.e., goals) and how these will be measured. Also consider how you will resolve disagreements between you and your vendors over how these acceptable levels are maintained.
    - All processes, procedures, and configurations under vendor control for your network must be properly documented. This documentation must be owned by you—not the vendors—so that it remains available to you if you change vendors or take over these duties yourself.
    - Vendors must allow independent assessments as you—not the vendors—deem necessary.
    - There must be agreement between you and the vendors on how to recognize, handle, and report network incidents.

Documentation

- For any user that does require elevated privileges, document the privileges given and the reasons for them. If applicable, also record the machine(s) the privileges are given on (perhaps in the device list from Milestone 2).

Consider

- **No Internet or e-mail from privileged accounts.** Letting users with local admin, root, or other elevated privileges surf the Internet or read e-mail is a VERY serious security risk! Malicious websites and e-mail attachments can make use of those elevated privileges to install malware on the network. Network administrators and other high-privileged users should not be allowed to access the Internet or e-mail from their privileged accounts. For suggestions on how to enforce this, see the "Enforcing No Internet or E-mail from Privileged Accounts" NSA Fact Sheet (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).

Crucial Security Tip

- **Least privilege administrative model.** To limit damage in case of credential theft, administrative accounts should not be granted access to overly large cross-sections of devices on your network. Administrative accounts at any level should only be used to administer devices at that level.
  - Suggestion: Set up your domain-based administrative accounts in tiers, so that different accounts (with different passwords/credentials) are used to administer devices of different criticality (for example, one account to administer workstations, another for servers, etc.). Deny these administrator accounts from logging onto devices in a different tier. At the top level, the Domain Administrator account must only be used to access the domain controller (and possibly other domain critical devices). Segregating administrator roles in this way reduces the exposure of these powerful accounts and makes it more difficult for an attacker to escalate his privileges.
  - Suggestion: Configure each machine to deny all remote attempts to logon as local administrator; the local administrator account should never be used for remote administration. In addition, divide your machines into different subgroups (within a tier) and assign different domain-based administrator accounts (with different passwords/credentials) to each subgroup; then for each machine, configure its host firewall to only accept network traffic from its subgroup's administration machine. Limiting administrator access in these ways makes it more difficult for an attacker to move laterally around your network.
  - For guidance on implementing a least privilege administrative model on a Windows network, see Microsoft's "Best Practices for Securing Active Directory" (http://www.microsoft.com/en-us/download/details.aspx?id=38785).

- **Users installing software.** Users with non-privileged accounts should not be able to install software. This is good from a security standpoint, but how will you handle those users who do actually need to install software? How will you handle your developers who write code and run arbitrary things?

- **No "entitlement."** Employees may need to be reminded that they are not "entitled" to have unfiltered Internet access and install whatever software they want on their workstations. After all, they do not own "their" workstations; the company does. Enforcing these restrictions will go far in making your network more manageable!

- **Expiration dates on accounts.** Consider setting expiration dates (quarterly or yearly) on all user accounts, so that unused accounts will be automatically disabled.

- **Hiring consideration.** Anyone with full administrative privileges on your network will have access to all its data. Are those individuals properly vetted in your hiring process? Are they periodically reinvestigated?

- **Disable accounts when employee leaves.** When an employee leaves or is terminated from your organization, are his or her accounts disabled? If the accounts cannot be immediately disabled, are they at least heavily monitored to catch any potential misuse? Do not overlook system administrator, database administrator, and remote access accounts, as well as any application-specific accounts and access to shared accounts. Remember to disable accounts on your ICS/SCADA network too. Unfortunately, in many ICS/SCADA networks, devices operate with a single system-wide or vendor installed default account and password. Disabling accounts in an ICS/SCADA network is administratively difficult to nearly impossible after the system has been certified and is operational. However, if it is possible on your ICS/SCADA network, then do disable the accounts of employees who are no longer part of the organization.

Ongoing

- For each of your users that has elevated privileges, regularly review the reasons for this. When the reasons are no longer valid or no longer justifiable, remove the privileges.

- Periodically verify that all accounts on your network are tied to specific, current, authorized users (who have up-to-date credentials). Any accounts that cannot be verified should be disabled and removed.

- Periodically analyze, survey, and assess vulnerabilities to further evaluate user activity and mishandling of privileged accounts.

Manageable Network Plan

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 5: Control Your Network (User Access)
				Have you established non-privileged user accounts for all users on your network? - % of *total* users on your network that are allowed to use *only* non-privileged accounts? (Higher % is more secure)
				For all users with elevated privileges, have you documented the privileges given and the reasons for giving those privileges, and are those reasons regularly reviewed? - How often are the reasons for giving those privileges reviewed? - If the reasons are no longer valid or no longer justifiable, how long before the privileges are actually removed? - % of elevated privilege accounts that do NOT have access to Internet or e-mail? (Higher % is more secure)
				Are you periodically verifying that all accounts on your network are tied to specific, current, authorized users? - How often are these verifications done? - If an account is found that cannot be so verified, how long before this account is disabled? - If a user becomes unauthorized (terminated, etc.), how long before his account(s) are actually disabled?
				Have you gone over the points to consider for this Milestone?

Checklist date:

Milestone 6: Manage Your Network, Part I (Patch Management)

Vulnerable devices on a network are often used as entry points for dangerous network attacks. Actively managing your network devices in a few areas can dramatically improve your security; this milestone and the next are focused on setting up these management areas. Note that specific implementations will differ for different device roles and operating systems. Note also that truly effective management of these areas relies on the previous milestones being completed.

To Do

- Establish a patch management process for ALL the firmware, operating system and application software on EVERY device on your network (workstations, servers, supporting devices such as printers, infrastructure devices such as routers and firewalls, and mobile devices such as laptops and smartphones).
  - Suggestion: Prioritize your patch management. All of your systems should be patched regularly, but those systems and applications that handle data from untrusted sources (such as the Internet) must be patched more often. In addition, critical patches must be applied whenever they are released. The sensitivity and criticality of certain systems may warrant exceptions however. If you make exceptions, be sure that those systems are isolated as much as possible and monitored closely for signs of known attacks; segregation behind a firewall is recommended.
  - Consider: Patching your laptops and other mobile devices may be difficult, because they may not be regularly connected to your network. The plan to administer these devices (developed in Milestone 4) should include regular patching of both firmware and software. Alternatively, consider using a network access control solution, to make sure that these devices are up to date before being allowed access to your network resources (see the *Network Access Control* Network Security Task).
  - Suggestion: As much as possible, patching should be automatic. Remember that a reboot may be required for a patch to be properly applied. Be careful patching your servers, however, so they do not all reboot at once and affect your network availability.
  - Consider: All patches and updates for ICS/SCADA systems must be tested and evaluated on non-operational test beds (development systems) before installing them on any operational systems. When possible, tested and approved patches should be installed as soon as possible. Administrators for ICS/SCADA devices and networks should apprise management of the vulnerabilities and risks associated with unpatched ICS/SCADA devices.
  - Suggestion: As with any firmware or software, patches and updates should be verified to come from authorized or trusted sources, and tested so that they do not interfere with the proper functioning of your network. To harmonize this with the automatic patching suggestion above, consider automatically deploying first to a small, isolated subnet for testing (but be sure this testing reflects actual application usage!), and then to the rest of the network either after approval from the testing group, or after a brief time period with no problems found. Deploying patches in a tiered manner such as this also prevents your support personnel from being flooded with calls if something goes wrong.
  - Suggestion: For the Windows operating system and Microsoft applications, use Windows Server Update Services (WSUS) or an automated commercial solution. Windows workstations should be set to automatically apply patches. For operating systems other than Windows, consider using Puppet, Spacewalk, or custom scripts.
    - For more information on WSUS, see http://technet.microsoft.com/en-us/wsus/default
    - For more information on Puppet, see https://puppetlabs.com
    - For more information on Spacewalk, see http://spacewalk.redhat.com
  - Consider: Upgrade your systems to use UEFI and Secure Boot when feasible. Some hardware may not work with Secure Boot for various reasons. Be sure to do your research before upgrading your systems to UEFI and Secure Boot to ensure compatibility with your hardware and operating systems. Upgrade machines one at a time and test each machine after you upgrade it to ensure it still operates normally.
  - Suggestion: Review after patching your systems, to verify that the patches were applied correctly. As a sanity check, use different tools than those used for pushing out the patches.
  - Suggestion: For additional recommendations on patch management, see NIST Special Publication 800-40: “Guide to Enterprise Patch Management Technologies” (Available at http://csrc.nist.gov/publications/).

- Consider: A good software asset management system, including license management, will help in identifying and tracking the various software used on your network along with the license status of each instance of software. This information will ensure that you do not overlook software when running your patching process. For additional information on software asset management, see NIST National Cybersecurity Center of Excellence publication "Software Asset Management: Continuous Monitoring" (Available at https://nccoe.nist.gov/sites/default/files/SAM.pdf).

Documentation

- Document your patch management process. Consider documenting it in the device list from Milestone 2. For each device (or group of identical devices), include:
  - How often (on what schedule) patches should be applied,
  - How patches are downloaded, verified, and tested,
  - How the patches are applied (automatically or manually),
  - The procedures if any patches need to be applied manually,
  - How the patch application is verified,
  - Each specific system that warrants an exception from the patch management process, the reasons for the exception, and how this vulnerability of an unpatched system is being mitigated.

Consider

- **Non-Microsoft updates.** How will you update and patch non-Microsoft applications, such as Adobe Acrobat? What about device drivers and Web browser plug-ins? These unpatched third-party applications, etc. are a huge attack vector for malware.

Crucial Security Tip

  - Suggestion: In order to know when new releases become available for your approved non-Microsoft applications, have a generic e-mail alias that maps to all the administrators and subscribe to release announcements for those applications.
  - Suggestion: WSUS can also be used to patch third-party applications. See http://windowsitpro.com/article/patch-management/Secure-non-Microsoft-applications-by-publishing-3rd-party-updates-to-WSUS-129241.

- **BIOS and other firmware patches.** Firmware such as a computer's Basic Input/Output System (BIOS) operates in the background where it is invisible to users and system administrators except possibly during a computer's boot up phase. Hence, these are often overlooked. Consider how you will update and patch BIOS and other firmware on computers, network devices such as routers, and other devices connected to your network. The number one mitigation against firmware vulnerabilities is simply to update!

Crucial Security Tip

- **No end-of-life software/hardware.** Any software (or hardware) that you are using that is End-of-Life (EOL)—and thus no longer able to be patched—should be removed from your network as soon as possible. It is a serious security risk.
- **Using virtualization.** Consider if Software as a Service (SaaS), application virtualization, and/or desktop virtualization might be used in your patch management process. Patching and managing images stored in a central location may be more efficient in your environment than patching widely-distributed individual workstations. Be sure to consider all the potential security, usability, and downtime issues.
- **Update administrative tools.** Your administrative tools (both commercial and open source) must also be kept updated. This includes tools such as nmap, Wireshark, PuTTY, Puppet, your remote desktop solution, your patch management solution, your network access control solution, etc. In addition, any security solutions you use must be considered critical assets and kept updated so that they themselves do not become vulnerable to attacks and thus *decrease* the security of your network. Be sure your patch management process does not overlook all of these!

Ongoing

- Continue to execute the patch management process that you established in this Milestone.
- As necessary, update your patch management process and documentation.

Manageable Network Plan

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 6: Manage Your Network, Part I (Patch Management)
				Have you established and documented a patch management process for ALL the OS and application software on EVERY device on your network (workstations, servers, supporting devices, infrastructure devices, and mobile devices)? - Within each device category, % of devices actually patched via this process? - Within each device category, % of devices that are assessed by an automated capability that they are adequately free of vulnerabilities?
				Are you updating your patch management process and documentation as necessary?
				Have you gone over the points to consider for this Milestone?

Checklist date:

Milestone 7: Manage Your Network, Part II (Baseline Management)

Establishing and documenting what hardware and software is currently on your network and allowed on your network will enable you to identify licensing requirements, patch requirements, and recognize when unauthorized hardware and software has been introduced to your network.

To Do

- Create a list of all the applications that are approved for use on your network. For each application, specify its name and specific version, the reason it was approved, the network ports and protocols it uses (if applicable), and whether it is approved for general use or only within specified enterprise functions.
- Establish the criteria and process for getting an application on the approved list.
  - Suggestion: The reason for having an application on the approved list should never be just "Because so-and-so wants it." The application should always be justified by a business case, like "We need Adobe Flash on our Internet-connected boxes because our clients' websites use it."
  - Suggestion: Before an application is added to the approved list, it should be researched for any security issues. Consider how much you trust the application's developers—and their subcontractors—to deliver a product with no code from questionable sources and with a minimum of vulnerabilities. In addition, consider whether the application conflicts with any of your existing security policies, and how easily it can be updated. Application security is critical to the overall security of your network.
  - Suggestion: Before an application is added to the approved list, it should be tested to make sure that it does not do anything malicious, that it works with the other applications in the baseline, and that it will not interfere with your network. Consider setting up a small, isolated subnet for this testing.
  - Suggestion: Once an application is added to the approved list, your patch management process from Milestone 6 will need to be updated appropriately.
  - Suggestion: Implement restrictions so that only those applications that have been approved are allowed to execute on your network. Consider using application whitelisting (see the *Executable Content Restrictions* Network Security Task).
- Create device baselines (including for infrastructure devices and mobile devices). All software applications in a device baseline should be from the approved list for that device. Note that virtual machines and thin clients need baselines as well.
  - Suggestion: If similar devices are used in environments that require different capabilities or pose different threats, the devices should have different baselines. For example, the workstations used by developers should have a different baseline than those used by managers, because the managers will most likely not require all the applications and privileges that the developers will. Having more machines "customized" to users' specific needs and fewer generic machines will limit the damage that can be done if a machine is compromised.
  - Suggestion: When creating your device baselines, be sure to "harden" them by implementing the recommended security guidance for those devices. All software included in the baselines should be fully patched and correctly and securely configured. Remove unneeded components from default installs, disable unnecessary services, and change default (and blank) passwords to prevent their use by malware. Limit the number of cached credentials, implement screen lock timeouts, disable Windows auto-run, etc. In addition, be sure that your patch management process from Milestone 6 covers all software in your baselines.
    - **ICS/SCADA passwords.** In many ICS/SCADA networks, devices operate with a single system-wide password or a vendor installed default password. Vendors frequently publish online documentation including the default password and device access procedures. Unfortunately, changing passwords in an ICS/SCADA network is administratively difficult to nearly impossible after the system has been certified and is operational. You should consider these default and vendor-supplied passwords when making risk management decisions.
    - **Securing Web browsers.** Properly securing the Web browsers in your workstation baselines is extremely important: the Internet can be a dangerous place!
      - For suggestions on securing Internet Explorer, Firefox, Safari, and other Web browsers, see https://www.us-cert.gov/publications/securing-your-web-browser. In addition, consider

minimizing the number of plug-ins in the browser, as these might contain security vulnerabilities.
  - For guidance on Google Chrome, see NSA's "Deploying and Securing Google Chrome in a Windows Enterprise" (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml).
- The Microsoft Baseline Security Analyzer (MBSA) can be used to scan for security misconfigurations in your Microsoft baselines before deploying them. For more information on MBSA, see http://technet.microsoft.com/en-us/security/cc184924.aspx.
- The Center for Internet Security (http://cisecurity.org) provides benchmarks and tools for checking that your operating systems, applications, and devices (including Windows, Linux, Solaris, Apple, Oracle, Cisco, etc.) are configured securely.
- For additional configuration guidance, see the following:
  - NSA configuration guides (https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml)
  - NIST National Checklist Program (http://web.nvd.nist.gov/view/ncp/information)
  - DISA Security Technical Implementation Guides (STIGs) (http://iase.disa.mil/stigs/Pages/index.aspx)
  - US Government Configuration Baseline (USGCB, formerly FDCC) (http://usgcb.nist.gov)

Documentation

- Document the approved application list and the criteria and process for getting an application on the approved list.
- Document the device baselines.

Consider

- **Backing up offline.** Backup your baselines and store them offline. An adversary who gains access to network copies of your baselines may modify them.
- **Same password problem.** If you use an application to clone or "ghost" the same baseline image to multiple machines, keep in mind that every machine baselined this way will have the same local administrator/root account *and password*. Without ever having to crack the password, an attacker using a pass-the-hash technique could use the same password *hash* to compromise all your machines. If you consider this risk of compromise to be greater than the administrative overhead, either disable the local administrator accounts or manually change all the passwords.
  - Suggestion: If you manually change all the passwords, *do not* store them in a file or e-mail on the network! Instead, use a simple algorithm to generate each password. For example, append the last few characters of the machine name to the original common password. This way your administrators know all the passwords, but the password hashes are different across all your machines. This makes the pass-the-hash attack ineffective. It is not a foolproof solution, but it is better than all of your machines having the same password!
  - Suggestion: For more information on pass-the-hash attacks and step-by-step guidance for mitigations, see Microsoft's "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" (http://www.microsoft.com/en-us/download/details.aspx?id=36036). For expanded implementation guidance including scripts to use on a Windows network, see NSA's "Reducing the Effectiveness of Pass-the-Hash" (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml).
- **Verify device integrity.** On a regular basis, use system integrity checking tools to verify the integrity of the baseline installs on your devices. This is very important to discover any unauthorized changes. If possible, automate these integrity checks. In addition, consider periodically reimaging your devices, to ensure compliance. An added benefit of reimaging is that it will encourage your administrators to document system changes and fixes, so they do not have to "rediscover" them after the devices have been reimaged. Be careful that reimaging does not lead to unacceptable user disruption or data loss, and that any host-based security still performs properly on the reimaged devices.
  - Suggestion: As part of verifying that no unauthorized software is present on your devices, do regular checks for malware (see the *Virus Scanners and Host Intrusion Prevention Systems* Network Security Task).

- **Automatic reboots.** Consider setting your workstations to automatically reboot on a regular basis (for example, every night) to keep any small problems from accumulating, clear up any memory issues, etc. Consider scheduling a server task to reboot all your workstations remotely; having this task on the server allows it to be easily adjusted for special situations, instead of having to modify a script on each individual machine. Be careful that rebooting does not lead to user disruptions (for example, if someone is working late), hardware failure, or data corruption if a process is interrupted.
- **Hardware configurations.** Do the baselines for your devices also include their hardware configurations? Some things to consider in this area might be disabling or removing wireless cards, setting the boot order in the BIOS to hard drive only, and creating BIOS passwords. In addition, make sure that your systems support signed BIOS updates (check with your vendor), to help prevent unauthorized BIOS modifications.
  - Suggestion: Limit your hardware based on the capabilities needed and the threats posed. For example, not all of your laptops may need built-in microphones, cameras, and wireless capability. Not all of your workstations may need USB ports, huge hard drives, powerful graphics cards, and CD/DVD writers. (As a bonus, this may reduce your power and cooling requirements!)
  - Suggestion: If available, use tools to calculate the BIOS checksums of your devices and record those values in a safe place. Be sure to update the checksums whenever you "flash" a BIOS.
  - Suggestion: Trusted Platform Modules (TPM) is a component of several security solutions. It is easiest to activate and provision TPMs when a device is added to the network. Keep abreast of developments in TPM as they apply to virtualized environments and mobile devices such as smartphones.
- **Supply chain risk management.** Your supply chain is everything and everyone involved in getting products, systems, and services to your organization. It impacts the full system development life cycle, from R&D and acquisition to disposal. The modern IT supply chain is complex and international, and subject to a variety of threats such as counterfeiting, tampering, theft, and the introduction of unwanted functionality and malicious content. Consider how your organization will deal with these risks. For more information and a set of best practices, see NIST Special Publication 800-161: "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" (Available at http://csrc.nist.gov/publications/).
  - Consider: ICS/SCADA components have a service life in excess of 15 years. There is a high probability that when a hardware failure occurs, a direct replacement part may not be available from the original equipment manufacturer. Consequently you may be required to obtain used components from an untrusted source. The integrity of used components must be considered compromised and steps must be followed to sanitize and initialize the device to a known good state. Your administrators can use trusted copies of the software from their secure storage.

Ongoing

- Update your device baselines on a regular basis. As far as possible, baselines should contain the latest versions of operating system and application software. Baselines should never contain software or hardware that is end-of-life and no longer supported.
- Update your approved application list, criteria and process for getting an application on the approved list, and baselines documentation whenever there is a change.
- From now on, whenever a device is added or replaced on your network, the new device should conform to the appropriate baseline. If the device cannot be wiped and re-baselined, consider a network access control solution (see the *Network Access Control* Network Security Task), or quarantining the device.
- As time permits, any installed applications and services that are not approved should be removed from the network.
- As time permits, reimage current devices with the appropriate baseline.
- Update BIOS checksums whenever you "flash" a BIOS.
- Activate and provision TPM on devices as they are added to the network.

Manageable Network Plan

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 7: Manage Your Network, Part II (Baseline Management)
				Have you created and documented a list of all the applications that are approved for use on your network? - Within each device category, % of devices that have an automated capability to prevent or restrict execution of unapproved applications and other unapproved executable content? (Higher % is more secure)
				Have you established and documented the criteria and process for getting an application on the approved list?
				Have you created and documented device baselines (including for infrastructure devices and mobile devices)? - Within each device category, % of devices actually covered by a documented baseline? - Within each device category, % of devices that are compliant with their documented baseline (no changes or additions)? - Within each device category, % of devices that have an automated capability to verify compliance (detect changes and additions)?
				Are you updating your device baselines on a regular basis?
				Are you updating your approved application list, criteria and process for getting an application on the approved list, and baselines documentation whenever there is a change?
				Have you gone over the points to consider for this Milestone?

Checklist date:

Milestone 8: Document Your Network

As time permits, your processes and procedures for your network should be documented. This helps keep your network manageable. Even if you only have time to document one process per week, that is still better than nothing! Be sure to give priority to documenting those things that are most important to keeping your organization doing business.

Documentation

- Document full procedures to rebuild servers and other important devices on the network, in case of catastrophic failure. (Ideally, this should be done within the context of a comprehensive contingency plan; see the *Incident Response and Disaster Recovery Plans* Network Security Task.) Do not forget to include your ICS/SCADA devices!
- Document all administrative processes and procedures used on your network. Obviously, an exhaustive list of what to document cannot be provided because each network will be different. However, for ANY network, four very important procedures to document are:
    1. How to add a new user
    2. How (and when) to remove a user
    3. How to add a new system
    4. How to remove a system

Consider

- **Completeness.** Consider the following scenario to determine if your documentation is complete and up-to-date: Suppose one of your most knowledgeable administrators cannot be contacted for an extended period of time. Will your network grind to a halt? Will it explode in chaos? What does that administrator know that is not written down? To test if you have thought of everything, have that administrator go on vacation… (Incidentally, "job security" is not a valid reason for not documenting!)
- **Hard copy.** Keep hard copies of your processes and procedures on hand, in case of emergencies. Keep duplicate copies at your continuity of operations site, in case of more serious emergencies.
- **Always followed.** The documented procedures should always be followed. Are they? Are new network administrators required to become familiar with and use this documentation?

Ongoing

- As time permits, continue to document your administrative processes and procedures.
- All documentation must be reviewed periodically (for example, annually) and updated as necessary. Consider occasionally hiring a technical writer to gather, clarify, and maintain your documentation.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 8: Document Your Network
				Are the procedures to rebuild servers and other important devices on your network fully documented and kept up to date?
				Are the procedures for adding and removing users and systems from your network fully documented and kept up to date?
				As time permits, are you documenting all other administrative processes and procedures, and keeping them up to date?
				Have you gone over the points to consider for this Milestone?

Checklist date:

And Now…

Congratulations! You now have a manageable network!

Ongoing

To recap, here are the ongoing tasks you should now be doing on your network. Look for cost-effective ways to automate these!

- ✓ Documenting whenever a change is made to your network or to the devices on your network
- ✓ Updating paperwork for newly hired system administrators to reflect the location of documentation as well as requirements and expectations for documentation
- ✓ Updating the network map and list of devices any time a device is added to or removed from the network
- ✓ Updating the list of protocols any time a new protocol is added to your network, or an old protocol is no longer used
- ✓ Periodically using tools to check your network map and your lists of devices and protocols for accuracy
- ✓ Updating your documentation whenever your network enclaves, high-value assets, or choke points change
- ✓ Periodically re-evaluating your network architecture, to determine if it still meets your security and manageability requirements
- ✓ As necessary, updating your device access/administration process and documentation
- ✓ For each of your users that has elevated privileges, regularly reviewing the reasons for this and removing the privileges when the reasons are no longer valid or no longer justifiable
- ✓ Periodically verifying that all accounts on your network are tied to specific, current, authorized users and disabling/removing accounts that cannot be verified
- ✓ Periodically analyzing, surveying, and assessing vulnerabilities to further evaluate user activity and mishandling of privileged accounts
- ✓ Continuing to execute your patch management process
- ✓ As necessary, updating your patch management process and documentation
- ✓ Updating device baselines on a regular basis
- ✓ Updating approved application lists, criteria and process for getting an application on the approved list, and baselining documentation whenever there is a change
- ✓ Whenever a device is added or replaced on your network, making sure the new device conforms to the appropriate baseline
- ✓ As time permits, removing any installed applications and services that are not approved
- ✓ As time permits, reimaging current devices with the appropriate baseline
- ✓ Updating BIOS checksums whenever you “flash” a BIOS
- ✓ Activating and provisioning TPM on devices as they are added to the network
- ✓ As time permits, documenting all administrative processes and procedures
- ✓ Periodically reviewing all documentation and updating it as necessary

Documentation

Develop checklists (e.g., daily, monthly, yearly) to remind administrators of activities that need to be carried out on a regular basis.

Consider

At this point, you can begin to consider adding additional features and security to your network. See the *Network Security Tasks* that follow.

Network Security Tasks

Once your network is manageable, you can begin to consider adding additional features and security to it. If your network is not manageable, or only barely manageable, it will be painfully difficult for you to fully implement *any* security measures. Once your network is manageable, you will be able to consider and implement security measures—and verify their implementation—much more efficiently and effectively. A tool that will help with implementing security on a network or information system is often referred to as a System Security Plan (SSP). The SSP becomes a standard by which security-related changes to a network or information system can be compared to determine the impact of a particular change. More information on SSPs may be found in NIST Special Publication 800-18: "Guide for Developing Security Plans for Federal Information Systems" (Available at http://csrc.nist.gov/publications/).

The following are security-related tasks to consider implementing on your network once it is manageable. Obviously, which of these you implement and what order you implement them will be specific to your network. Be sure to document everything you do in sufficient detail. Remember that each of these tasks requires man-hours both to implement and to maintain; if a task is not properly staffed, it will not be beneficial—and may even be detrimental—to your network. Make sure you include the cost of this additional manpower in any cost-benefit analysis you do.

These tasks present things to consider; they only occasionally offer specific guidance, in the form of suggestions and references to additional material. The implementation details are going to be network specific and can be handled far better by the individual network's CIO and administrators. The best thing to do is to give your administrators some research time to find the best solution for your specific network, and then give them time to implement and configure it correctly.

Business Functionality Tasks

Backup Strategy

A comprehensive backup strategy for your network is needed to ensure business continuity in the event of unexpected failure or data loss. Your strategy should address *what* gets backed up, *when* it gets backed up, *where* the backup media are stored, and *how* to restore from backup media. Your strategy should be documented and kept updated. Be sure to regularly test the restore part of your strategy! Storing your backups in a physically secure area will help ensure they are protected from unauthorized modification.

- Suggestion: Encrypt your backups to prevent compromise of your data.
- Consider: If you outsource your backup storage, be sure that you have full confidence in the vendor who provides this service. A crisis situation is not the time to discover that there are problems!

Incident Response and Disaster Recovery Plans

Sooner or later, something bad will happen on your network. Without plans for incident response and disaster recovery, you will lose valuable information and possibly business. Your plans should be documented, regularly tested, and kept updated.

- Consider: If your organization does not have the skills, resources, or time to do a good job of cleaning up your network after a security incident, call in the professionals! Doing a poor job of eradicating an intrusion and then having to spend more money to fix the mess is much worse than spending the little

extra to get it done right the first time. An important part of your incident response plan should be to define which types of incidents you can handle yourself and which types you cannot.

- Suggestion: Read *Incident Response & Computer Forensics, Third Edition* by Luttgens, Pepe, and Mandia (McGraw-Hill/Osborne, 2014), especially Chapter 2 ("IR Management Handbook") and Chapter 3 ("Pre-Incident Preparation").
- Suggestion: For some considerations on remediation, see
  https://www.mandiant.com/blog/challenges-remediating-apt/,
  https://www.mandiant.com/blog/avoid-knee-jerk-reaction/,
  https://www.mandiant.com/blog/dod-cyber-crime-conference-presentation-recipes-remediation/,
  https://www.mandiant.com/blog/black-hat-usa-2012-presentation-targeted-intrusion-remediation-lessons-front-lines/, and
  https://dl.mandiant.com/EE/library/BH2012_Aldridge_RemediationPaper.pdf.[5]
- Suggestion: For additional recommendations on incident response, see the following NIST Special Publications (Available at http://csrc.nist.gov/publications/):
  - SP 800-61: "Computer Security Incident Handling Guide"
  - SP 800-83: "Guide to Malware Incident Prevention and Handling for Desktops and Laptops"
- Suggestion: For additional recommendations on contingency planning, see NIST Special Publication 800-34: "Contingency Planning Guide for Federal Information Systems" (Available at http://csrc.nist.gov/publications/).
- Consider: If your network is integrated with "the cloud", be sure you and your cloud provider(s) have agreements codified in contracts and SLAs on how to recognize and handle incidents and disasters.
- Consider: After an incident, review your incident response and disaster recovery plans and update them to include any lessons learned.

Security Policy

According to the "Site Security Handbook" (RFC 2196), "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide." In other words, your security policy specifies how your network is to be used. Your security policy should be reviewed at least yearly to check that it matches what you are currently doing.

- Consider: In and of itself, a security policy provides *no protection* for your network. Your security policy must be technically and automatically enforced to have benefit. Is security enforced automatically on your network so you do not have to just rely on users to remember your policies?
- Suggestion: Your security policy should include the following sections:
  - *Acceptable Use Policy,* defining how the organization's computer equipment and network resources are to be used
  - *Privacy Policy,* specifying employee expectations of privacy regarding monitoring of email, keystrokes, and access to their files
  - Depending on your organization's security posture, other policy sections that may be important for your network include an Access Policy that specifies permissible access to network resources and permissible connections to other networks and devices; an Accountability Policy that specifies responsibilities of employees and how incidents will be handled; a Password Policy; Purchasing and Disposal Guidelines; etc.
  - *User Agreement,* which employees must sign, stating that they agree to comply with the security policy
- Suggestion: For more information on security policy development and implementation, see the SANS Security Policy Project website (http://www.sans.org/security-resources/policies).
- Suggestion: Make sure your security policy is not so restrictive that it annoys your users, or they will find ways to get around it.

[5] The NSA makes no endorsement of the services offered by this company.

Training

People need training. Training allows your administrators to learn from the pros and meet people they can contact (possibly for free) if they have a problem. Users need regular training so they are aware of how your network should and should not be used. Managers need training to learn how they can better enable and support the administrators trying to manage and secure the organization's network. Training should be interactive, hands-on, and useful.

- Consider: Are your administrators certified? Certification helps ensure a baseline level of understanding of IT functions and lends credibility to the IT staff.
- Consider: Do you have management buy-in for needed network security changes? If not, management may require better presentation of the reasons why the changes are needed, and what the results of *not* implementing the changes could be.
- Consider: Do your users know what is in your *current* security policy?

Crucial Security Tip

- Consider: If there is a security breach, your users may notice odd things happening on their computers and the network long before the administrators do. Do your users know to report these things? Do they know *how* and *to whom* to report these things? If an alert from one of your network security solutions pops up on their screen, do your users know what to do?
- Suggestion: The Defense Information Systems Agency (DISA) has many training courses available for free on a variety of Information Assurance topics. These courses are available on CD and/or online. For more information, see http://iase.disa.mil/eta/online-catalog.html.
- Suggestion: For additional recommendations on training, see the following NIST publications (Available at http://csrc.nist.gov/publications/):
  - ITL Bulletin October 2003: "Information Technology Security Awareness, Training, Education, and Certification"
  - SP 800-16: "Information Technology Security Training Requirements: A Role- and Performance-Based Model"
  - SP 800-50: "Building an Information Technology Security Awareness and Training Program"

Host-Based Security Tasks

Executable Content Restrictions

The only applications and code that should run on your operational network should be applications and code that you have approved. Unapproved—and possibly malicious—code should not be allowed to run, as this may compromise your network.

Crucial Security Tip

- Suggestion: Unapproved applications (those not in your baselines from Milestone 7) should not be allowed to run. This can be enforced through application whitelisting, using Windows Software Restriction Policies (SRP), Windows AppLocker, or a commercial solution.
  - For more information on using SRP for location-based application whitelisting, see NSA's "Application Whitelisting Using Software Restriction Policies" (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml).
  - Windows AppLocker is the new version of SRP for Windows 7 and Windows Server 2008 R2, with a better implementation, new features, and more flexibility. SRP is still supported for backwards compatibility; for example, if you have a mixed network of XP, Vista, and Windows 7, then you can set up SRP rules and all three OS versions will enforce them. For more information on AppLocker, see http://technet.microsoft.com/en-us/library/dd548340(WS.10).aspx.
  - For more information on application whitelisting see "Application Whitelisting" trifold and factsheet (Available at https://www.nsa.gov/ia/_files/factsheets/Application_Whitelisting_Trifold_Jan_2013.pdf and https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/SlickSheet_ApplicationWhitelisting_Standard.pdf). For detailed information for various Windows operating systems see "Application Whitelisting Using Software Restriction Policies" (Available at https://www.nsa.gov/ia/_files/os/win2k/Application_Whitelisting_Using_SRP.pdf) and "Application Whitelisting Using Microsoft AppLocker" (Available at https://www.nsa.gov/ia/_files/app/Application_Whitelisting_Using_Microsoft_AppLocker_FINAL.pdf).
  - On Linux/Unix, execution restrictions can be enforced by mounting world-writable directories (e.g., /tmp) as separate partitions with the noexec option enabled. On Mac OS X, the Parental Controls can be used to prevent unapproved applications from launching.
- Suggestion: If an application becomes infected by malware, it must be prevented from doing things it should not be doing. Various techniques can be used to enforce this, first and foremost by having your users not run as administrator. Other techniques include Data Execution Prevention (DEP), Address

Space Layout Randomization (ASLR), Linux mandatory access control technology (such as SELinux), and UNIX chroot "jails". Host Intrusion Prevention Systems (HIPS) can also be used to enforce execution restrictions.

Crucial Security Tip

- Suggestion: The Enhanced Mitigation Experience Toolkit (EMET) is a free Windows utility that can use techniques such as DEP, ASLR, certificate pinning, etc. to help prevent vulnerabilities in software from being exploited. EMET can be configured to protect *any* software running on Windows, no matter when or by whom it was written (legacy apps, Web browsers, media players, Microsoft Office products, Adobe products, Java, etc.). For more information on EMET, see http://support.microsoft.com/kb/2458544. Note that EMET might prevent legitimate programs from working, so be sure to test before deploying.
- Suggestion: Microsoft Office documents are often used to deliver malicious code. If you use Office, upgrade to Office 2007 or later, which uses the newer Open XML file formats. Office 2010 offers additional protection by opening documents from untrusted sources in a read-only isolated sandbox known as "Protected View".
  - If you cannot immediately upgrade to Office 2007 or later, use the Microsoft Office Isolated Conversion Environment (MOICE) to sanitize your Office documents when they are opened, before any malicious code can execute.
- Suggestion: Consider accessing high-risk applications and files (Web browsers, e-mail clients, files downloaded from the Internet, etc.) within a virtual machine (VM). This can help keep malware and malicious mobile code (such as malicious JavaScript, Java applets, Flash animations, and embedded macros) contained. If the VM becomes compromised, it can be reverted to a known good state and the host computer remains unaffected. However, note that if transferring files out of the VM is allowed, or the VM has network connectivity to unprotected hosts, then your network could still become compromised.

Virus Scanners and Host Intrusion Prevention Systems (HIPS)

A host-based virus scanner detects and removes known threats; a Host Intrusion Prevention System (HIPS) detects suspicious host behavior to protect against not-yet-known threats. Your hosts need protection from both kinds of threats (many product suites include both technologies). All of your hosts should employ a HIPS and should regularly run virus scans. Also, the virus scanners and HIPS must be kept up to date.

- Suggestion: Many host security products offer file reputation services that rate the trustworthiness of files by checking them against online global threat databases. Using such services can improve the malware detection accuracy of the security products.
- Suggestion: A HIPS usually has an adaptive or "learning" mode to help ease its integration into your network defenses. This mode "learns" what network traffic normally flows to and from your hosts and automatically creates rules to allow that traffic. DO NOT leave the HIPS in this mode indefinitely! Otherwise, when a network attack happens, the HIPS will just automatically create a rule to allow it.
- Consider: A HIPS provides administrators with great flexibility in securing their networks, but it is expensive, and time-consuming to configure and monitor. Protection roughly equivalent to a basic default HIPS installation can be obtained by using the following four technologies on each host (note that all four are needed):
  - Host firewall
  - Buffer overflow protection (such as DEP, mentioned above)
  - Program execution blocking (such as AppLocker or SRP, mentioned above)
  - Virus scanner with real time protection ("guard") functionality enabled.

Personal Electronic Device (PED) and Removable Media Management

Without proper management of Personal Electronic Devices (BlackBerry devices, iPhones, etc.) and removable media, unauthorized devices will be connected to your operational systems. Data could be stolen or malicious software unknowingly transferred.

- Suggestion: As with any device that will be connected to your network, personal electronic devices should only be supplied and supported by authorized or trusted vendors. If necessary, limit the functionality of these devices to reduce the risk to your organization.
- Suggestion: Your security policy should specify what can and cannot be connected to workstations by users. However, this must be enforced ("device whitelisting") so you do not have to just rely on users to remember your

policy. Consider using an endpoint device control or endpoint data loss prevention (DLP) security application to do this enforcement automatically. (See also the *Network Access Control* Network Security Task.)
  - In Windows Vista and later, Group Policy can be used to do this enforcement. For more information, see http://technet.microsoft.com/en-us/library/cc731387(WS.10).aspx.

- Suggestion: Implement mitigations to defend your network hosts from potential malware on removable media such as CDs, DVDs, floppy disks, flash memory cards, and USB drives. For suggestions and more information, see the "Defense against Malware on Removable Media" NSA Fact Sheet (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).
- Suggestion: Use a mobile device management (MDM) solution to ensure that the mobile devices on your network are properly configured and secured. For more information on the capabilities of MDM solutions and security issues to consider, see the "Mobile Device Management: A Risk Discussion for IT Decision Makers" NSA Fact Sheet (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).
- Suggestion: For iPhone and iPad security tips, see the "Security Tips for Personally-Managed Apple iPhones and iPads" NSA Fact Sheet (Available at http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml). For information on managing iOS devices in an enterprise, see http://www.apple.com/support/iphone/enterprise.
- Suggestion: For BlackBerry and Android devices, a mobile device integrity solution can be used to help ensure that the devices have remained in a secure state without being compromised. For U.S. Government organizations, a free tool (Sentinel AutoBerry) is available at https://www.iad.gov, under Mitigations - Tools.
- Suggestion: For smartphone and tablet security implementation guides from DISA (including for iOS, Android, BlackBerry, etc.), see http://iase.disa.mil/stigs/net_perimeter/wireless/Pages1/index.aspx.
- Suggestion: For additional recommendations on Personal Electronic device security, see NIST Special Publication 800-124: "Guidelines for Managing the Security of Mobile Devices in the Enterprise" (Available at http://csrc.nist.gov/publications/).

Data-at-Rest Protection

Without proper protection, your sensitive data is vulnerable to unauthorized access, modification, destruction, and disclosure. Data stored on servers and workstations is at risk from network intruders. Data stored on mobile devices (such as laptops and smartphones) and removable media (such as CDs/DVDs, SD cards, USB drives, and hard drives in removable caddies/trays) is at risk if the device/media is lost or stolen. In all these cases, the primary ways to protect your sensitive data are through access controls and encryption.

- Consider: The best data protection is to *not use or store* sensitive data in insecure places, or places not under your control where it will persist for a long time. Is it really necessary to send your sensitive data via e-mail? Or store it on mobile devices? Or save it on a shared drive that someone with no need to know can access?
- Suggestion: For U.S. Government organizations, encryption of sensitive but unclassified data must use approved algorithms and key lengths. Other organizations should also consider using these criteria. For information on what algorithms are currently approved and when they are to be phased out, see NIST Special Publication 800-131A: "Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" (Available at http://csrc.nist.gov/publications/).
- Suggestion: Use either a software or hardware encryption solution to encrypt data automatically when it is written to a device or to removable media. Be sure to *not* then store the decryption key on the device/media.
- Consider: Some mobile devices do not offer full-disk encryption; however, they may support encryption of data stored in certain areas. In addition, some mobile devices offer a "self-destruct" (data wipe) capability that can be activated remotely or if someone fails logging on too many times.
- Consider: Many ICS/SCADA systems do not use any encryption on data at rest. Access to the primary database by unauthorized persons will allow them to view data stored on ICS/SCADA devices as well as delete, change or add data, and change the system configuration definitions. Any unauthorized change could result in shutdowns, damage, or product tampering. If control system data is needed by entities outside of the control system network, then a second copy of the database should be created on a server outside of the control system network. The primary and copy database should be separated by a firewall or data diode that will only permit pushing of data from the primary

to the copy database. Corporate queries or malicious attacks against the copy database will then have no effect on the primary database. The primary will continue to function without the need for encryption that may slow or hamper required access to the primary database by the control system.

- Suggestion: For additional recommendations on data-at-rest protection, see NIST Special Publication 800-111: "Guide to Storage Encryption Technologies for End User Devices" (Available at http://csrc.nist.gov/publications/). Appendix A of this NIST document contains some alternatives to encryption.
- **Data loss prevention.** Data loss prevention (DLP) is a comprehensive approach to discover, monitor, and protect data wherever it is stored, used, or transferred over a network. DLP solutions can be either host-based or network-based, and typically use a method of tagging data or discovering data that match defined patterns, so that the data can be tracked and access to it controlled.
  - A malicious insider—who already has legitimate access—poses a particularly serious threat for data loss. For more information and mitigation recommendations, see the CERT "Common Sense Guide to Mitigating Insider Threats" (http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm).
- **Data spillage.** Data spillage is the transfer (either accidental or intentional) of classified or sensitive information to unauthorized systems, individuals, applications, or media. Organizations should have an appropriate policy in place on how to handle data spills. For recommendations on handling data spills, see the "Securing Data and Handling Spillage Events" NSA Fact Sheet (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).

Network Monitoring and Control Tasks

Network Access Control (NAC)

When someone plugs a device into your network, that device should not automatically have access to everything. Unauthorized "rogue" devices and devices that are misconfigured, behind in patches or malware scans, etc. should be prevented from accessing your network resources, because they may open up vulnerabilities on your internal network. This applies especially in BYOD ("Bring Your Own Device") environments. Devices (and any users of the devices) should be denied access to your network resources until after a verification and authentication procedure.

- Suggestion: For basic access control, configure your network switches to only allow certain MAC addresses to connect to their physical ports (port-based authentication, or port security) or implement IEEE 802.1X, where client machines must authenticate at the network layer before gaining access to network resources.
  - Whenever possible, require client machines to authenticate using certificates (which, unlike MAC addresses, generally cannot be spoofed). Record these certificates with their associated devices in the device list from Milestone 2.
  - For your mobile devices, be sure that your NAC solution and your MDM solution are compatible.
- Suggestion: For more robust access control, use a Comply-to-Connect (C2C) solution. A C2C solution can, for example, assign machines connected to your network to separate VLANs based on device type, initial (and even ongoing) health and configuration checks and policies that you set. C2C is an automated Network Access Control (NAC) solution that verifies that an endpoint is authorized and meets security requirements before allowing access to the network. C2C can take automated security actions to enforce network security requirement and provide continuous network monitoring for deviations from these requirements.
- Consider: If you have machines that have not been connected to the network for a period of time (such as laptops taken on business trips) and so have fallen behind with patches and configuration, you can use Windows Active Directory to prevent those machines from connecting to your internal network. Place each such machine into a "disabled" OU that has no access to internal network resources. The user of the machine will then have to call in and get his machine properly updated, after which the machine can be placed back into its proper OU.
- **User authentication.** Users must also be authenticated before they are allowed access to your network resources. Your network likely has an authentication mechanism in place already; however, your authentication process may not be as robust as it should be, or your authentication

mechanism itself may be vulnerable to attack. For more information and suggestions on hardening this critical piece of your infrastructure, see the following:

- "Hardening Authentication" NSA Fact Sheet (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml)
- NIST Special Publication 800-63: "Electronic Authentication Guideline" (Available at http://csrc.nist.gov/publications/)

Security Gateways, Proxies, and Firewalls

Security gateways, proxies, and firewalls can examine traffic and provide a way to allow, deny, or modify the traffic between nodes. These devices should be placed at the choke points on your network, so that sensitive information is adequately segregated from the rest of the network by means of the infrastructure.

- **White-listing vs. black-listing.** When generating rule sets for your gateways, proxies, firewalls, or any other type of access control, keep in mind that white-listing (specify trusted and deny everything else) is generally more effective than black-listing (specify untrusted and allow everything else). This is because it is impossible to list *everything* that is untrusted in your black list.
- Suggestion: Direct all your e-mail traffic through a gateway. Consider doing filtering, virus scanning, or blocking of attachments there. Also consider doing spam blocking and domain enforcement (for example, e-mails from outside that appear to originate from inside are blocked).
  - E-mail spoofing, e-mail spam, and phishing attacks can be reduced by using the Sender Policy Framework (SPF) or Microsoft's Sender ID, both of which use the Domain Name System (DNS) to verify that a received e-mail comes from the domain that it claims to originate from. Related technologies to authenticate the content of e-mail header information include Secure MIME (S/MIME), Pretty Good Privacy (PGP), and DomainKeys Identified Mail (DKIM).
- Suggestion: Direct all your Web traffic through a proxy or secure Web gateway; your workstations should never directly connect outside of your network. Consider blocking or restricting downloads there. Inspect all Web application traffic for common attacks such as cross-site scripting and SQL injection (a Web application firewall can also do this). In addition, various commercial services offer feeds rating the trustworthiness of Web domains; consider screening Web access requests against such services and redirecting dangerous requests to a warning page.
- Consider: For your firewalls, consider whether they should be simple packet-filtering, stateful inspection, or application-proxy firewalls. Besides doing ingress filtering, also do egress filtering: do not allow any traffic to leave from a workstation or server on your network that is not absolutely essential for that machine to fulfill its role. This can help contain attacks, as it will likely prevent any malware from "phoning home". Rate-limiting (throttling) can also be used to protect your network from (and keep it from contributing to) denial of service attacks.
  - For recommendations on configuring firewalls, see NIST Special Publication 800-41: "Guidelines on Firewalls and Firewall Policy" (Available at http://csrc.nist.gov/publications/).

Out-of-band Management

Out-of-band (OOB) management uses dedicated channels for managing network-connected devices, generally remotely. These management channels may be implemented as a separate physical infrastructure or as virtual encrypted channels (using the same medium as in-band channels) with the decision typically driven by cost. This enables the network administrator to improve security by separating user traffic from OOB management traffic. Additionally, a separate physical infrastructure increases the likelihood of maintaining management connectivity independent of the working state of in-band network components.

Crucial Security Tips

- Consider: Limit the services and protocols used on OOB management channels to those that are actually required.
- Consider: Manage all administrative functions over secure, encrypted channels from fully patched dedicated hosts accessible only by network administrators. Recommend using at least two such hosts to provide redundancy should one of the hosts fail.
- Consider: Use Simple Network Management Protocol (SNMP) version 3 or newer. Upgrade or replace SNMP version 1 and version 2 devices as soon as practicable.
- Consider: Apply encryption to all OOB management channels, including remote dial-up. Encryption should be used even when a separate physical OOB infrastructure is implemented.

Remote Access Security

Remote access (wireless access, people accessing your network from home, etc.) can be difficult to secure. First consider: Should users be allowed remote access to your network? Should administrators be able to access and control your network from home? If so, make sure that unauthorized people cannot access your network because of insecure protocols or security mechanisms.

Crucial Security Tip

- Suggestion: Limit the access that remote devices have to your network, place them in quarantine, or subject them to increased monitoring. Remote access clients should never be allowed to connect directly to your internal network; they should connect to a DMZ (demilitarized zone) so they at least have to go through a firewall to get to the internal network. In addition, strong authentication should be enforced for remote access users. Consider using a network access control solution (see the *Network Access Control* Network Security Task).
- Suggestion: Require users accessing your network remotely to use a secure Virtual Private Network (VPN) and to only access the network from company-owned machines. Require ALL traffic to go through the VPN; do not allow split-tunnels. All VPN traffic should be inspected (*after* it is decrypted) before it is allowed to interact with any of your network resources.
- Suggestion: Use secure wireless protocols. If you are using a legacy IEEE 802.11 wireless implementation with WEP-based security, move to IEEE 802.11i/WPA2-based security: WEP has serious security flaws. Disable Wi-Fi Protected Setup (WPS), as WPS may allow compromise of WPA2. Authenticate your wireless users by using a TACACS+ or RADIUS server, or VPN solution.

  For additional recommendations on wireless security, see the following NIST Special Publications (Available at http://csrc.nist.gov/publications/):
  - SP 800-48: "Guide to Securing Legacy IEEE 802.11 Wireless Networks"
  - SP 800-97: "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i"
  - SP 800-121: "Guide to Bluetooth Security"
  - SP 800-153: "Guidelines for Securing Wireless Local Area Networks (WLANs)"
- Suggestion: Regularly audit your remote access. Make sure that you know in general *who* is accessing your network and *how* they are accessing it. You also need to know *when* they are accessing your network and, in general, *what* they are doing, so you can spot any anomalous activity.
- Suggestion: For additional recommendations on remote access security, see the following NIST Special Publications (Available at http://csrc.nist.gov/publications/):
  - SP 800-46: "Guide to Enterprise Telework and Remote Access Security"
  - SP 800-114: "User's Guide to Securing External Devices for Telework and Remote Access"

Network Security Monitoring

No matter how much time and effort you devote to preventing problems on your network, eventually something will go wrong. *Prevention eventually fails!* Without knowing what is happening on your network, you will be unable to detect problems early. By knowing what traffic normally flows through your network ("baselining"), you will be able to detect anomalies (unexpected traffic occurring; expected traffic dropping out). Your network security monitoring solution should be configurable and precise enough so that you can quickly adjust it to monitor select traffic more in depth if you suspect a problem or infection. Be sure you have a process in place for what to do when a problem is found.

- Suggestion: Read *The Practice of Network Security Monitoring* by Richard Bejtlich (No Starch Press, 2013) and consider also reading the prequels, *The Tao of Network Security Monitoring Beyond Intrusion Detection* (Addison-Wesley, 2004) and *Extrusion Detection* (Addison-Wesley, 2005). Mr. Bejtlich advocates network security monitoring as the *first* step to take to secure a network (http://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html and http://taosecurity.blogspot.com/2009/03/requirements-for-defensible-network.html).[6]
- Suggestion: Consider implementing a system so that network administrators are automatically informed when anomalous events occur. In some cases, the system could even actively respond by automatically altering device configurations to protect the network from known threats. But remember, an automated system *will not* detect all anomalies! A team of experts (either internal, external, or in partnership with other organizations) must still conduct regular log reviews, looking for new problems and new attacks.

[6] The NSA makes no endorsement of the services offered on this website.

- Suggestion: Consider using a network intrusion detection/prevention system (IDS/IPS), such as Snort (https://www.snort.org). Note that for quick response—like when your network is under attack—preconfigured versions of Snort are available on live CD/DVD. Other IDS/IPS options are available besides Snort. There are some Linux distributions available that specialize in network security monitoring and include many useful tools. One such distribution is Security Onion (http://sourceforge.net/projects/security-onion).
  - For recommendations on using intrusion detection and prevention systems, see NIST Special Publication 800-94: "Guide to Intrusion Detection and Prevention Systems (IDPS)" (Available at http://csrc.nist.gov/publications/).
- Consider: Is your monitoring solution effective not only at the edge of your network (external threats), but also *inside* your network, such as at choke points and trust boundaries (insider threats)? Can it monitor OOB management activities?
- Consider: Ensure that your monitoring solution does not become an avenue for unauthorized entry into your OOB management channels.
- Consider: Passive monitoring only detects bad things *after* they happen. To discover potential threats *before* they strike, use proactive malware-hunt tools and techniques.
- Consider: Routinely test your detection methods to ensure they work.

Log Management

Your logs (gateway, proxy, and firewall logs, router logs, IDS logs, DNS logs, host OS logs, virus scan and HIPS alerts, network flow data, etc.) contain information that can help with troubleshooting, compliance, incident response, and statistics. However, these logs can rapidly become completely unmanageable and hence, completely ignored. Having a way to manage and protect these log files will ensure that you will be able to retrieve information when you need it. Configure your logging to provide sufficient useful information, but not too much: for example, only record events at warning level and above. Your logs should be reviewed regularly—more often if you suspect a problem or infection. Be sure you review your logs within a short enough time from when they were generated so as to be actually useful—it is no good first noticing malicious activity a year after it happened!

- Suggestion: Deploy a centralized logging solution. Consider using syslog, an application like Splunk (http://www.splunk.com) or Snare (http://sourceforge.net/projects/snare), or a commercial Security Information and Event Management (SIEM) solution.
  - For the Windows OS, built-in tools can be used to do centralized event logging. For implementation guidance as well as recommendations on what to look for in the logs, see NSA's "Spotting the Adversary with Windows Event Log Monitoring" (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml).
  - Restrict access to your central log servers. To enable proper oversight (and defend against insider threats), administrators who make changes on your network should not also be able to modify the logs of those changes recorded at the central log server. If an administrator disables logging on a device, a record of that must be preserved at the central log server.
  - If your network includes virtual machines, be sure your log management solution supports retention of transient log data from virtual sessions, and event correlation and user attribution across virtual sessions.
- Suggestion: Time synchronization in your logs is very important, so that events can be properly correlated. Use Network Time Protocol (NTP).
- Suggestion: Consider implementing a system so that network administrators are automatically informed when anomalous events occur. But remember, an automated system *will not* detect all anomalies! Regular log reviews will still be necessary.
- Suggestion: For suggestions on what to look for in logs from various sources, see the "Critical Log Review Checklist for Security Incidents" (http://www.sans.org/brochure/course/log-management-in-depth/6). Note especially the following:
  - *Windows OS, Object access denied:* If you have restricted access to your important directories and files, denied accesses to those are suspicious. Note that auditing must be turned on for each specific directory and file.
  - *Network Devices, Bytes transferred:* Large byte transfers to or from unexpected machines or at unexpected times are suspicious.
  - *Network Devices, Administrator access:* Administrator accesses from unexpected accounts (non-person service accounts, the Guest account, etc.) or at unexpected times are suspicious.

- *Web Servers, Error code 200 on files that are not yours:* Successful (status code 200) GETs or POSTs of files that you do not recognize are suspicious—especially if they are large (bytes transferred is a large number) and/or compressed (file extension is .zip, .rar, .tar.gz, .tgz, .sit, etc.). This may indicate that your data is being exfiltrated.
- *An additional suggestion (not on the checklist) for Database Servers:* High privilege actions (running stored procedures, creating or destroying links, etc.) that are unexpected are suspicious. Note that auditing must be turned on; most databases do *not* have auditing on by default.

- Suggestion: For additional recommendations on log management, including details on syslog, see NIST Special Publication 800-92: "Guide to Computer Security Log Management" (Available at http://csrc.nist.gov/publications/). For the Windows OS, also see NSA's "Spotting the Adversary with Windows Event Log Monitoring" (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml).

Configuration and Change Management

To better control your network and to keep it reliable and stable as it is upgraded and expanded, your organization may want to create a formal configuration and change management process. This process establishes review of changes before they are made, as well as backup of configurations so that any changes that break things can be quickly undone. (Note that the milestones of the Manageable Network Plan already established rudimentary configuration and change management; this Network Security Task is about *formalizing* the process.)

- Suggestion: For information on developing a formal configuration and change management process, see "The Definitive Guide to Enterprise Network Configuration and Change Management" (http://www.realtimepublishers.com/chapters/1264/dgenccm-1.pdf).
- Suggestion: Obtain tools that will enable you to detect changes to your network device configurations such as RANCID (Really Awesome New Cisco config Differ) (http://www.shrubbery.net/rancid/) or COSI (The Cisco-centric Open Source Community) (http://cosi-nms.sourceforge.net/). Ensure your network administrators become familiar with the tools and use them. Develop and document procedures for handling incidents where unauthorized changes have occurred. Unauthorized changes may indicate a security breach or a lack of network administrator training. Use encrypted channels when transferring network device configuration data to prevent the accidental spillage of passwords, network mapping information or other restricted data.
- Suggestion: For additional information, see the "Service Transition" volume of the IT Infrastructure Library (ITIL), and the Change and Configuration Service Management Function (SMF) of the Microsoft Operations Framework (MOF). The complete ITIL and MOF are both good general "best practice" lifecycle frameworks for delivering quality IT services.
  - IT Infrastructure Library (ITIL) (https://www.axelos.com/best-practice-solutions/itil/what-is-itil)
  - Microsoft Operations Framework (MOF) (http://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx)
- Suggestion: For recommendations on configuration management with a focus on information security and using the Security Content Automation Protocol (SCAP), see NIST Special Publication 800-128: "Guide for Security-Focused Configuration Management of Information Systems" (Available at http://csrc.nist.gov/publications/).
- **Risk management.** The level of tolerance for information security risk must be clearly defined and documented. Managing information security risk is important as your network grows and changes. Decision makers must recognize that explicit, well-informed risk-based decisions are necessary in order to balance the benefits of network changes with the risk that those changes will allow purposeful attacks, environmental disruptions, or human errors to cause mission and business failure. For guidance, see the following:
  - NIST Special Publication 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View" (Available at http://csrc.nist.gov/publications/)
  - NIST Special Publication 800-37: "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" (Available at http://csrc.nist.gov/publications/).
    Note: A brief summary of the Risk Management Framework process can be found in Appendix F of this document.
  - ISO 31000, *Risk management – Principles and guidelines* (Available at http://www.iso.org)

- Consider: For a process improvement approach to managing operational resilience (i.e., your ability to achieve your mission under adverse conditions), consider the CERT Resilience Management Model (http://www.cert.org/resilience/rmm.html).
- Consider: For another approach to getting a network under control, based on ITIL and change management, see *The Visible Ops Handbook* by Behr, Kim, and Spafford (IT Process Institute, 2005).

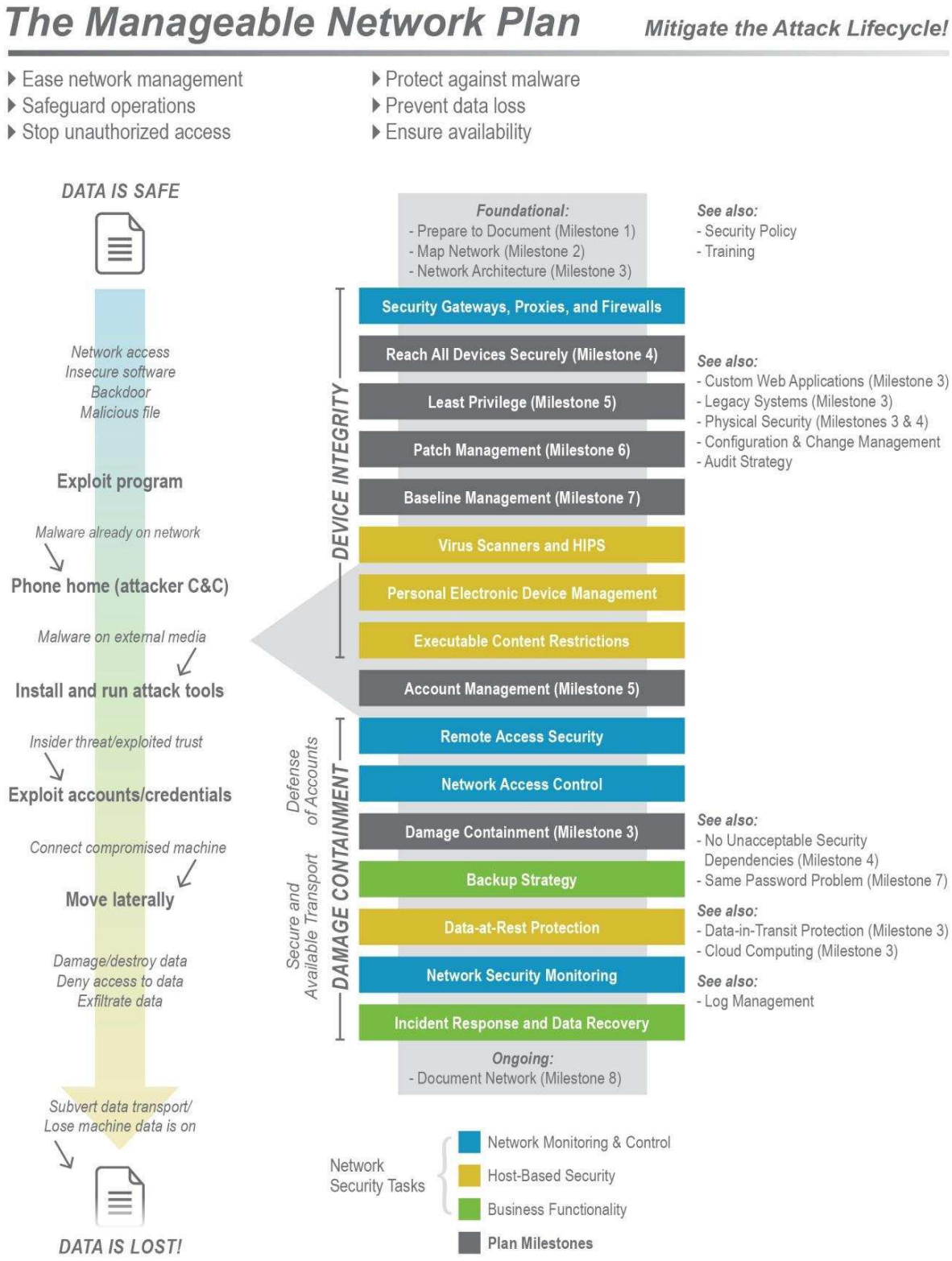
Audit Strategy

To verify that everything is working, that your network is in compliance with your security policy, that no unauthorized changes are being made, and that your administrative actions are having the desired effect on your devices and users, you need an audit strategy. You can also use an audit to make sure all the protocols and applications currently running on your network are approved, and gather metrics about your network. Your audit strategy should address *what* gets audited, *when* it gets audited, *what* you are looking for, and *what* you are going to do (based on risk considerations) if you find something non-compliant.

- Suggestion: Consider using a network vulnerability scanner and/or a Security Content Automation Protocol (SCAP) validated tool (http://nvd.nist.gov/scapproducts.cfm). Before using these tools on your ICS/SCADA network or devices, ensure that they will not cause problems with these devices.
- Suggestion: Consider at least gathering the following information:
  - How many total devices/hosts are on your network? How many of these devices cannot be contacted by the administrator? How many do not comply with your documented baselines? How many are running unapproved applications? How many are not fully patched? Are all the devices being tracked in your asset management system accounted for?
  - How many total user accounts exist on your network? How many of these are old, unused, or disabled (and perhaps unauthorized) accounts? How many have incorrect privileges? How many have weak passwords? If you are transitioning from passwords to more robust credentials, how many users have not yet been transitioned?
  - Do you have any unauthorized "rogue" wireless access points? Check by conducting a wireless network survey. Do you have any rogue wired access points, such as modems?
- Suggestion: Read *Security Metrics: Replacing Fear, Uncertainty, and Doubt* by Andrew Jaquith (Addison-Wesley, 2007).
- Suggestion: Consider using the Microsoft Security Assessment Tool (MSAT). The MSAT assesses your network based on your responses to questions, and provides recommendations based on accepted best practices and standards

  (http://www.microsoft.com/en-us/download/details.aspx?id=12273).
- Suggestion: For additional recommendations on information security measurement, see NIST Special Publication 800-55: "Performance Measurement Guide for Information Security" (Available at http://csrc.nist.gov/publications/).
- Suggestion: Have a yearly independent audit of your network done by a well-known provider.
- **Continuous monitoring.** Consider implementing a process to maintain ongoing awareness of your information security, to support your risk decisions. For more information and recommendations, see NIST Special Publication 800-137: "Information Security Continuous Monitoring for Federal Information Systems and Organizations" (Available at http://csrc.nist.gov/publications/).

Appendix A: Defend Your Network



Appendix B: Related Guidance

The following table specifies elements in other guidance that relate to the milestones and network security tasks in the Manageable Network Plan. The relations are not one-to-one, as different guidance has different purposes, approaches, and technical depth. Blanks do not necessarily imply an IA gap, but show where there is no specific relation, although the concepts may still be covered at a higher level.

Manageable Network Plan	NSA Community Gold Standard, v2.0[7]	CIS Critical Security Controls, v5.1[8]	NIST SP 800-53, Rev. 4, Controls[9]	NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0[10]
1: Prepare to Document				
- Ease of use				
- Purpose				
- Sufficient level of detail				
- Timestamps				
- Backing up				
- Protection				
- Hard copy				
2: Map Network	Network Mapping, Hardware Device Inventory	1	CM-8, PM-5	DE.AE-1, DE.CM-8
- Physical routes				ID.AM-3
- No unapproved devices and protocols		11-1		
- Asset management		1-4		ID.AM-1, PR.DS-3, PR.MA-1
- Network Map Distribution				
3: Network Architecture	Understand Mission Flows, Understand Data Flows, Network Boundary Protection	15	PM-11, RA-2, SA-14	ID.AM-5, ID.RA-1, ID.RA-3, PR.PT-3
- Damage containment	Network Boundary Protection, Independent Security Evaluations	7-10, 10-2, 11, 13, 15, 19, 20	AC-4, AC-20, CA-3, CA-8, CM-7, PL-8, PM-7, SC-2, SC-7, SC-32	DE.CM-3, ID.RA-6, PR.AC-5, PR.PT-3, PR.PT-4, RS.MI-1
- Data-in-transit protection	Communication Protection	15-1, 17-7	SC-8, SC-20, SC-23	PR.DS-2
- Cloud computing		8-3, 17-4	AC-20, CA-3	
- Virtualization security		2-7, 2-8, 5-6		
- Physical security	Physical Protection		MA-5, MP-2, PE-3, PE-5, PE-6	DE.CM-2, PR.MA-1
- No single points of failure			CP-8 (2), MA-6, PE-9 (1), SI-13	PR.IP-12, PR.PT-4
- Custom Web applications	Secure Lifecycle Management	2.1, 6	SA-8, SA-11, SI-10	

[7] For more information on the NSA Community Gold Standard, see https://www.iad.gov/iad/cgs/cgs.cfm.
[8] For more information on the CIS Critical Security Controls, see https://www.cisecurity.org.
[9] NIST Special Publication 800-53 is available at http://csrc.nist.gov/publications/.
[10] NIST Framework for Improving Critical Infrastructure Cybersecurity is available at http://www.nist.gov/cyberframework/.

Manageable Network Plan

Manageable Network Plan	NSA Community Gold Standard, v2.0[7]	CIS Critical Security Controls, v5.1[8]	NIST SP 800-53, Rev. 4, Controls[9]	NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0[10]
- Legacy systems			SA-8, SI-10, SI-15	PR.IP-12
- Risk assessment	Risk Management	4-10	RA-3	1.2, 2.2, 3.2, ID.RA-5
4: Device Accessibility		3	MA-2	PR.AC-2, PR.AC-3, PR.IP-12
- No clear-text administration protocols	Communication Protection	3-7, 10-5	MA-4 (6)	PR.PT-4
- No unacceptable security dependencies			MA-4 (3)	ID.BE-4
- Remote administration	Configuration Management	3-7, 10-5, 16-16	MA-4	PR.AC-3
- Physical security	Physical Protection		CM-5, PE-3	PR.AC-2
- Automating administration		3-2, 3-9, 3-10, 4-1, 4-5, 5-1, 5-2, 5-8, 8-1, 10-3, 11-3, 12-2, 13-5, 16-3	MA-2 (2)	
- Same administrative tools			MA-3	
- Outsourcing administration				DE.CM-6, ID.GV-2, PR.AT-3, PR.MA-1, PR.MA-2
5: User Access	Credential Management, Logical Access Management	12, 16	AC-2, AC-3, AC-6, CM-5	PR.IP-12, PR.PT-3
- No Internet or e-mail from privileged accounts		12-8	AC-6 (2)	
- Least privilege administrative model		3-3, 12-1, 12-8, 12-14	AC-6	PR.AC-4
- Users installing software		3-3	CM-11	
- No “entitlement”		3-3		
- Expiration dates on accounts	Credential Management	16.2	AC-2 (3)	
- Hiring consideration	IA Workforce Structure		PS-3	PR.IP-11
- Disable account when employee leaves	Credential Management	16	PS-4	DE.CM-3
6: Patch Management	Configuration Management	3-2, 4	SI-2, SI-5	ID.RA-1, PR.IP-12
- Non-Microsoft updates				
- BIOS and other firmware patches				
- No end-of-life software/hardware		3-2		
- Using virtualization		2-8		
- Update administrative tools				
7: Baseline Management	Software Inventory, Configuration Management, Acquisition Management	2, 3, 6, 10, 11-4, 12-5	CM-2, CM-6, CM-7, SA-12	DE.AE-1, DE.CM-5, DE.CM-7, ID.AM-2, PR.DS-7, PR.IP-1, PR.PT-3
- Backing up offline		8		
- Same password problem	Configuration Management		AC-4	

Manageable Network Plan

Manageable Network Plan	NSA Community Gold Standard, v2.0[7]	CIS Critical Security Controls, v5.1[8]	NIST SP 800-53, Rev. 4, Controls[9]	NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0[10]
- Verify device integrity	Configuration Management	3-10	SI-7	DE.CM-7, PR.DS-6
- Automatic reboots				
- Hardware configurations		3, 7-4, 7-5, 10		ID.AM-1
- Supply chain risk management	Acquisition Management		SA-12	ID.BE-1
8: Document Network	Risk Management		CP-2	PR.IP-9, RS.CO-2
- Completeness				
- Hard copy		18-1		
- Always followed				
Backup Strategy	Data Protection	8	CP-9, MP-4	PR.IP-4
Incident Response and Disaster Recovery Plans	Incident Handling, Risk Management	18	CP-2, CP-4, IR-3, IR-4, IR-8	PR.IP-10, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RS.CO-2, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.IM-1, RS.IM-2, RC.RP-1
Security Policy	IA Policy		PL-4, PS-6	DE.CM-3, ID.GV-1, ID.GV-3, RS.CO-1
Training	IA Awareness, IA Professional Development	9, 18-6	AR-5, AT-1, AT-2, AT-3, IR-2, PL-4, PM-13, PM-15	DE.DP-4, ID.AM-6, ID.RA-2, PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5
Executable Content Restrictions	Configuration Management	2, 3-8, 5-7	CM-7, CM-7 (5), SC-18, SC-44, SI-14, SI-16	PR.PT-3
Virus Scanners and Host Intrusion Prevention Systems (HIPS)	Intrusion Detection and Prevention	5	SC-18, SI-3	DE.CM-4, DE.DP-5
Personal Electronic Device (PED) Management	Data Protection, Network Access Control, Configuration Management, Acquisition Management	5, 17-8	AC-19, CA-9, CM-2, MP-7, SC-43	DE.CM-7, PR.PT-2
Data-at-Rest Protection	Data Protection	17	AC-7 (2), AC-19 (5), MP-6 (8), SC-4, SC-13, SC-28	DE.CM-7, PR.DS-1, PR.IP-7, PR.PT-2
- Data loss prevention	Data Protection	15-5, 17	AC-4, PM-12, SC-7 (10)	PR.DS-5, PR.PT-4
- Data spillage	Incident Handling		IR-9	PR.IP-6
Network Access Control	Network Access Control	1, 7-5	AC-19, CM-2 (7), IA-3	DE.CM-7
- User authentication	Logical Access Management	16-10	IA-2, IA-5, IA-8	PR.AC-1
Security Gateways, Proxies, and Firewalls	Network Boundary Protection	5, 6-2, 10, 11, 13	AC-4, CM-7, SC-5, SC-7, SI-3, SI-8, SI-10	PR.PT-3, PR.PT-4
- White-listing vs. black-listing		2-1		

Manageable Network Plan

Manageable Network Plan	NSA Community Gold Standard, v2.0[7]	CIS Critical Security Controls, v5.1[8]	NIST SP 800-53, Rev. 4, Controls[9]	NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0[10]
Out-of-band Management				
Remote Access Security	Communication Protection, Network Access Control	7, 13, 14-5	AC-17, AC-18, SC-7 (7)	DE.CM-7, PR.PT-1, PR.PT-4
Network Security Monitoring	Network Enterprise Monitoring, Intrusion Detection and Prevention	5, 13, 16-11, 16-13, 17-12	SI-4	DE.AE-2, DE.AE-5, DE.CM-1, DE.CM-3, DE.DP-3, DE.DP-4, ID.AM-3
Log Management	Network Enterprise Monitoring	14	AU-2, AU-3, AU-4, AU-6, AU-7, AU-8, AU-9	DE.AE-3, DE.DP-4, PR.PT-1
Configuration and Change Management	Configuration Management	3, 10	CM-3, CM-4, CM-9	ID.BE-5, PR.IP-2, PR.IP-3
- Risk management	Risk Management		PM-9	ID.GV-4, ID.RA-4, ID.RM-1, ID.RM-2
Audit Strategy	Vulnerability Assessment, Independent Security Evaluations, Network Enterprise Monitoring	All, especially 4	AU-1, AU-2, AU-3, CA-2, RA-5	DE.CM-7, DE.CM-8, PR.PT-1
- Continuous monitoring	Network Enterprise Monitoring	All, especially 14 and 16	CA-7	

Appendix C: The Manageable Network Plan Roadmap

The following specifies major elements related to the milestones.

Appendix D: Program of Record and Other Systems on Your Network but Not Under Your Control

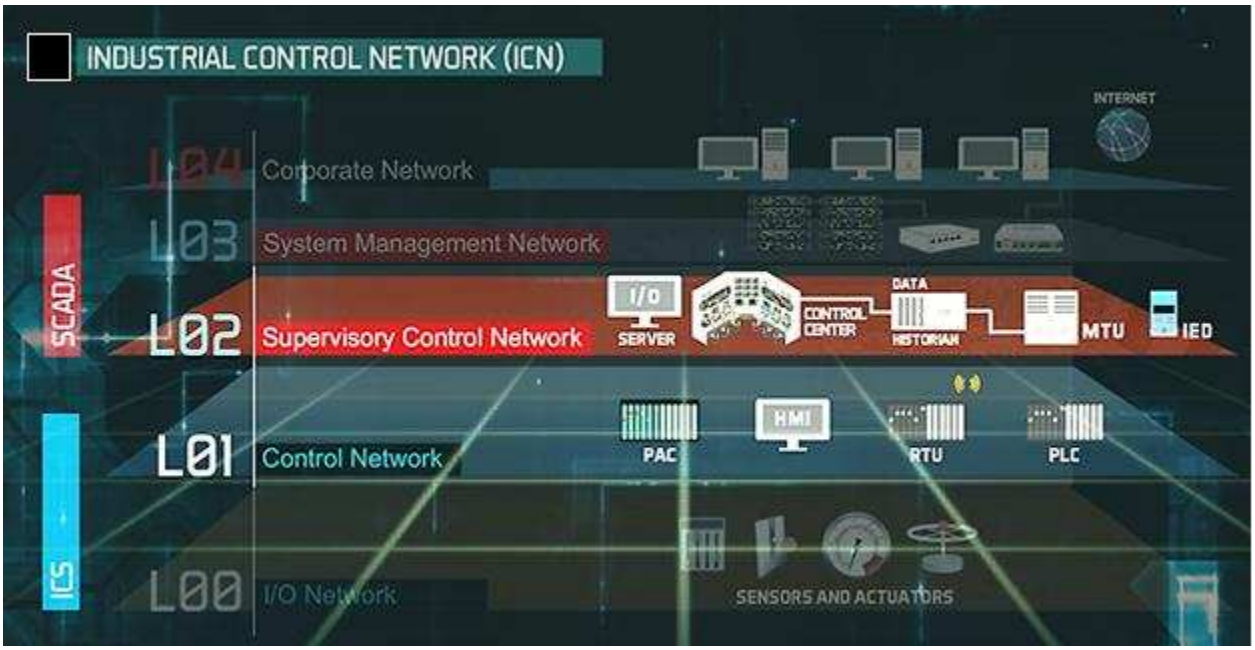
A program of record (PoR) is an acquisition effort that has been formally recorded as such in the programming and budgeting process, typically of a government or military organization. A system developed under a PoR usually cannot be updated without the prior approval of its managing office, sometimes referred to as a Program Management Office. The PoR's managing office, not your system administrators, will test any modifications (updates/patches) prior to their installation on an operational system to ensure that the system will not be degraded. This testing and approval process can take a considerable period of time during which the system will be vulnerable. In some instances, approval may never be given because of a complex interaction of different software!

Consequently, it is highly undesirable to have such a system connected to your network as your lack of control over it presents a substantial risk. However, there may be instances where you have no choice but to connect such a system to your network. When you do, segregate it behind a firewall to minimize the risk to the rest of your network. Also, be sure to keep up-to-date contact information for the PoR's managing office on file where you can access it quickly and easily should the need arise, such as to report a network failure that will prevent access to the PoR's system.

Appendix E: Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA)

Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems or networks historically have been physically isolated networks relying on modems or leased lines for remote access. However, many organizations have chosen to leverage their existing Information Technologies (IT) to interconnect their ICS/SCADA networks to their corporate network and even the Internet. The enhanced system flexibility and potentially reduced operational cost make this extended connectivity a highly attractive option for the ICS/SCADA network owner. However, the interconnected systems increase an adversary's attack vectors and put all networks at risk for unauthorized access. Some unique characteristics associated with ICS/SCADA networks that must be considered are described throughout the Manageable Network Plan.

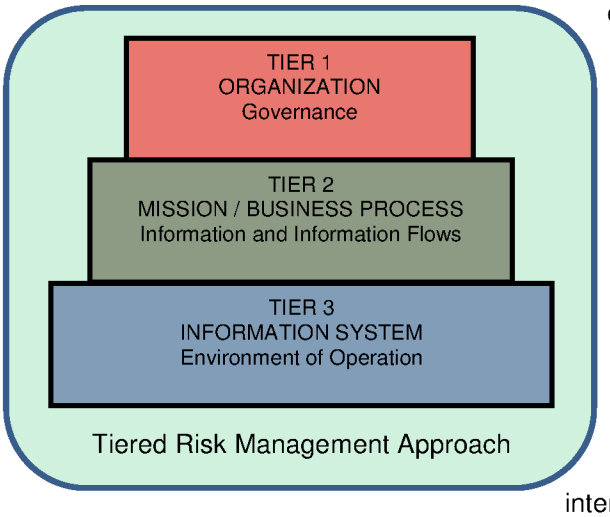
Many of the field level controllers and devices on ICS/SCADA networks operate on proprietary hardware, software and protocols. However, these devices depend on standard IT network connectivity to link them to their supporting clients and servers (human-machine interface (HMI), engineering workstations, historians, and other systems). These supporting clients and servers operate on commercial operating systems with known vulnerabilities. In many cases these supporting systems are so fragile and outdated that companies are reluctant to implement any changes including security patches. However, asset owners need to be apprised of the possible risks to their systems resulting from the failure to install security patches in a timely manner. Network owners will require all relevant information from both the corporate and ICS/SCADA administrators in order to make wise risk management decisions.



Appendix F: Risk Management Framework

As discussed in NIST Special Publication 800-37: "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" (Available at http://csrc.nist.gov/publications), the Risk Management Framework (RMF) is a common information security framework developed by the National Institute of Standards and Technology (NIST) in partnership with various U.S. Government agencies. Its purpose is to improve information security and strengthen risk management processes.

The RMF addresses organization-wide risk management on three levels. Tier 1 discusses risk from a top level organizational perspective. At Tier 1 you develop a comprehensive governance structure and organization–wide risk management strategy. Applying risk decisions made at Tier 1, you would proceed with Tier 2 activities to address the risks to your network from a mission and business process (enterprise architecture) point of view. At Tier 3 you address the risk from an information system perspective. Here you choose and deploy required safeguards and countermeasures (security controls) at the information system level. As you might expect, the risk activities and decisions at Tier 3 are affected by those from Tier 1 and Tier 2.

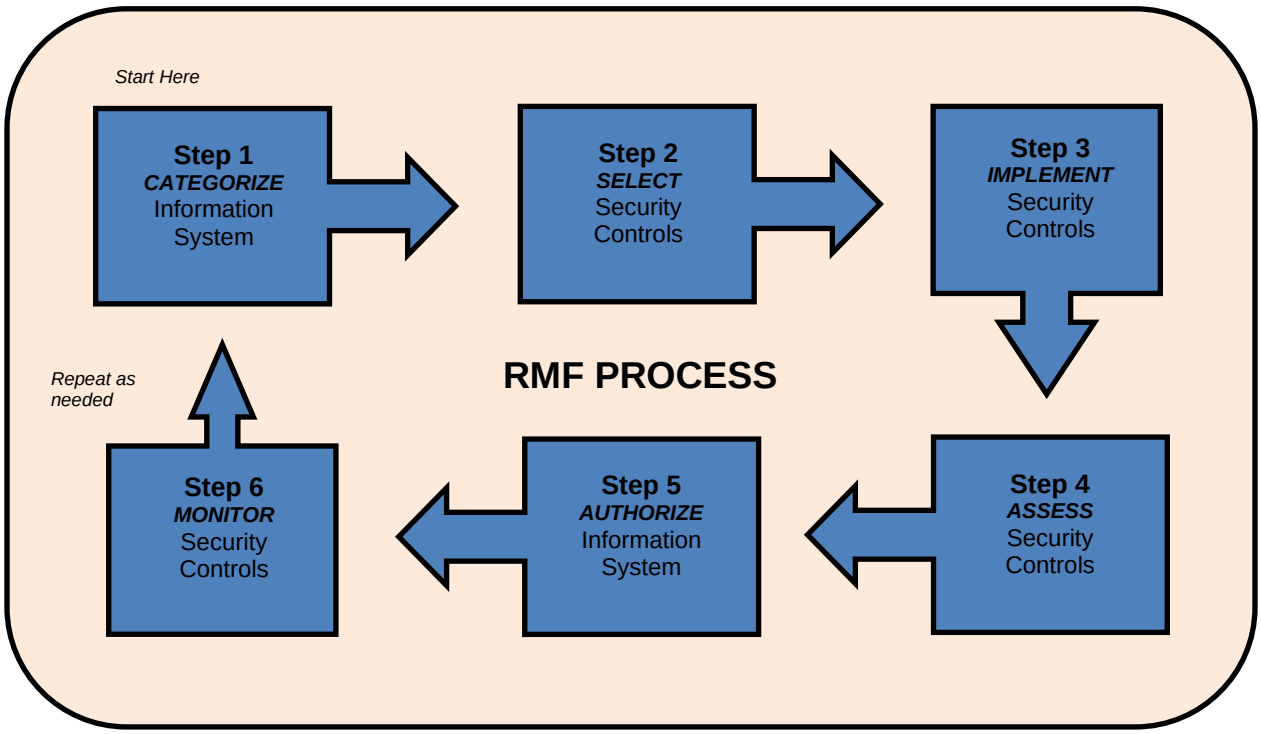


Tiered Risk Management Approach

Before you apply the RMF to your existing network or to the design of a new network, you should develop a risk management strategy for the network. A risk management strategy describes how an organization intends to assess risk, respond to risk and monitor risk. Information on developing a risk management strategy can be found in NIST Special Publication 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View" (Available at http://csrc.nist.gov/publications/). You should conduct risk management activities early in your network's development life cycle because the later in the development process these activities occur, the more costly they are to implement.

The RMF steps and associated tasks can be applied to a new network under development or to an existing network. There are six steps you need to perform when applying the RMF:

1. **Categorize.** First identify the types or categories of information stored, processed, and transmitted by your network. Types of information might include private personnel data (names, home addresses, social security numbers, and payroll data), proprietary project information, facility diagrams or maps, and emergency or continuity of operations information. Next, determine the potential adverse impact to your organization's operations, assets and people should each type of information be disclosed to unauthorized persons, damaged, lost or otherwise inaccessible. Additional information on assessing information types may be found in NIST Special Publication 800-60 Volume I: "Guide for Mapping Types of Information and Information Systems to Security Categories" and Federal Information Processing Standards Publication FIPS PUB 199: "Standards for Security Categorization of Federal Information and Information Systems" (Both available at http://csrc.nist.gov/publications/). If you are maintaining a system security plan (SSP), be sure to document the assessed impact levels in the plan. More information on SSPs may be found in NIST Special Publication 800-18: "Guide for Developing Security Plans for Federal Information Systems" (Also available at http://csrc.nist.gov/publications/).



2. **Select.** Select the necessary security controls based on the categorization you did in step 1. Tailor and supplement the security controls as needed based on an organizational assessment of risk and local conditions. Information on selecting security controls is available in NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" and Committee on National Security Systems (CNSS) instruction CNSSI 1253 Appendix D Table D-1. You can read CNSSI 1253 Appendix D Table D-2 for information on tailoring security controls for particular systems depending upon the risks associated with them. CNSSI 1253 "Security Categorization and Control Selection for National Security Systems" is available at https://www.cnss.gov/cnss/issuances/Instructions.cfm. NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" can be found at http://csrc.nist.gov/publications/.

3. **Implement.** After selecting and tailoring your security controls, you need to implement them and describe how the controls are employed within your network.

4. **Assess.** Now assess the security controls. Using appropriate assessment procedures you need to determine the extent to which the controls are implemented correctly and operating as intended. You also need to ensure that the results of the security controls are meeting the security requirements for your network. More information on how to assess security controls is detailed in NIST Special Publication 800-53A: "Assessing Security and Privacy Controls in Federal Information Systems and Organizations" and unique requirements for National Security Systems will be available in CNSS publication CNSSI 1253A: "Guide to Assessing Security Controls for National Security Systems" which is under development.

5. **Authorize.** Determine the risks to your organization's operations and assets as well as its individuals resulting from the operation of your network and the information systems on it. Also consider the risk to other organizations. If the authorizing official deems the risks acceptable, then the network can be authorized to operate.

6. **Monitor.** Monitor the security controls on your network on an ongoing basis. Assess the effectiveness of the controls and document changes to your network or its operating environment. Conduct security impact analyses of changes to your security controls and report the security state of your network to management or other designated individuals.

Quick Reference

Readings Mentioned

NIST publications are available at http://csrc.nist.gov/publications/
CNSS instructions are available at http://www.cnss.gov/cnss/issuances/Instructions.cfm
NSA Fact Sheets are available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml

Introduction

- NIST Special Publication 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View"
- "Strategies to Mitigate Targeted Cyber Intrusions" (http://www.asd.gov.au/infosec/mitigationstrategies.htm)
- NIST Special Publication 800-117: "Guide to Adopting and Using the Security Content Automation Protocol (SCAP)"

Network Architecture (Milestone 3)

- *Top-Down Network Design, Third Edition* by Priscilla Oppenheimer (Cisco Press, 2010)
- *Windows Server 2008 Security Resource Kit* by Jesper Johansson (Microsoft Press, 2008)
- "VLAN Provisioning for Logical Separation" (http://iase.disa.mil/stigs/Documents/vlan_provisioning_security_guidance_at-a-glance_v8r1.pdf)
- "Limiting Workstation-to-Workstation Communication" NSA Fact Sheet (https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_LimitingWtWCommunication_Web.pdf)
- NIST Special Publication 800-77: "Guide to IPsec VPNs"
- NIST Special Publication 800-81: "Secure Domain Name System (DNS) Deployment Guide"
- NIST Special Publication 800-146: "Cloud Computing Synopsis and Recommendations"
- "Security Guidance for Critical Areas of Focus in Cloud Computing" (https://cloudsecurityalliance.org/research/security-guidance)
- FedRAMP (http://www.fedramp.gov)
- NIST Special Publication 800-125: "Guide to Security for Full Virtualization Technologies"
- OWASP secure Web app development guide (https://www.owasp.org/index.php/Category:OWASP_Guide_Project)
- OWASP Web app testing guide (https://www.owasp.org/index.php/Category:OWASP_Testing_Project)
- OWASP Enterprise Security API (ESAPI) (https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API)
- OWASP AppSensor (https://www.owasp.org/index.php/Category:OWASP_AppSensor_Project)
- "DoD Legacy System Migration Guidelines" (http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=13311)
- NIST Special Publication 800-30: "Guide for Conducting Risk Assessments"
- ISO/IEC 31010, *Risk management – Risk assessment techniques* (Available at http://www.iso.org)

Device Accessibility (Milestone 4)

- *Group Policy: Fundamentals, Security, and Troubleshooting* by Jeremy Moskowitz (Wiley, 2008)

User Access (Milestone 5)

- NIST Special Publication 800-162: "Guide to Attribute Based Access Control (ABAC) Definition and Considerations"
- NSA Fact Sheet: "Enforcing No Internet or E-mail from Privileged Accounts"
- "Best Practices for Securing Active Directory" (http://www.microsoft.com/en-us/download/details.aspx?id=38785)

Patch Management (Milestone 6)

- NIST Special Publication 800-40: "Guide to Enterprise Patch Management Technologies"
- NIST National Cybersecurity Center of Excellence Publication: "Software Asset Management: Continuous Monitoring" (https://nccoe.nist.gov/sites/default/files/SAM.pdf)
- Using WSUS to patch third-party applications (http://windowsitpro.com/article/patch-management/Secure-non-Microsoft-applications-by-publishing-3rd-party-updates-to-WSUS-129241)

Baseline Management (Milestone 7)

- Securing Web browsers (https://www.us-cert.gov/publications/securing-your-web-browser)
- "Deploying and Securing Google Chrome in a Windows Enterprise" (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml)
- Center for Internet Security (http://cisecurity.org) [Windows, Linux, Solaris, Apple, Oracle, Cisco, etc.]
- NSA configuration guides (https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml)
- NIST National Checklist Program (http://web.nvd.nist.gov/view/ncp/information)
- DISA Security Technical Implementation Guides (STIGs) (http://iase.disa.mil/stigs/Pages/index.aspx)
- US Government Configuration Baseline (USGCB, formerly FDCC) (http://usgcb.nist.gov)
- "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" (http://www.microsoft.com/en-us/download/details.aspx?id=36036)
- "Reducing the Effectiveness of Pass-the-Hash" (Available at https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml)
- NIST Special Publication 800-161: "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"

Network Security Tasks

- NIST Special Publication 800-18: "Guide for Developing Security Plans for Federal Information Systems"

Manageable Network Plan

Incident Response and Disaster Recovery Plans (Business Functionality Network Security Task)

- *Incident Response & Computer Forensics, Third Edition* by Luttgens, Pepe, and Mandia (McGraw-Hill/Osborne, 2014)
- Remediation considerations (https://www.mandiant.com/blog/challenges-remediating-apt/, https://www.mandiant.com/blog/avoid-knee-jerk-reaction/, https://www.mandiant.com/blog/dod-cyber-crime-conference-presentation-recipes-remediation/, https://www.mandiant.com/blog/black-hat-usa-2012-presentation-targeted-intrusion-remediation-lessons-front-lines/, https://dl.mandiant.com/EE/library/BH2012_Aldridge_RemediationPaper.pdf)
- NIST Special Publication 800-61: "Computer Security Incident Handling Guide"
- NIST Special Publication 800-83: "Guide to Malware Incident Prevention and Handling for Desktops and Laptops"
- NIST Special Publication 800-34: "Contingency Planning Guide for Federal Information Systems"

Security Policy (Business Functionality Network Security Task)

- The SANS Security Policy Project (http://www.sans.org/security-resources/policies)

Training (Business Functionality Network Security Task)

- DISA Information Assurance training (http://iase.disa.mil/eta/online-catalog.html)
- NIST ITL Bulletin October 2003: "Information Technology Security Awareness, Training, Education, and Certification"
- NIST Special Publication 800-16: "Information Technology Security Training Requirements: A Role- and Performance-Based Model"
- NIST Special Publication 800-50: "Building an Information Technology Security Awareness and Training Program"

Executable Content Restrictions (Host-Based Network Security Task)

- "Application Whitelisting Using Software Restriction Policies" (https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml)
- Windows AppLocker (http://technet.microsoft.com/en-us/library/dd548340(WS.10).aspx)
- Application Whitelisting (https://www.nsa.gov/ia/_files/factsheets/Application_Whitelisting_Trifold_Jan_2013.pdf)

Personal Electronic Device (PED) Management (Host-Based Network Security Task)

- Enforcing restrictions with Group Policy (http://technet.microsoft.com/en-us/library/cc731387(WS.10).aspx)
- NSA Fact Sheet: "Defense against Malware on Removable Media"
- NSA Fact Sheet: "Mobile Device Management: A Risk Discussion for IT Decision Makers"
- NSA Fact Sheet: "Security Tips for Personally-Managed Apple iPhones and iPads"
- Managing iOS devices in an enterprise (http://www.apple.com/support/iphone/enterprise)
- Smartphone/tablet security guides (http://iase.disa.mil/stigs/net_perimeter/wireless/Pages/index.aspx) [iOS, Android, BlackBerry, etc.]
- NIST Special Publication 800-124: "Guidelines for Managing the Security of Mobile Devices in the Enterprise"

Data-at-Rest Protection (Host-Based Network Security Task)

- NIST Special Publication 800-131A: "Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths"
- NIST Special Publication 800-111: "Guide to Storage Encryption Technologies for End User Devices"
- CERT "Common Sense Guide to Mitigating Insider Threats" (http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm)
- NSA Fact Sheet: "Securing Data and Handling Spillage Events"

Network Access Control (NAC) (Network Monitoring and Control Network Security Task)

- NSA Fact Sheet: "Hardening Authentication"
- NIST Special Publication 800-63: "Electronic Authentication Guideline"

Security Gateways, Proxies, and Firewalls (Network Monitoring and Control Network Security Task)

- NIST Special Publication 800-41: "Guidelines on Firewalls and Firewall Policy"

Remote Access Security (Network Monitoring and Control Network Security Task)

- NIST Special Publication 800-48: "Guide to Securing Legacy IEEE 802.11 Wireless Networks"
- NIST Special Publication 800-97: "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i"
- NIST Special Publication 800-121: "Guide to Bluetooth Security"
- NIST Special Publication 800-153: "Guidelines for Securing Wireless Local Area Networks (WLANs)"
- NIST Special Publication 800-46: "Guide to Enterprise Telework and Remote Access Security"
- NIST Special Publication 800-114: "User's Guide to Securing External Devices for Telework and Remote Access"

Network Security Monitoring (Network Monitoring and Control Network Security Task)

- *The Practice of Network Security Monitoring* by Richard Bejtlich (No Starch Press, 2013)
- *The Tao of Network Security Monitoring Beyond Intrusion Detection* by Richard Bejtlich (Addison-Wesley, 2004)
- *Extrusion Detection* by Richard Bejtlich (Addison-Wesley, 2005)
- As first step to security (http://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html, http://taosecurity.blogspot.com/2009/03/requirements-for-defensible-network.html)
- NIST Special Publication 800-94: "Guide to Intrusion Detection and Prevention Systems (IDPS)"

Log Management (Network Monitoring and Control Network Security Task)

- "Spotting the Adversary with Windows Event Log Monitoring" (https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml)
- "Critical Log Review Checklist for Security Incidents" (http://www.sans.org/brochure/course/log-management-in-depth/6)
- NIST Special Publication 800-92: "Guide to Computer Security Log Management"

Configuration and Change Management (Network Monitoring and Control Network Security Task)

- "The Definitive Guide to Enterprise Network Configuration and Change Mgmt" (http://www.realtimepublishers.com/chapters/1264/dgenccm-1.pdf)
- IT Infrastructure Library (ITIL) (https://www.axelos.com/best-practice-solutions/itil/what-is-itil)
- Microsoft Operations Framework (MOF) (http://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx)
- NIST Special Publication 800-128: "Guide for Security-Focused Configuration Management of Information Systems"
- NIST Special Publication 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View"
- NIST Special Publication 800-37: "Guide for Applying the Risk Mgmt Framework to Federal Info. Systems: A Security Life Cycle Approach"
- ISO 31000, *Risk management – Principles and guidelines* (http://www.iso.org)
- CERT Resilience Management Model (http://www.cert.org/resilience/rmm.html)
- *The Visible Ops Handbook* by Behr, Kim, and Spafford (IT Process Institute, 2005)
- NSA's "Spotting the Adversary with Windows Event Log Monitoring" (https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/applications.shtml)

Audit Strategy (Network Monitoring and Control Network Security Task)

- *Security Metrics: Replacing Fear, Uncertainty, and Doubt* by Andrew Jaquith (Addison-Wesley, 2007)
- NIST Special Publication 800-55: "Performance Measurement Guide for Information Security"
- NIST Special Publication 800-137: "Information Security Continuous Monitoring for Federal Information Systems and Organizations"

Appendix B

- CIS Critical Security Controls (https://www.cisecurity.org)
- NIST Framework for Improving Critical Infrastructure Cybersecurity (http://www.nist.gov/cyberframework)

Appendix F

- NIST Special Publication 800-37: "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
- NIST Special Publication 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View"
- NIST Special Publication 800-60 Volume I: "Guide for Mapping Types of Information and Information Systems to Security Categories"
- NIST FIPS PUB 199: "Standards for Security Categorization of Federal Information and Information Systems"
- NIST Special Publication 800-18: "Guide for Developing Security Plans for Federal Information Systems"
- NIST Special Publication 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST Special Publication 800-53A: "Assessing Security and Privacy Controls in Federal Information Systems and Organizations"
- CNSSI 1253 "Security Categorization and Control Selection for National Security Systems" (https://www.cnss.gov/cnss/issuances/Instructions.cfm)
- CNSSI 1253A: "Guide to Assessing Security Controls for National Security Systems" (Due for publication in 2016)

Tools Mentioned

Note that these tools have not been evaluated by the NSA and might not be approved for use in your organization.

Map Your Network (Milestone 2)

- Nmap (http://nmap.org)
- arpwatch (http://ee.lbl.gov)
- NetReg (http://netreg.sourceforge.net
- Wireshark (https://www.wireshark.org)
- tcpdump (http://www.tcpdump.org)
- WinDump (http://www.winpcap.org/windump)

Device Accessibility (Milestone 4)

- Puppet (https://puppetlabs.com)
- PuTTY (http://www.chiark.greenend.org.uk/~sgtatham/putty)
- WinSCP (http://winscp.net)
- FileZilla (https://filezilla-project.org)

Patch Management (Milestone 6)

- Windows Server Update Services (WSUS) (http://technet.microsoft.com/en-us/wsus/default)
- Puppet (https://puppetlabs.com)
- Spacewalk (http://spacewalk.redhat.com)

Baseline Management (Milestone 7)

- Microsoft Baseline Security Analyzer (MBSA) (http://technet.microsoft.com/en-us/security/cc184924.aspx)

Executable Content Restrictions (Host-Based Network Security Task)

- Enhanced Mitigation Experience Toolkit (EMET) (http://support.microsoft.com/kb/2458544)

Personal Electronic Device (PED) Management (Host-Based Network Security Task)

- Free mobile device integrity tool (Sentinel AutoBerry) for U.S. Government organizations (https://www.iad.gov, under Mitigations - Tools)

Network Security Monitoring (Network Monitoring and Control Network Security Task)

- Snort (https://www.snort.org)
- Security Onion (http://sourceforge.net/projects/security-onion)

Log Management (Network Monitoring and Control Network Security Task)

- Splunk (http://www.splunk.com)
- Snare (http://sourceforge.net/projects/snare)

Configuration and Change Management (Network Monitoring and Control Network Security Task)

- RANCID (Really Awesome New Cisco config Differ) (http://www.shrubbery.net/rancid)
- COSI (The Cisco-centric Open Source Community) (http://cosi-nms.sourceforge.net)

Audit Strategy (Network Monitoring and Control Network Security Task)

- SCAP validated tools (http://nvd.nist.gov/scapproducts.cfm)
- Microsoft Security Assessment Tool (MSAT) (http://www.microsoft.com/en-us/download/details.aspx?id=12273)

Index

Comments or feedback? manageable@nsa.gov

Disclaimer of Endorsement:

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact Information

Industry Inquiries
410-854-6091
bao@nsa.gov

Client Requirements and General Information Assurance Inquiries

IAD Client Contact Center
410-854-4200
IAD_CCC@nsa.gov