Hardening of Devices

1. Purpose
   In an effort to further increase the overall security posture of the State of Montana, several agencies agreed to collaborate on a strategic goal of increasing security on end-user workstations. The team met on a monthly basis between the March and August of 2015. The MT-ISAC Best Practices and Tools workgroups reviewed and updated this document.

2. Research and Discussion
   Originally intended to assess the posture of antivirus, it became clear that budgetary constraints as a result of legislative decisions would prohibit any change or additional acquisition of an antimalware solution. The group decided to focus on studying security practices that could be developed collaboratively, implemented with minimal monetary cost but would require internal agency technology efforts, with the goal of increasing workstation and server security.

3. Policy
   Hardening of Devices applies to the following controls found within the Information Security Policy.
   a. Information Security Policy
      - Identify
        - 1.7, 1.7.6, 1.7.10, 1.7.12
      - Protect
        - 2.1.9, 2.6, 2.7, 2.7.1, 2.7.2, 2.9.2, 2.9.5.3, 2.9.5.8, 2.9.6, 2.10, 2.10.2,2.10.9, 2.11.6, 2.14.6, 2.15.6, 2.18.8, 2.19, 2.19.3, 2.19.4, 2.19.5
      - Detect
        - 3.1
   b. Information Security Policy – Appendix A
      - Access Control (AC)
        - AC-2 – Account Management
        - AC-3 – Access Enforcement
        - AC-6 – Least Privilege
        - AC-18 – Wireless Access
      - Configuration Management (CM)
        - CM-2 – Baseline Configuration
        - CM-5 – Access Restrictions for Change
        - CM-7 – Least Functionality
        - CM-11 – User Installed Software
      - Identification and Authentication (IA)
        - IA-2 – Identification and Authentication

- IA-5 – Authenticator Management
- IA-7 – Cryptographic Module Authentication

- Media Protection (MP)
  - MP-4 – Media Storage
  - MP-5 – Media Transport
- System and Services Acquisition
  - SA-5 – Information System Documentation
- System and Information Integrity (SI)
  - SI-2 – Flaw Remediation (Patch Management)
  - SI-3 – Malicious Code Protection
  - SI-4 – Information System Monitoring
  - SI-7 – Software, Firmware, and Information Integrity
  - SI-16 – Memory Protection

4. Best-Practices to be Adopted as Standard Configuration

   a. Image Configuration (Enterprise Information Security Policy – 1.7, 2.6, 2.9.5.3, 2.10, 2.11.6, 2.19, 3.1; Enterprise Information Security Policy - Appendix A - CM-2, CM-5, CM-7, SI-2, SA-5) – **All servers and workstations shall be imaged with the most recent "reference image"**, which will be configured by each agency. Security practices dictate that new workstations and servers be imaged or configured from a fresh installation of the system's operating system. Traditionally, workstations and servers are configured by the manufacturer focusing on ease-of-use, and not security. By rebuilding or reimaging all workstations and servers, this will provide for the distribution of a common system image for an agency to build upon. Due to the frequency that security updates are distributed from various software manufacturers, it is recommended that the "reference image" for workstations and servers be updated and documented on a monthly basis. The previous two images should be retained for roll-back purposes. System hardening shall include the removing of any unnecessary system accounts, processes, services, or applications, and closing network ports. This "reference image" shall be validated against security benchmarks from trusted sources. Vulnerability Scans must be completed on "reference image" and the vulnerabilities reviewed for impact and risks mitigated before deployment.

   b. Patch Management (Enterprise Information Security Policy - 1.7.6, 1.7.10, 1.7.12, 2.11.6, 2.14.6; Enterprise Information Security Policy - Appendix A - SI-2)– It is imperative that all agencies develop, institute and document an effective patch management process for both workstations and servers in order to remediate vulnerabilities and threats. Policy dictates that no unpatched system, unsupported

operating system, or application is allowed connectivity to SummitNet without an exception. Agencies shall develop a process in order to ensure compliance with state policy. As a guideline, all patches shall be deployed to their respective technology after appropriate testing.

c. Principle of Least Privilege (Enterprise Information Security Policy - 2.6, 2.9.5.3, 2.10.9, 2.19; Enterprise Information Security Policy – Appendix A - AC-2, AC-6, CM-7) – **Agencies shall employ the use of the principle of least privilege for all user and service accounts. Basic user and service accounts will be assigned the most restrictive type of account that only allows them to perform necessary job functions.** Privileged users shall have an additional separate account for performing privileged commands. Elevated level access given to employees shall be documented and approved by the Agency Security Officer. Privileged users' access shall be reviewed regularly and removed when no longer necessary. Though it is often convenient for support staff to allow for end-users to have elevated privileges, the security risks this introduces are increased exponentially. Many flavors of malware typically include elevation of privileges in order to fully take advantage of an exploit and spread to critical information systems.

d. Multifactor Authentication (Enterprise Information Security Policy - 2.1.2, 2.5.2; Enterprise Information Security Policy – Appendix A – IA-2) – **All state workstations and servers shall have the RSA client installed to force multi-factor authentication. All state users including contactors who log into state systems shall use the approved RSA multifactor authentication enterprise provided tokens.**

e. Deploying of EMET on Microsoft Windows Workstations (Enterprise Information Security Policy – 2.7.1, 2.7.2, 2.9.6, 2.15.6; Enterprise Information Security Policy – Appendix A - SI-3, SI-4, SI-7, SI-16) – **Workstations shall be configured with EMET** – The Microsoft Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited by using security mitigation technologies. These technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities. These security mitigation technologies do not guarantee that vulnerabilities cannot be exploited. However, they work to make exploitation as difficult as possible to perform. EMET will require some investment in time from agency staff administrating it and testing it before its introduction into an agency's environment, as unique applications used may cause conflicts that could inhibit

business processes instead of securing them. Some software applications are not compatible with EMET.

f. Application restriction software (Enterprise Information Security Policy – 2.6, 2.19.3, 2.19.4, 2.19.5 ; Enterprise Information Security Policy – Appendix A - AC-2, AC-3, AC-6, CM-7, CM-11, PL-4, SI-2) – **Workstations shall be configured with application restriction software. Until an enterprise solution is determined, tools listed on the approved software list must be used.** It is a recommended best practice to install application restriction software on servers once the server is fully configured for production and appropriate testing has been done. (Note: Testing should be done before pushing application restriction software to agency developer(s) workstations) Application control and whitelisting features allows you to specify which users or groups can run particular applications based on unique identities of files. Agencies can create rules to allow or deny applications from running. Application restriction software provides administrators with the ability to specify which users can run specific applications. This also allows administrators to control the following types of applications: executable files (.exe and .com), scripts (.js, .ps1, .vbs, .cmd, and .bat), Windows Installer files (.msi and .msp), and DLL files (.dll and .ocx). Before any application is restricted, it should be thoroughly tested within the agency business environment to identify any problems and mitigate them if possible.

   Commonly malware runs out of the following folders:
   - **%OSDRIVE%\Windows\System32**
   - **%OSDRIVE%\ProgramData**
   - **%OSDRIVE%\Program Files**
   - **%OSDRIVE%\Users\<*user*>\AppData\Local\Microsoft\Windows\Temporary Internet Files**
   - **%OSDRIVE%\Users\<*user*>\AppData\Local\Temp**
   - **%OSDRIVE%\Users\<*user*>\Downloads**
   - **%OSDRIVE%\Users\<*user*>\Documents**

   Ransomware most commonly running out of the following folders (in order of frequency):
   - **%AppData% – User > AppData > Roaming**
   - **%Temp% – AppData > Local > Temp**
   - **%UserProfile% – Current User Profile**
   - **%AllUsersProfile% – Computer > C: > ProgramData**

Applications could be installed into a user profile without that user having administrative rights on the system. This is how advanced malware bypasses a system locked down without administrative rights. The ability to whitelist applications is another feature that shall be utilized. A combination of preventing executables from running out of common malware folders along with the whitelisting of applications with trusted digital signatures (use a certificate rather than hash value where possible) would be a significant improvement in hardening an OS to prevent an infection.

g. Phased Elimination of Mapped Drives (Enterprise Information Security Policy – 2.7; Enterprise Information Security Policy – Appendix A - SI-3) – **This is a recommendation** for agencies to consider if their business processes will allow for it. Malware, specifically ransomware if loaded onto a workstation, may target not only the device's local drive, but also mapped network or attached drives as well. Ransomware looks for any other drives on the system, including mapped drives, and begins encrypting those files on the mapped drive as well. In an enterprise this could be catastrophic. By using shortcuts that point to a drive path you eliminate the ability for ransomware to find that drive and encrypt its contents. Simply putting the shortcuts into a folder and adding that folder into your favorites group on Windows Explorer makes the transition from using mapped drives to UNC shortcuts much easier for the end user.

h. Device drive encryption (Enterprise Information Security Policy – 2.1.9, 2.18.8, 2.9.2, 2.9.5.8; Enterprise Information Security Policy – Appendix A - IA-7, MP-4, MP-5) – **All workstations, laptops and media storage devices must have encryption enabled- Bitlocker.** BitLocker is a full disk encryption feature included with select editions of Windows. It is designed to protect data (in the event of physical loss of the device) by providing encryption for entire volumes. BitLocker is available in Ultimate and Enterprise versions of Vista and 7, as well as Pro and Enterprise versions of Windows 8 and 10.
BitLocker Drive Encryption can be configured to back up recovery information for BitLocker-protected drives and the Trusted Platform Module (TPM) to Active Directory Domain Services (AD DS). Backing up recovery passwords for a BitLocker-protected drive allows administrators to recover the drive if it is locked. This ensures that encrypted data belonging to the enterprise can always be accessed by authorized users.
Alternatively, BitLocker recovery information can be managed manually and stored securely using any of several widely available tools.

i. SmartScreen Filter (Enterprise Information Security Policy - 2.7.1, 2.7.2, 2.9.6, 2.15.6; Enterprise Information Security Policy - Appendix A - SI-3, SI-4, SI-7, SI-16) - **SmartScreen Filter shall be set to "On".** SmartScreen Filter is a feature in Internet Explorer that helps detect phishing websites. SmartScreen Filter can also help protect you from downloading or installing malware (malicious software). SmartScreen Filter helps to protect you in three ways:
   1) As you browse the web, it analyses webpages and determines if they have any characteristics that might be suspicious. If it finds suspicious webpages, SmartScreen will display a message giving you an opportunity to provide feedback and advising you to proceed with caution.
   2) SmartScreen Filter checks the sites you visit against a dynamic list of reported phishing sites and malicious software sites. If it finds a match, SmartScreen Filter will show you a warning notifying you that the site has been blocked for your safety.
   3) SmartScreen Filter checks files that you download from the web against a list of reported malicious software sites and programs known to be unsafe. If it finds a match, SmartScreen Filter will warn you that the download has been blocked for your safety. SmartScreen Filter also checks the files that you download against a list of files that are well known and downloaded by many Internet Explorer users. If the file that you're downloading isn't on that list, SmartScreen Filter will warn you.

j. Windows Firewall (Enterprise Information Security Policy – 2.7.1, 2.7.2; Enterprise Information Security Policy – Appendix A - SI-3) - **Windows Firewall shall be enabled.** State Agencies shall have a documented port exception process. A firewall is software or hardware that helps prevent hackers and some types of malware from getting to your PC through a network or the Internet. It does this by checking the info that's coming from the Internet or a network and then either blocking it or allowing it to pass through to your PC. A firewall isn't the same thing as an antivirus or antimalware app. Firewalls help protect against worms and hackers, antivirus apps help protect against viruses, and antimalware apps help protect against malware. You need all three. You only need one firewall app on your PC. Having more than one firewall app on your PC can cause conflicts and problems. Agencies shall use these firewall settings;

   •The firewall is on for all network connections.
   • The firewall is set to block all inbound connections except those explicitly allowed.
   •The firewall is on for all network types (Private, Public, or Domain).

k. Antivirus Software (Enterprise Information Security Policy – 3.2.3.3; Enterprise Information Security Policy – Appendix A – SI-3, SI-4) – **Antivirus Software must be installed, up to date and running on all connected devices.** Antivirus, sometimes known as anti-malware is software that used to prevent, detect and remove malicious software on devices. The Information Security Policy states virus scanning software must be installed, updated and used on servers, workstations and other devices used to connect to the state's network.

l. AES encrypted wireless input devices. (Enterprise Information Security Policy – 2.20.2.3; Enterprise Information Security Policy – Appendix A – AC-18, IA-5, IA-7) All future wireless input devices shall be AES encrypted. Wireless keyboards transmit information over the air, which creates an often overlooked point of vulnerability. Without proper security measures in place, a cyber-thief could intercept your keystrokes and gain access to your passwords, credit card numbers, and other vital information.

5. Compliance

   Compliance shall be evidenced by implementing Hardening of Devices as described above. Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this Hardening of Devices are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

6. Conclusion

   Hardening of Devices document is the result of a multi-agency collaboration as well as has the MT-ISAC Best Practices approval. The representatives from these groups worked well together to endorse the recommendations contained here-in. A methodical, well-planned approach to effectively testing and measuring these controls will introduce additional layers to the security of the State of Montana's end-users.

Appendix A

Approved Tools

a. Image Configuration
    i. Security Benchmarks –
        1. CIS Secure Configuration Benchmarks
        2. IRS Safeguards Program (uses CIS Benchmarks and supplements with IRS requirements)
b. Patch Management
c. Principle of Least Privilege
d. Multifactor Authentication
    i. RSA
e. Deploying of EMET on Microsoft Windows Workstations
f. Application restriction software
g. Elimination of Mapped Drives
h. Device drive encryption
    i. BitLocker
i. SmartScreen Filter
j. Windows Firewall
k. Antivirus Software
    i. Microsoft Endpoint Protection
l. AES encrypted wireless input devices.

Appendix B

Future Proposed Improvements

1. Consider the consistent use of the terms workstation, server, and device.
2. Section 4A - may wish to add language about the image being certified for use by an authorizing authority.
3. Section 4B - we may need to revisit “applications” as part of this section. The intention is to require patching of applications such as Java and Flash which are used by the majority of devices. One option may be to create a list of applications to which this applies. This should be discussed by the MT-ISAC as a whole.
4. Section 4C – add language to disable guest accounts and change password for local admins.
5. Section 4D - need for discussion about how this applies to workstations/applications/county/public users/Kiosk.
6. Section 4H - revise to reflect enterprise verbiage rather than a specific product. remote devices need to be considered. Anne Kane looked into and currently Microsoft does not have a remote devices solution.