

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices / Tools Workgroup – Vulnerability Management Procedure

Vulnerability Management Standard



STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices / Tools Workgroup – Vulnerability Management Procedure

1. Purpose

This procedure identifies the process for vulnerability management to protect information systems against known vulnerabilities.

2. Scope

This procedure applies to enterprise systems. The Information Security Policy requires all systems to routinely be updated and patched.

3. Policy

Vulnerability Management Procedure applies to the following controls found within the Information Security Policy.

a. Information Security Policy

- Identify
 - 1.7, 1.8
- Protect
 - 2.9.7, 2.10, 2.11.6, 2.17
- Detect
 - 3.1

b. Information Security Policy – Appendix A

- Audit and Accountability (AU)
 - AU-6 – Audit Review, Analysis, and Reporting
- Configuration Management (CM)
 - CM-3 – Configuration Change Control
 - CM-6 – Configuration Settings
 - CM-9 – Configuration Management Plan
- Risk Assessment (RA)
 - RA-5 - Vulnerability Scanning
- System and Information Integrity (SI)
 - SI-2 – Flaw Remediation (Patch Management)
 - SI-5 – Security Alerts, Advisories, and Directives
 - SI-7 – Software, Firmware, and Information Integrity

4. Recommended Best-Practices to be Adopted as Standard Configuration

Security vulnerabilities are identified on a daily occurrence. State agencies shall proactively manage vulnerabilities of systems to reduce or eliminate the potential for exploitation.

A. Monitoring Vulnerabilities

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices / Tools Workgroup – Vulnerability Management Procedure

State agencies are responsible for reviewing and monitoring new patch releases through announcements and notifications from SITSD's Security Information Alerts. Agencies should also consider monitoring the following:

- notifications from vendors, and
- Security web sites

B. Vulnerability Communication

For enterprise wide vulnerability communications SITSD's Information Security Bureau (ISB) will determine the need for communication of vulnerabilities to agencies. This communication will be sent through the SITSD Service Desk. The agency will then communicate vulnerabilities to individuals as necessary. This will be dependent upon the vulnerability and the systems to which they pertain.

Vulnerability communication is conducted in more than one method:

- Email
- Network Managers Meeting (NMG)
- MT-ISAC and ITMC meetings
- Agency Technical and or Supervisor meetings
- Meetings with the business

C. Vulnerability Scanning

To reduce the State of Montana's cyber-security attack surface, both external and internal, there is a need for a formalized, enterprise-wide vulnerability scanning to;

- Identify vulnerabilities in information systems that may be leveraged by a malicious actor, or exploited by a malicious process
- Identify missing system updates and security patches on information systems for state-agencies.
- Provide a means for key state-agencies to attest to following federally mandated compliance requirements

The scope is intended to address all information systems within the State of Montana's internal 10.x IP space, and the State DMZ, occupying the assigned 161.x IP space that operates on a supported Microsoft Windows operating system, or Linux operating system, where applicable.

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices / Tools Workgroup – Vulnerability Management Procedure

To limit the potential adverse impact vulnerability scanning may have upon network and information system performance:

- The State Information Technology Services Division (SITSD) will provide vulnerability scanning solutions as well as scanning services for agencies as requested through cases opened through the Service Desk.
- If an agency requests to perform their own scans of their environment the following criteria must be satisfied before a dedicated scanner is provided.
 - All agency employees who will perform scanning on their behalf must complete the necessary SITSD approved training courses provided by the vulnerability scanning vendor. A Certificate of Completion of the course will satisfy this requirement.
 - A written agreement by the agency to SITSD that they will submit an Enterprise Change Notification each time they perform scans on production systems only, including follow up remediation or patch verification scans. Development/Testing systems are not included in the change management policy and can be scanned at any time without submission of a change request. In the event of scans setup on an automated schedule, a single Change Notification detailing the scan information will need to be submitted by the agency. Any changes made to the scans after initial setup would require a new Change Notification. If an agency analyst fails to follow this requirement, repeatedly, SITSD has the right to revoke their scanning privileges.
 - The scanner must be setup and managed by SITSD staff. Rights providing access to scan assets will be given to agency staff once identified by the agency security contact.
 - An agency email resource inbox will be created and owned by SITSD. Read-only rights will be assigned to an Active Directory group provided by the agency in order for them to control who has viewing privileges within their organization. All scheduled scan SMTP notifications will be sent to the respective agency inbox.
- Only SITSD will update and maintain the enterprise vulnerability scanning tool on behalf of all state-agencies.

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices / Tools Workgroup – Vulnerability Management Procedure

- Information systems externally accessible will be scanned using a trusted third-party monthly.
- State-agencies may use a third-party (including the Department of Homeland Security) to conduct external vulnerability scanning on information systems that are externally accessible. The agency using third-party services will provide communication to the SITSD Service Desk at least 48 hours in advance. Information required in the communication to the Service Desk will include source IP(s), target IP(s), and the time the scanning or penetration testing is to occur.
- Monthly, the Multi-State Information Sharing & Analysis Center (MS-ISAC) conducts an operating system finger-print scan (non-credentialed) on all external-facing information systems in the State's DMZ; system-owners are notified via SITSD of any findings that need to be resolved.
- If a highly critical and exploitable vulnerability is announced from trusted sources and threatens assets on the network, SITSD will have the right to perform out-of-band or unscheduled vulnerability scans to determine the scope of our vulnerable systems. SITSD will provide notification of out-of-band or unscheduled vulnerability scanning to all appropriate entities as documented in the SITSD Change Management Procedure.
 - NOTE: depending upon the criticality of the vulnerability scan, emergency change notifications may be used in order discover currently exploited-in-the-wild vulnerabilities in a timely manner.
- SITSD has the right to perform host discovery scans to identify active IP's that exist on the state network. All Host-Based Discovery Scanning conducted by SITSD will follow the SITSD Change Management Procedure with notifications sent out via the SITSD Service Desk accordingly.
- Host discovery scans will be done monthly by SITSD to identify active IP's that exist on the state network

D. Vulnerability Remediation

Remediation for vulnerabilities will be deployed to all systems that have the vulnerability, even for systems that are not at immediate risk of exploitation. Remediation for vulnerabilities will also be incorporated into the standard builds and configurations for hosts. There are three primary methods of remediation

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices / Tools Workgroup – Vulnerability Management Procedure

that can be applied to an affected system: the installation of a software patch, the adjustment of a configuration setting, or the removal of the affected software.

1. Patch Management will be conducted as follows:

- Agency shall assign staff or contracted services that will:
- Manage and maintain system updates for agency systems.
- Deploy patches for appropriate systems using enterprise approved methods or tools
- Review security patches, determine their applicability to agency systems, and communicate necessary patches to appropriate staff.
- Initialize testing of security patches
- Distribute patches to vulnerable systems

All agencies shall use the following chart when determining alert level when distributing information about the patch:

- **RED** – Immediately within 48 hours or two working days
- **Orange** – As Soon as Possible (next General Maintenance Window)
- **Yellow** – Within one Month

2. Configuration Setting

Agency will monitor information from various sources to determine the need for system configuration setting changes. System configuration changes are generally a result of vulnerability scans or vendor communications.

The process that agencies will follow as it relates to configuration setting changes:

- The agency security officer receives information regarding a configuration setting from a vulnerability scan or a communication from the vendor.
- The agency security officer will discuss the configuration change with system owner experts.
- A determination will be made as to whether the configuration will be changed. If it is not to be changed, this should be noted and the reason for not making the change in the agency change

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices / Tools Workgroup – Vulnerability Management Procedure

management or risk assessment application. If the change is going to be made, agencies will follow their Change Management Process.

3. Removal of affected software

Agency will monitor information from various sources to determine the need for software removal. An example of this would be the use of non-standard software on an agency computer. This is the process that the agency will follow as it relates to software removal:

- The agency security officer receives information regarding software that may need to be removed from systems.
- The agency security officer will discuss the software removal with various system owner experts
- A determination will be made as to whether the software will be removed. If it is determined that the software will not be removed, this should be noted and the reason for not removing the software in the agency change management or risk assessment application. If the software is to be removed, a service request is to be made and assigned to the appropriate group for the software to be removed
- Software shall be removed when it is end of life and no longer supported.

E. Verification of Remediation

The agency will verify vulnerability remediation using several methods:

- Patch Management
 - Verify patch installation by auditing patch logs or automated software reports
- Configuration Management
 - Verify that files or configuration changes remediated the vulnerability.
 - Review change management reports for removal of affected software from devices.
 - Credentialed scan of host with vulnerability scanner that is capable of detecting known vulnerabilities
 - Perform annual vulnerability scanning.

5. Compliance

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices / Tools Workgroup – Vulnerability Management Procedure

Compliance shall be evidenced by implementing Vulnerability Management Procedure 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 Vulnerability Management Procedure 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.

Changes since version 09-07-2016

Page 5 – in Removal of affected software section – added last bullet - **Software shall be removed when it is end of life and no longer supported.** This was added upon approval of MT-ISAC by Mr. Daugherty

Page 3 – Section C “Vulnerability Scanning” is a new section.