

9400-P183 – Technical Vulnerability Management

I. PURPOSE

This policy specifies how the State and State agencies will reduce the risk of attack to information and information technology (IT) resources by proactively managing exploitable vulnerabilities.

II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as "agency" or "agencies").

III. POLICY

- A. Agencies shall take proactive steps to identify and minimize vulnerabilities in their technology environments before they can be exploited.
 1. Personnel who are performing vulnerability management shall use security scanning tools on a prescribed basis to identify vulnerabilities. Multiple tools with different technologies shall be used to identify as many vulnerabilities as possible. Both Internet and Intranet-facing assets shall be scanned. The Information Resource Owner shall be notified of and accept potential effects of the scanning activity on the target environment before scanning is initiated.
 2. Third party sources of technical vulnerability information (e.g., security alerts, system patches, workarounds, and virus updates) shall be monitored for agency-relevance. As vulnerabilities are reported by these third party sources, personnel performing vulnerability management duties shall compare each vulnerability to their inventory to determine whether their IT resources are susceptible.
 3. When a vendor releases a patch or update to repair a security related control, the release shall be considered an implicit vulnerability notification and risk mitigation shall be taken.
 4. All devices attached to a State network with identified security vulnerabilities shall be patched/updated to address those vulnerabilities. If a device attached to a State network cannot be patched/updated, the vulnerability shall be mitigated with an alternate security control.
- B. Processes for detecting and remediating vulnerabilities shall be established and maintained.
 1. Software assets shall be inventoried to ensure that known vulnerabilities can be readily identified by personnel tasked with vulnerability management.

9400-P183 – Technical Vulnerability Management

2. Without impairing production and/or system performance, systems shall be up to date and patched per vendor specification or industry best security practices.
 3. Systems shall be hardened in accordance with applicable industry best security practices prior to release into the production environments.
 4. Security controls that detect malicious code, vulnerabilities, or attack signatures shall use current versions of their detection databases and/or signatures.
 5. Mitigation procedures shall be put into place in the event that vulnerabilities are exploited before they can be removed from the environment (see policy 9400-P190: Reporting Security Events and Vulnerabilities and pending policy 9400-P191: Information Security Incident Management).
 6. When appropriate, security monitoring and scanning tools shall be used to verify that remediation activities have been performed and a new system vulnerability baseline shall be created.
 7. Configuration procedures, hardening scripts, inventories, etc. shall be updated as required to reflect the current system state (after the vulnerability has been remediated). Procedures shall prevent new systems being deployed with existing vulnerabilities.
- C. Vulnerabilities shall be prioritized in terms of risk (e.g., if the vulnerability is exploited, what is the risk to their agency?). Personnel tasked with vulnerability management duties shall ensure that:
1. Vulnerabilities that pose an unacceptable risk are remediated.
 2. Vulnerabilities that pose the highest risk to State resources (e.g., resources used by multiple agencies) are fixed first before systematically progressing to lower risk vulnerabilities.
 3. Alternate security controls are employed when there is no immediate patch/update from vendor.
 4. Information Resource Owners assist with determining if system vulnerabilities pose unacceptable risks to the data, information, and/or process. ITD shall be the mediator when such a determination affects multiple agencies.
 5. Agency heads shall make the final determination of risk that is acceptable.

9400-P183 – Technical Vulnerability Management

D. Patches and Updates

1. Operating system patches and updates (e.g., service packs, firmware) shall be researched then applied when there is reasonable assurance that the patch/update will not affect production.
2. All patch and update procedures shall be conducted in accordance with established configuration management and change management policies (see policy 3100-P010: Information Technology Change Management Oversight and policy 9400-P180: Information Security in the System Lifecycle).
3. All patches and updates shall be obtained from an authorized patch delivery source.
4. No patches or updates shall be obtained or installed without the oversight or direction of appropriate agency IT staff.
5. Patch and update procedures shall include back out procedures to return to the last working configuration whenever possible.

CIO Approved Date: 1/5/2011