State of Iowa Enterprise Vulnerability Management
Security Standard
May 9, 2012

Purpose
This Standard establishes the minimum requirements for vulnerability management for state IT systems.

Overview
The State of Iowa maintains a variety of data in its IT systems, including confidential customer information. In order to protect data and systems it is necessary to identify and remediate vulnerabilities in those systems. Vulnerability scanning identifies security weaknesses within systems and allows agencies to prioritize their resources to the most critical areas. Timely remediation of vulnerabilities is critical to maintaining the availability, confidentiality, and integrity of information technology (IT) systems.

Scope
This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise standards.

Definitions
Selected terms used in the Enterprise Vulnerability Management Standard are defined below:

- **Authenticated Scan**: Vulnerability scan conducted using system credentials.
- **Critical Vulnerabilities**: Vulnerabilities identified as critical by software\hardware vendors, EVMS scanning tool; or vulnerabilities with a CVSS[1] rating of 9.0 or higher.
- **Enterprise Vulnerability Management System (EVMS)**: Enterprise-wide system to:
  - Inventory software\hardware deployed in an agency,
  - Identify vulnerabilities in the software\hardware; and
  - Report on vulnerabilities using a common format.
- **External Scan:** Vulnerability scan conducted from outside the organization's perimeter firewall.
- **Internal Scan**: Vulnerability scan conducted from within the organization's perimeter firewall.
- **Remediation:** Correction of the vulnerability or elimination of the threat. Examples of remediation efforts include: installation of a software patch, adjustment of a configuration setting, or removal of affected software.
- **Vulnerability:** Software flaw or misconfiguration that causes a weakness in the security of a system. Vulnerabilities can be exploited by a malicious entity to violate policies—for example, to gain greater access or permission than is authorized on a computer.
- **Vulnerability Scan**: Scan to identify hosts/host attributes and associated vulnerabilities.

[1] Common Vulnerability Scoring System (CVSS) http://nvd.nist.gov/cvss.cfm

Elements

The following are the elements of the Enterprise Vulnerability Management Security Standard.

1. **Inventory**: Agencies shall maintain an inventory of hardware, operating systems, and software applications used within the agency.

2. **Monitor**: Agencies shall monitor security sources for vulnerability announcements, patch notifications, and emerging threats.

3. **Scans**: Agencies shall conduct vulnerability scans of their network using an Enterprise Vulnerability Management System (EVMS) system.
    a. External, internal and authenticated scans shall be conducted.
    b. Scans shall be conducted at least weekly.
    c. New systems and applications shall be scanned before going to production.

4. **Access**: Server administrators shall provide sufficient administrative access to allow the vulnerability scan engine to scan all services provided via their systems.

5. **Exceptions\Credentials**: Firewall exceptions and credentials used by the EVMS in performing vulnerability scans shall be deactivated when not in use.

6. **Remediation**: Agencies shall remediate vulnerabilities identified (via scanning, vendor alert or the National Vulnerability Database) as follows:

    a. **High Risk\Critical Vulnerabilities With An Active Exploit**: Within 5 business days of discovery\notification;

    b. **High Risk\Critical Vulnerabilities With No Active Exploit**: Within 10 business days of discovery\notification;

    c. **Medium Risk Vulnerabilities**: Within 30 business days of discovery\notification.

    d. **All Others**: According to the agency remediation\patch management schedule.

7. **Vulnerabilities**: Agencies shall maintain a list of un-remediated vulnerabilities.

    a. Agencies shall notify the Information Security Office monthly of un-remediated vulnerabilities.

    b. Agencies shall accept responsibility for any un-remediated vulnerability in their systems.

8. **Training:** Agencies shall train system administrators on vulnerability monitoring and remediation.

Updates This document shall be reviewed at least every two years and updated as needed.

Effective Date This standard shall be effective September 30, 2012.

Enforcement This standard shall be enforced pursuant to Iowa Administrative Code 11—25.11(8A).

Variance Iowa Administrative Code 11 - 25.11(2) provides for variances from security standards. Requests for a variance from any of the requirements of this policy will be submitted in writing to the Chief Information Security Officer prior to implementation. http://das.ite.iowa.gov/standards/waiver.html