

# State of Minnesota



Office of Enterprise Technology (OET)

## **Enterprise Vulnerability Management Security Standard**

Enterprise Security Office (ESO) Standard

Version 1.00

Approval:

**Gopal Khanna**

State Chief Information Officer

Signature

Approval Date



## Table of Contents

<b>1.0 STANDARD STATEMENT</b> .....	<b>3</b>
1.1 BUSINESS RISK ASSESSMENT PROCESS.....	3
1.2 REPORTING REQUIREMENTS .....	3
1.3 VULNERABILITY MANAGEMENT CONTROL PHASES.....	3
1.4 VULNERABILITY MANAGEMENT CONTROL PHASES REQUIREMENTS .....	4
<b>2.0 ROLES &amp; RESPONSIBILITIES</b> .....	<b>6</b>
2.1 OFFICE OF ENTERPRISE TECHNOLOGY .....	6
2.2 GOVERNMENT ENTITY .....	6
<b>3.0 RELATED INFORMATION</b> .....	<b>7</b>
3.1 REASON FOR STANDARD .....	7
3.2 APPLICABILITY AND EXCLUSIONS .....	7
3.3 REFERENCES .....	7
3.4 FORMS AND INSTRUCTIONS .....	7
3.5 COMPLIANCE.....	7
<b>APPENDIXES:</b> .....	<b>8</b>
APPENDIX A: ASSET EXPOSURE.....	8
APPENDIX B: STANDARD VULNERABILITY SCANNING REQUIREMENTS .....	9
APPENDIX C: VULNERABILITY PRIORITIZATION .....	9
APPENDIX D: ENTERPRISE VULNERABILITY METRICS .....	10
<b>HISTORY &amp; OWNERSHIP</b> .....	<b>11</b>
REVISION HISTORY – RECORD ADDITIONS AS MAJOR RELEASES, EDITS/CORRECTIONS AS MINOR.....	11
REVIEW HISTORY – PERIODIC REVIEWS TO ENSURE COMPLIANCE WITH PROGRAM .....	11
APPROVAL HISTORY – RECORD OF APPROVAL PHASES.....	11
OWNERSHIP – CURRENT OWNERS OF THE DOCUMENT .....	11



## Enterprise Security Office Standard

### 1.0 Standard Statement

To manage vulnerability exposure across the Executive branch the following requirements must be incorporated by government entities in order to comply with the Enterprise Vulnerability Management Policy.

#### 1.1 Business Risk Assessment Process

Each government entity must:

- Assess and assign an Asset Exposure ranking to all *computing devices* based on their risk (see Appendix A)
- Document exposure ranking in the Enterprise Vulnerability Management System (EVMS)

#### 1.2 Reporting Requirements

The following reporting requirements are necessary to ensure compliance to this document:

##### 1.2.2 Enterprise Vulnerability & Threat Management Team (VTMT)

- Report enterprise vulnerability management metrics (**Appendix D**) to the State CISO on a monthly basis.
- Report to effected government entities any critical and high vulnerabilities found during external scanning

##### 1.2.3 Government Entity

- Report external facing networks and systems to the Enterprise VTMT to facilitate external scanning
- Must escalate unresolved vulnerabilities to the Enterprise Security Office (ESO) of the vulnerability to determine enterprise mitigation requirements.
- Must escalate vulnerabilities that could cause an enterprise security incident (see **Enterprise Security incident management Standard**) to the ESO
- Must report vulnerability management exclusions to ESO on a monthly basis (see **Section 1.4, Phase G**)

#### 1.3 Vulnerability Management Control Phases

In order to meet the requirements of the Enterprise Vulnerability Management Standard the following phases must be implemented (see detailed requirements in section 1.4):

- A. Initialize and Configuration
- B. Asset Discovery
- C. Vulnerability Scanning
- D. Vulnerability Analysis
- E. Vulnerability Resolution
- F. Resolution Confirmation
- G. Vulnerability Reporting



# Enterprise Security Office Standard

## 1.4 Vulnerability Management Control Phases Requirements

The government entity must implement and maintain the following detailed requirements to address each phase of the vulnerability management process:

Phase		Requirements										
<b>A</b>	<b>Initialize and Configuration</b>	<ul style="list-style-type: none"> <li>Identify all networks by IP addresses</li> <li>Identify all operational support teams (OST) with vulnerability management responsibilities</li> <li>Report external facing networks and systems to the Enterprise VTMT</li> </ul>										
<b>B</b>	<b>Asset Discovery</b>	<ul style="list-style-type: none"> <li>Inventory all <i>computing devices</i> that generate, process, transmit, or store government data</li> <li>All <i>computing devices</i> must have a designated operational support team and a separate <i>data owner</i> assigned</li> <li>Computing devices must be assessed for exposure criticality (see <b>Appendix A</b>)</li> </ul>										
<b>C</b>	<b>Vulnerability Scanning</b>	<p><b>Internal Assessment</b></p> <p>All computing devices must be scanned with the Enterprise Vulnerability Management System (EVMS).</p> <p>Scan Requirements</p> <ul style="list-style-type: none"> <li>At a minimum, all computing devices must be scanned with the Standard Scanning Requirements (see <b>Appendix B</b>)</li> <li>Target <i>computing devices</i> must be accessible for scanning.</li> </ul> <p>Entity Specific Minimum Scan Frequency:</p> <table border="1"> <thead> <tr> <th>Risk Exposure Rating</th> <th>Frequency</th> </tr> </thead> <tbody> <tr> <td>Critical</td> <td>Weekly</td> </tr> <tr> <td>High*</td> <td>Weekly</td> </tr> <tr> <td>Medium</td> <td>Monthly</td> </tr> <tr> <td>Low</td> <td>Quarterly</td> </tr> </tbody> </table> <p>* NOTE: Computing devices without a risk exposure rating must be scanned as High until rated</p> <p><b>External Assessment</b></p> <p>All State of Minnesota publicly routable IP addresses (i.e., devices that are accessible from the Internet) must be scanned on a monthly basis by the Enterprise VTMT.</p> <p>Scan Requirements:</p> <ul style="list-style-type: none"> <li>Devices must be scanned with the standard Enterprise VTMT scan profile</li> <li>External scan must be conducted at least monthly</li> <li>External scans must be conducted from ESO authorized external IP addresses</li> <li>Targeted computing devices must be accessible by the ESO authorized IP addresses (scanning devices)</li> <li>ESO authorized scanning devices must not have any privileged access</li> </ul>	Risk Exposure Rating	Frequency	Critical	Weekly	High*	Weekly	Medium	Monthly	Low	Quarterly
Risk Exposure Rating	Frequency											
Critical	Weekly											
High*	Weekly											
Medium	Monthly											
Low	Quarterly											



## Enterprise Security Office Standard

<b>D</b>	<b>Vulnerability Analysis and Prioritization</b>	<ul style="list-style-type: none"> <li>• Vulnerabilities must be validated in a timely manor</li> <li>• Vulnerabilities rated as critical by either the vendor or US-CERT (<a href="http://nvd.nist.gov/">http://nvd.nist.gov/</a>) must be validated within 24 hours of acknowledgement of the vulnerability</li> <li>• False positive must be reported to the VTMT as soon as possible</li> </ul>												
<b>E</b>	<b>Vulnerability Resolution</b>	<ul style="list-style-type: none"> <li>• Resolution of critical and high vulnerabilities are prioritized based on asset exposure rating. (see <b>Appendix C</b>)</li> <li>• Vulnerabilities must be resolved within the timelines listed in the table below             <ul style="list-style-type: none"> <li>○ “Action Plan By” is the time from the scan completion to identify and document a resolution</li> <li>○ “Resolved Within” is the time from the scan completion to the implementation of the resolution</li> </ul> </li> </ul> <table border="1" data-bbox="548 751 1203 884"> <thead> <tr> <th>Priority</th> <th>Action Plan By</th> <th>Resolved Within</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>1 Day</td> <td>1 Week</td> </tr> <tr> <td>2</td> <td>1 Week</td> <td>1 Month</td> </tr> <tr> <td>3</td> <td>2 Weeks</td> <td>6 Weeks</td> </tr> </tbody> </table> <ul style="list-style-type: none"> <li>• All other vulnerabilities are resolved at agencies discretion</li> </ul>	Priority	Action Plan By	Resolved Within	1	1 Day	1 Week	2	1 Week	1 Month	3	2 Weeks	6 Weeks
Priority	Action Plan By	Resolved Within												
1	1 Day	1 Week												
2	1 Week	1 Month												
3	2 Weeks	6 Weeks												
<b>F</b>	<b>Resolution Confirmation</b>	<ul style="list-style-type: none"> <li>• Testing must be done to determine that remediation has been completed or the mitigating controls put in place are effective</li> <li>• False positives must be reported to the VTMT as soon as possible</li> </ul>												
<b>G</b>	<b>Vulnerability Reporting</b>	<p>Government entities must report on which computing devices have been excluded from vulnerability scanning and why</p> <p>The Enterprise VTMT must provide monthly:</p> <ul style="list-style-type: none"> <li>• Aggregate asset discovery and vulnerability scanning reports</li> <li>• Vulnerability resolution reports</li> </ul>												



## 2.0 Roles & Responsibilities

### 2.1 Office of Enterprise Technology

- Maintain this document
- Conduct enterprise wide vulnerability scans
- Monitor enterprise vulnerability resolution process
- Provide aggregated reporting on enterprise vulnerability findings
- Provide training and guidance on this standard and related tools
- Provide threat tracking and dissemination services
- Work with government entities on defining acceptable mitigating controls
- Maintain an Enterprise Vulnerability and Threat Management Team (VTMT)
- Maintain the Enterprise Vulnerability Management System (EVMS)
- Identification and escalation of enterprise wide vulnerabilities
- Adjust vulnerability risk rating based on potential impact to the enterprise
- Fulfill the Government Entity roles and responsibilities for the Office of Enterprise Technology

### 2.2 Government Entity

- Identify information assets and define their criticality
- Maintain remediation and mitigation processes for resolving vulnerabilities
- Maintain an entity specific exception process for risk acceptance of unresolved vulnerabilities
- Report vulnerability scanning data into enterprise vulnerability management system
- Maintain an entity specific vulnerability and threat management team
- Conduct internal vulnerability scanning



### 3.0 Related Information

#### 3.1 Reason for Standard

Vulnerability Management is essential to help reduce the overall reputational and regulatory risks posed by breaches in security caused by the exploitation of known vulnerabilities. The proper management of security vulnerabilities must also be done to help organizations understand their vulnerability risk exposure.

Government entity and enterprise procedures for the management of vulnerabilities must have a consistent approach across the Executive branch to ensure the proper identification and resolution of security vulnerabilities.

#### 3.2 Applicability and Exclusions

This standard is applicable to all government entities identified in the Enterprise Security Applicability Standard. It is also offered as guidance to other government entities outside the Executive Branch.

Agency Heads, Responsible Authorities, Chief Information Officers, Chief Information Security Officers, Data Practices Compliance Officials, and their designees who are responsible for responding to, management of, and reporting on security incidents must be aware of this standard.

The requirements of this standard must be incorporated into agreements with third parties to ensure proper notification of information security incidents and their impact on state information assets.

#### 3.3 References

Minnesota Statutes 16E Office of Enterprise Technology  
Enterprise Vulnerability Management Policy  
Enterprise Vulnerability Resolution Process Guideline  
Enterprise Security Glossary of Terms

#### 3.4 Forms and Instructions

Terms in *italics* can be found in the Enterprise Security Glossary of Terms.

Requests for changes and additions to this document maybe submitted to the Enterprise Security Office for consideration. All submissions must include the specific change and a detailed reason for the change.

#### 3.5 Compliance

Compliance to this standard is required within 1 year from approval date.



# Enterprise Security Office Standard

## Appendixes:

### Appendix A: Asset Exposure

Impact Rating:	Risk Exposure			
	Standalone system with limited or no network connectivity	System with network visibility is limited to local network	System with network visibility is available to MNET or a broader audience (not internet facing)	System visibility is available from the internet
<p><b>HIGH IMPACT:</b></p> <p><b>Confidentiality:</b> System contains not public data</p> <p><b>Availability:</b> System must be available at all times.</p> <p><b>Integrity:</b> System transmits, processes or stores important data that may be used to make significant business decisions</p>	Medium	High	Critical	Critical
<p><b>MODERATE IMPACT:</b></p> <p><b>Confidentiality:</b> System contains data with an unknown classification</p> <p><b>Availability:</b> System can experience some down time or limited availability outside of normal business hours</p> <p><b>Integrity:</b> system contains data that is important to the business function of the agency</p>	Low	Medium	High	Critical
<p><b>LOW IMPACT:</b></p> <p><b>Confidentiality:</b> System does not contain Not Public data</p> <p><b>Availability:</b> System can experience extended down time or no availability required outside of normal business hours.</p> <p><b>Integrity:</b> Does not transmit, process or store data that is important to the business function of the agency.</p>	Low	Low	Medium	High



## Enterprise Security Office Standard

### Appendix B: Standard Vulnerability Scanning Requirements

The following table lists the minimum requirements for vulnerability scanning

Item	Description
Host Discovery	Identify hosts on a network through ICMP ping and TCP connections on common TCP ports.
Port Scanning	Identify open ports, by scanning for commonly used ports and ports associated with known vulnerabilities.
Stack Fingerprinting	Identify operating systems and third party applications.
Application Scan	Identify vendor and version of the application
Vulnerability Scan	Scans for all known vulnerability conditions.
Host Configuration Check	Provides basic configuration information, such as machine name, available shares, banners, such as SSH or SMTP banners.
Vulnerability Rules: Verified	Ensure all vulnerability rules are "verified" by the vendor to execute for a scan profile.
Vulnerability Rules: Intrusive	Disables rules that are known to cause applications to crash or access violations.
Vulnerability Rules: Auth Attempt	Attempt authentication without credentials and using default accounts and passwords.
Credentials scanning	Authenticated scans must be conducted on all internal computing devices, except where limitations in the tool or specific environment prevent authenticated scanning.

### Appendix C: Vulnerability Prioritization

All validated vulnerabilities must be remediated based on the following prioritization matrix:

Asset Exposure	Vulnerability Severity*			
	Low	Medium	High	Critical
<b>Critical</b>	Entity Discretion	Entity Discretion	Priority 2	Priority 1
<b>High</b>	Entity Discretion	Entity Discretion	Priority 3	Priority 2
<b>Medium</b>	Entity Discretion	Entity Discretion	Entity Discretion	Entity Discretion
<b>Low</b>	Entity Discretion	Entity Discretion	Entity Discretion	Entity Discretion

\* Vulnerability Severity is determined by the rating provided by the vendor and the Common Vulnerability Scoring System (CVSS) run by the National Institute for Standards and Technology's (NIST) with other federal agencies and compiled into the national vulnerability database (<http://nvd.nist.gov>).



### Appendix D: Enterprise Vulnerability Metrics

The Enterprise VTMT's must collect the following metrics:

- Aggregate asset discovery and vulnerability scanning metrics:
  - Percent of total IT assets scanned per month
  - Number of assets per criticality (critical, high, medium and low)
  - Number and percentage of assets scanned by criticality
  - Percentage of assets scanned in accordance with criticality scan frequency; total and by criticality rating
- Vulnerability resolution metrics
  - Number of vulnerabilities in total and by priority
  - Number of new vulnerabilities in total and by priority
  - Number of vulnerabilities resolved in total and by priority
  - Number of vulnerabilities resolved within standard time frame for the given priority in total and by priority



## Enterprise Security Office Standard

### History & Ownership

Revision History – record additions as Major releases, edits/corrections as Minor

Date	Author	Description	Major #	Minor #
<TBD>	Neal Dawson	Initial Release	1	00

Review History – periodic reviews to ensure compliance with program

Date	Reviewer	Description	Compliance

Approval History – record of approval phases

Phase	Description	Date
SME	Neal Dawson Eric Breece ESO Governance Team	
ISC	Information Security Council Approval	
CIOC	CIO Council Approval	
CAB	Commissioners' Advisory Board Approval	

Ownership – current owners of the document

	Owner	Division	Department
Primary	Deb Stafford	Enterprise Security Office (ESO)	Planning & Preventive Controls
Secondary	Neal Dawson	Enterprise Security Office (ESO)	Planning & Preventive Controls