Maryland

DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

STATE MINIMUM CYBERSECURITY STANDARDS

Version 1.0

Date Issued: May 22, 2023

Date Last Revised: May 22, 2023

Maryland Government
Department of Information Technology
100 Community Place
Crownsville, MD 21032

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary
Melissa Leaman | Deputy Secretary

Table of Contents

List of Tables

Revision Control History

Date	Reason for Change	Changed by	Version
05/25/2023	Finalized 2023 State Minimum Security Standards	Office of Security Management	1.0

Table 1: Revision Control History

Approval

Katherine M. Savage
_____
Secretary Katie Savage

May 26, 2023
_____
Date

1. Executive Summary

This document establishes the State Minimum Cybersecurity Standards for each agency or unit of the Executive Branch of State government.

2. Purpose

Pursuant to Section 5 of SB812, Ch. 242 (2022),[1] in a manner and frequency established in regulations adopted by the Department of Information Technology (DoIT), each agency in the Executive Branch of State government shall certify to the Office of Security Management compliance with State Minimum Cybersecurity Standards established by DoIT on or before Jun 30, 2023. Statewide NIST Cybersecurity Framework Assessments, as performed by an independent assessor, may serve the purpose "review" by independent auditors.

3. Scope

This standard applies to each agency or unit of the Executive Branch of State government ("unit of State government").

4. Authority

- Section 5 of SB812, Ch. 242 (2022)

5. Definitions & Acronyms

All defined terms below should be capitalized within the document and defined below.

Acronym/Phrase	Definition
CSF	Cybersecurity Framework, published by NIST

[1] See Maryland SB0812 (2022) at https://mgaleg.maryland.gov/2022RS/bills/sb/sb0812E.pdf

CMMI	Cybersecurity Maturity Model Institute
DoIT	Maryland Department of Information Technology
NIST	National Institute of Standards and Technology

Table 2: Definitions & Acronyms

6. Standards

The State of Maryland's Minimum Cybersecurity Standards align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), consisting of controls that contribute to an organization's overall cybersecurity maturity while mitigating or reducing cybersecurity risk and vulnerabilities. The controls below are subject to change on an annual basis and represent the "State Minimum Cybersecurity Requirements" required for the June 30, 2023 certification. Independent audit or 3rd party assessment [2]must validate that each control meets a minimum Cybersecurity Maturity Model Institute (CMMI) maturity score of *at least* a "1" (meaning "Initial" or "Performed) or "2" (meaning "Managed"), depending on the control.

A score of "**1**" indicates that the control is **performed** by the organization in an ad-hoc fashion without consistency or documentation. A score of "**2**" indicates the control is **performed consistently with supporting documentation** such as written plans, procedures, or standards. To certify compliance, units of State government must meet the minimum required CMMI maturity scores for each NIST CSF control in sections below.

6.1 Identify (ID) Controls

CSF Control #	CSF Subcategory	Min Requirement
ID.AM-1	Physical devices and systems within the organization are inventoried.	1

[2] All Executive Branch units of State Government are required to have a NIST CSF assessment performed bi-annually. Recent assessments performed by RSM provide CMMI-aligned maturity scores in the appendices section of the assessment. Draft or Final assessment scores may be used to meet minimum requirements.

CSF Control #	CSF Subcategory	Min Requirement
ID.AM-2	Software platforms and applications within the organization are inventoried	1
ID.AM-3	Organizational communication and data flows are mapped	1
ID.AM-4	External information systems are catalogued	1
ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	1
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	2
ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	1
ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	2
ID.BE-4	Dependencies and critical functions for delivery of critical services are established	2
ID.BE-5	Resilience requirements to support delivery of critical services are established	2
ID.GV-1	Organizational information security policy is established and communicated	2
ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	1
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	1
ID.RA-1	Asset vulnerabilities are identified and documented	1
ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	1
ID.RA-3	Threats, both internal and external, are identified and documented	1
ID.RA-4	Potential business impacts and likelihoods are identified	1
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	2
ID.RA-6	Risk responses are identified and prioritized	2
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	1
ID.RM-2	Organizational risk tolerance is determined and clearly expressed	1

CSF Control #	CSF Subcategory	Min Requirement
ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	1

6.2 Protect (PR) Controls

CSF Control #	CSF Subcategory	Min Requirement
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	2
PR.AC-2	Physical access to assets is managed and protected	2
PR.AC-3	Remote access is managed	2
PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties	2
PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	1
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	1
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	1
PR.AT-1	All users are informed and trained	1
PR.AT-2	Privileged users understand roles & responsibilities	1
PR.AT-4	Senior executives understand roles & responsibilities	1
PR.AT-5	Physical and information security personnel understand roles & responsibilities	1
PR.DS-1	Data-at-rest is protected	1
PR.DS-2	Data-in-transit is protected	1
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	1
PR.DS-5	Protections against data leaks are implemented	1
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	1
PR.IP-4	Backups of information are conducted, maintained, and tested periodically	1
PR.IP-6	Data is destroyed according to policy	1

CSF Control #	CSF Subcategory	Min Requirement
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	2
PR.IP-10	Response and recovery plans are tested	1
PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	1
PR.IP-12	A vulnerability management plan is developed and implemented	2
PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	1
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	1
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	1
PR.PT-2	Removable media is protected and its use restricted according to policy	1
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	1
PR.PT-4	Communications and control networks are protected	1

6.3 Detect (DE) Controls

CSF Control #	CSF Subcategory	Min Requirement
DE.AE-2	Detected events are analyzed to understand attack targets and methods	1
DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors	1
DE.AE-4	Impact of events is determined	1
DE.AE-5	Incident alert thresholds are established	1
DE.CM-1	The network is monitored to detect potential cybersecurity events	1
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	1
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	1
DE.CM-4	Malicious code is detected	1
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	1
DE.CM-8	Vulnerability scans are performed	1

CSF Control #	CSF Subcategory	Min Requirement
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability	1
DE.DP-2	Detection activities comply with all applicable requirements	1
DE.DP-4	Event detection information is communicated to appropriate parties	1
DE.DP-5	Detection processes are continuously improved	1

6.4 Respond (RS) Controls

CSF Control #	CSF Subcategory	Min Requirement
RS.RP-1	Response plan is executed during or after an event	2
RS.CO-1	Personnel know their roles and order of operations when a response is needed	1
RS.CO-2	Incidents are reported consistent with established criteria	1
RS.CO-3	Information is shared consistent with response plans	1
RS.CO-4	Coordination with stakeholders occurs consistent with response plans	1
RS.AN-1	Notifications from detection systems are investigated	1
RS.AN-2	The impact of the incident is understood	1
RS.AN-3	Forensics are performed	1
RS.AN-4	Incidents are categorized consistent with response plans	1
RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	1
RS.MI-1	Incidents are contained	1
RS.MI-2	Incidents are mitigated	1
RS.IM-1	Response plans incorporate lessons learned	2

6.5 Recover (RC) Controls

CSF Control #	CSF Subcategory	Min Requirement
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident	2
RC.CO-1	Public relations are managed	1
RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams	1

6.6 Insurance Application Requirement Standard

All units of State government must submit an annual Insurance Supplemental Application by to qualify for cybersecurity insurance coverage under the State's policy. Insurance Supplemental Applications shall be submitted at the time of Statement of Compliance submission via Secure File Transfer. Alternatively, the Insurance Supplemental Application can be submitted via encrypted email to Muriel Turner (mturner@treasurer.state.us.md) in the Maryland Treasurer's Office.

7. Roles & Responsibilities

To certify a unit of State Government's Minimum Cybersecurity Standards, the following roles and responsibilities shall be established:

Role	Responsibility
DoIT OSM	Update the State's Minimum Cybersecurity Standards as needed
DoIT Secretary	Review and Approve the State's Minimum Cybersecurity Standards
Unit of State Government	Complete online form submission to certify minimum cybersecurity standards; and Complete Statement of Compliance, Insurance Supplemental Application, and Remediation Plan and Status (if required); and Submit online form with required documents to DoIT by June 30th of current year
Authorized Signee for Unit of State Government	Sign Statement of Compliance on behalf of unit of State Government

8. Documents and Maintenance

The following documents shall be maintained in conjunction with this standard:

Document	Description
Statement of Compliance	Signed statement certifying compliance with standards
Remediation Plan	Plan for remediation of any controls receiving a “0 – Not Performed” maturity score
Insurance Supplemental Application Over $200M Annual Revenue	Required for Submission for Insurance Coverage
Insurance Supplemental Application Under $200M Annual Revenue	Required for Submission for Insurance Coverage

9. Appendices

9.1 Appendix A - Statement of Compliance

Date: [Date]

To: [DoIT Secretary]

From: [Organizational Representative]

Subject: [Statement of Compliance]

Dear [DoIT Secretary],

Pursuant to the requirements established in Senate Bill 812 (2002), and after consultation with our qualified information technology and cybersecurity experts, I certify, to the best of my knowledge, that:

- A 3rd party evaluation or audit of our cybersecurity preparedness evaluating all NIST CSF controls has been performed within the previous two (2) years; and
- Our systems are compliant with the State's Minimum Cybersecurity Standards; and/or
- All controls not performed at the time of 3rd party assessment or audit are documented in a "Remediation Plan & Status" document submitted to DoIT; and
- We have ensured that the State has up-to-date contact information for our Information Technology and Cybersecurity team.

Sincerely,

[Signature]

[Name]

[Title]

9.2 Appendix B – Remediation Plan

Org Name: [Enter Unit of State Government Name]

Plan Submitted by: [Enter Name of Individual Completing This Form]

Role of Submitter: [Enter Role of Individual Completing This Form]

Email of Submitter: **[Enter Email Address] Phone # for Submitter:** Enter Phone #

Directions: For any non-remediated controls that do not meet the specified CMMI Maturity Score per the State's Minimum Cybersecurity Standard at the time of 3rd party assessment, each Maryland unit of State Government shall complete this form and submit to the Department of Information Technology, Office of Security Management prior to June 30, 2023.

CSF Control #	CSF Subcategory	Plan to Remediate Control	Remediation Status
Enter Control #	Enter Subcategory description	Enter Remediation Plan	Enter "Complete" or "To Be Performed"