Maryland

DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

GUIDELINES FOR LOCALS TO CERTIFY COMPLIANCE WITH STATE MINIMUM CYBERSECURITY STANDARDS

Version 1.0

Date Issued: June 7, 2023

Date Last Revised: June 9, 2023

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

Table of Contents

1. EXECUTIVE SUMMARY 4
2. PURPOSE 4
3. SCOPE 4
4. AUTHORITY 4
5. AUDIENCE 5
6. DEFINITIONS & ACRONYMS 5
7. GUIDELINES 6
7.1 CERTIFICATION 6
7.2 REMEDIATION 7
8. DOCUMENTS AND MAINTENANCE 7
9. APPENDICES 8
9.1 APPENDIX A – STATEMENT OF COMPLIANCE 8
9.2 APPENDIX B ASSESSMENT TOOL 9

List of Tables and Figures

Table 1: Revision Control History 2
Table 2: Definitions & Acronyms 3

Revision Control History

Date	Reason for Change	Changed by	Version
06/07/2023	Original Guidelines Draft	Netta Squires	1.1

Table 1: Revision Control History

Approval

Katherine M. Savage

Katie Savage
Secretary

Jun 13, 2023

Date

1. Executive Summary

Pursuant to Section 5 of SB754 (CH. 241, 2022), each unit of local government must certify its compliance with the State Minimum Cybersecurity Standards (SMCS) established by the Department of Information Technology (DoIT). The certification process must be completed and submitted to the Office of Security Management (OSM) no later than June 30, 2023. The certification is subject to review by independent auditors, and any identified findings must be remediated.

If a unit of local government fails to remediate findings pertaining to State cybersecurity standards identified in the independent audit by July 1, 2024, the Office of Security Management will provide guidance to the unit on achieving compliance with the cybersecurity standards.

The document provides essential information, instructions, and recommendations to assist the Units of Local Government in understanding the certification process, undergoing independent audits, remediating findings, and ultimately achieving compliance with the cybersecurity standards.

2. Purpose

The purpose of this guidance is to support local governments in meeting the required certification of cybersecurity standards and enhancing the overall security and protection of digital assets and sensitive information across the State.

3. Scope

This guidance is intended to be used by all Units of Local Government that are required to certify compliance with the State's Minimum Cybersecurity Standards.

4. Authority

- This guidance is intended to support the requirements established in Section 5 of SB754 (Ch. 241, 2022).

5. Audience

This guidance document is intended for units of local government, including relevant officials, administrators, and personnel responsible for cybersecurity compliance, who are required to certify their adherence to State minimum cybersecurity standards established by the Department of Information Technology.

6. Definitions & Acronyms

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

Acronym/Phrase	Definition
CMMI	Capability Maturity Model Institute
DoIT	Department of Information Technology
Independent Auditor	An external professional or firm that will review the certification by local government
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
OSM	Office of Security Management
Section 5	Section 5 of Senate Bill 754 that relates to local government certification to OSM
Senate Bill 754	Local Cybersecurity Support Act of 2022
SMCS	State Minimum Cybersecurity Standards

Table 2: Definitions & Acronyms

7. Guidelines

7.1 Certification

7.1.1 Timing

On or before June 30, 2023, each unit of local government shall certify to the Office of Security Management compliance with State minimum cybersecurity standards established by the Department of Information Technology.

7.1.2 Manner of Certification

Certification may be submitted by providing DoIT with the Statement attached in Appendix A below, or electronically by completing this form (https://forms.gle/kuAvYjksMKFpj38D6). Certification should be made by an individual within the organization having signatory authority.

To assess compliance with Maryland's SMCS, units of local governments should review the State's Minimum Cybersecurity Standards published on OSM's website.

7.1.2.1 NIST CSF Controls as the Standard

Units of local government should adhere to the State Minimum Cybersecurity Standards, which are based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) controls. The NIST CSF is a widely recognized and widely adopted framework that provides guidance and a common language for organizations to manage and improve their cybersecurity posture.

7.1.2.2 CMMI Maturity Rating

CMMI stands for Capability Maturity Model Integration. It is a globally recognized framework used to evaluate and improve the process maturity and capabilities of organizations across various domains, including software development, systems engineering, and service delivery. CMMI provides a set of best practices and guidelines that help organizations optimize their processes, enhance productivity, and deliver high-quality products and services.

7.1.2.3 Mapping Compliance to NIST CSF Controls/ SMCS

As part of the certification process, units of local government should demonstrate how their cybersecurity measures align with the NIST CSF controls. This mapping will illustrate how the organization has implemented appropriate controls in each category to mitigate risks and enhance cybersecurity resilience.

Units of local government may use the worksheet in Appendix B below to help assess alignment with the SMCS. Units of local government may also leverage the available resources provided by NIST, such as the NIST CSF Framework, implementation guides, and other documentation.

Units of local government are encouraged to conduct comprehensive risk assessments based on the NIST CSF framework. These assessments will help identify and prioritize cybersecurity risks specific to the organization and guide the implementation of controls tailored to address those risks.

7.1.3 Review by Independent Auditors

Pursuant to Section 5., certification shall be reviewed by independent auditors, and any findings must be remediated. The certification of compliance must be based on an independent assessment conducted within two years of submission. The assessment must evaluate the NIST CSF controls, in the State's Minimum Cybersecurity Standards (SMCS), using the Capability Maturity Model Integration (CMMI) cybersecurity Maturity Scale.

If an assessment was performed in the past two years that does not explicitly align to CSF controls in the SMCS, the assessed org may have the independent auditor validate that the SMCS are met. For example, if a maturity assessment aligned to a different framework such as CIS, was performed by an independent assessor, the assessor may validate that the SMCS are met.

7.2 Remediation

7.2.1 Timing

Units of local government should remediate any findings by July 1, 2024.

7.2.2 Non-remediated Findings

Pursuant to Section 5, if a unit of local government has not remediated any findings pertaining to State Minimum Cybersecurity Standards found by the independent audit by July 1, 2024, the Office of Security Management shall provide guidance for the unit to achieve compliance with the cybersecurity standards.

8. Documents and Maintenance

This document shall be posted on DoIT's website. DoIT reserves the right to update the guidance as necessary.

9. Appendices

9.1 Appendix A – Statement of Compliance

Date: [Date]
To: Katie Savage, Secretary
From: [Organizational Representative]
Subject: Certification of Compliance

Dear Secretary Savage

Pursuant to the requirements established in Section 5 of Senate Bill 754 (Ch. 241, 2022), I certify, to the best of my knowledge, that (please check the applicable statement):

- _____ (name of jurisdiction) complies with the State Minimum Cybersecurity Standards and this statement has been assessed by an independent auditor.
- _____ (name of jurisdiction) complies with the State Minimum Cybersecurity Standards and an assessment of this statement by an independent auditor will be conducted.
- _____ (name of jurisdiction) does NOT fully comply with the State Minimum Cybersecurity Standards and this statement has been assessed by an independent auditor.
- _____ (name of jurisdiction) does NOT fully comply with the State Minimum Cybersecurity Standards and an assessment of this statement by an independent auditor will be conducted.

Sincerely,
[Signature]

[Name]
[Title]

9.2 Appendix B Assessment Tool

LOCAL Assessment Tool for Certification of MD State Min Security Requirements - NIST CSF