Maryland

DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

# Minimum Security Standards for Connecting to networkMaryland™

# Table of Contents

# Revision History

| Version | Date | Description of Changes |
|---|---|---|
| 1.0 | October 1, 2022 | Initial Version |

# Approval

Charles I Stewart IV

Charles "Chip" Stewart
State Chief Information Security Officer

**10/1/2022**
Date

# Introduction

Pursuant to Section 3.5-404 of SB754, Ch. 241 (2022)[1], in a manner and frequency established in regulations adopted by the Department, each unit of local government and any local agencies that use the network established in subsection (B) of Maryland State Finance and Procurement §3.5-404, hereafter referred to as networkMaryland™, shall certify to the Department of Information Technology (Department) that the unit is in compliance with the Department's minimum security standards.

# Scope

The Department interprets the scope of this requirement to include any entities connecting to the networkMaryland™ network.

# Frequency

While not yet established in regulation, the Department requires certification of compliance at least annually or within 30 days of identifying a circumstance of material non-compliance, as determined by the State Chief Information Security Officer.

# Manner of Certification

A statement of compliance, attached below as Appendix A, must be provided to the DoIT Secretary by an individual within the organization that has signatory authority.

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

# Standard

## Internet

- Maintain a network boundary device or devices capable of performing packet filtering to ensure that only authorized traffic is permitted over the networkMaryland™ Internet connection.
    - It is also recommended that all customers monitor the connection using the following security functions: content filtering, intrusion detection/intrusion prevention system (IDPS), and authentication.
- Ensure that devices connected directly to networkMaryland are installed and designed in a secure configuration, regularly monitored, and upgraded.
- Conduct, at least quarterly, reviews of the external network exposure:
    - This could be achieved in several ways, including network port scans of all assigned public IP addresses, attack surface detection services, or other tools.
- Maintain the ability to suspend/temporarily deactivate the connection to networkMaryland in the event that suspicious or malicious activity is detected.
- Prohibit direct external access to high-risk or frequently abused network protocols (listed below) except from specific, authorized, network addresses.
- In a timely manner, respond to notifications from the State Security Operations Center regarding reports of malicious activity, vulnerable services, or other security issues that could create operational risk to the networkMaryland network.

## Statewide Government Intranet (SwGI)

- Implement all standards required for Internet connections as described above
  **AND**
- Monitor the connection using advanced security functions such as content filtering, intrusion detection systems, and intrusion prevention systems.
- Limit access for non-employees to only specific systems.
- Use authentication where appropriate.
- Monitor and log all connections to SwGI to include session information (e.g., source, destination, session start, session end, bytes transferred, etc.).
- Ensure that all systems with access to SwGI are maintained in compliance with the Maryland IT Security manual. To include, at a minimum:
    - Vulnerability identification and remediation
    - Maintain up-to-date antivirus protection
    - Are designed and maintained in a secure configuration, regularly monitored, and updated. (e.g., Center For Internet Security Level 1 Baseline)

# High-Risk and Frequently Abused Protocols

The following protocols are high-risk and commonly abused, and listed with its default port(s). Moving protocols to non-standard ports is not an effective security measure.

- Remote Desktop Protocol (3389)
- Network Time Protocol (123)
- SQL/MySQL (1433,1434, 3306)
- BGP (179)
- Telnet (23)
- SMB/NetBIOS (135,137,139,445)
- SNMP (161)
- Cisco Smart Install (4786)

# Note

The Office of Security Management reserves the right to update these standards when necessary while giving notice to all interested parties before doing so.

# 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 Maryland Code, State Fin. & Proc. § 3.5-404(d), and after consultation with our qualified information technology and cybersecurity experts, I certify, to the best of my knowledge, that:

- A competent evaluation of our connectivity to the State has been performed; and
- Our systems are compliant with currently published standards; and
- We have ensured that the State has up-to-date contact information for our Information Technology and Cybersecurity team.

Sincerely,
[Signature]

[Name]
[Title]