Policy on the Utilization of a Shared Risk Management Platform

February 24, 2020
Version 1.0

Table of Contents

1 Introduction

As the technology landscape changes, many organizations are experiencing a decentralization of services at a level and in ways not previously seen. As a result, developing a comprehensive representation of the assets and risks has become more challenging. The complete picture of risk is vital to the State being able to prioritize resources appropriately. This awareness ensures that risk management execution aligns with the State's goals and objectives.

This document should not be construed as an alternative to the Maryland IT Security Manual or any other Maryland Department of IT documentation.

The wording conventions in this guidance document follow Request For Comments (RFC) 2119 (more information here: https://www.ietf.org/rfc/rfc2119.txt) and as outlined in the definitions section of this document. The words defined in this RFC are presented in **bold underline** to ensure clarity that the definition is noted.

This document will be updated as needed to provide additional clarity and as risks and mitigations evolve.

2 Applicability

The policy **applies** to all entities that meet any of the following descriptions, as defined in the Maryland Manual, hereafter referred to as "units".

- The Governor's Office and Coordinating Offices
- Each of the Twenty Principal Departments
- Each of the Maryland Independent Agencies
- Each of the Maryland Executive Commissions, Committees, Task Forces, Advisory Boards
- The Military Department
- The Office of the Attorney General
- The Board of Public Works
- The Comptroller of Maryland
- The Secretary of State
- The State Treasurer

3 Key Take-Aways

1. Units **must** provide the Office of Security management with insight into the resources that they utilize, including those in cloud providers.
2. Units **must** provide the Office of Security management with vulnerability feeds from their existing centralized tools from all assets.

3. Units that do not have a centralized vulnerability management platform that meets the requirements of the State IT Security Manual **must** either procure their own or utilize the DoIT Vulnerability management platform.
4. DoIT will provide units with access to the information collected and enriched to ensure that they are able to proactively address and remediate issues.

4 Policy

Effective 4/1/2020, all units **must** provide, upon DoIT's written request, integrations for any supported tools in the "Network Scanner", "Web Application Scanner", and "Asset Management System" categories.

Additionally, units **must** provide a detailed accounting of any public IPv4 and IPv6 network allocations, whether or not they are in active use, as a CSV file. The file format **must** match that found in Appendix A, Table 1 below. For any external domain names that are in use by the unit, including those that resolve to third party services, the unit **must** provide a list of those in a CSV file, using the format found in Appendix A, Table 2 below. File names should follow the International Organization for Standardization (ISO) format for date (ISO 8601), and use the following structure as the file name:

ISODATE.UNIT.[DNS|IP].csv

For example, 2020-02-24.DOIT.IP.csv would contain the inventory of all of the DoIT owned IPv4 and IPv6 addresses.

4.1 Supported Integrations

The following tools are supported for input. This list will be updated as new integrations are added.

- Network Scanners
    - AWS Inspector
    - BeyondTrust Retina
    - GFI LandGuard
    - Greenbone Networks OpenVAS
    - Qualys Vulnerability Management
    - Rapid7 Nexpose
    - SAINT
    - Tanium Comply
    - Tenable Security Center & tenable.io
- Web Application Scanners
    - Accunetix
    - Arachni
    - Checkmarx
    - HCL AppScan
    - Fortify Security Center & Fortify WebInspect

  - Netsparker
  - Nikto
  - OWASP Zap
  - PortSwigger Burp Suite
  - Qualys Web Application Scanning
  - Veracode SAST, DAST
  - W3af
  - WhiteHat Security Sentinel Dynamic
- Asset Management Systems
  - Nmap
  - ServiceNow CMDB
  - Qualys Asset Management
- Ticketing Systems
  - BMC Remedy
  - Atlassian Jira
  - ServiceNow Incident, Service Request
- Compliance
  - Qualys
- Generic
  - Generic CSV input of any of these tools

4.2 Exceptions for Integration Requirement

There are no exceptions to this policy.

5 Definitions

5.1 Acronyms and Definitions

Asset – Any organization, sub-organization, or entity described in Section, including any departments or divisions not explicitly defined in the Maryland manual.

CSV – Comma-Separated Values file format, typically used in Microsoft Excel or by applications to share structured data.

DNS – Domain Name System – A protocol that used to translate between IP addresses and human-readable names.

IPv4 – A 32-bit Internet Protocol version 4 address, typically provided with a CIDR based mask.

IPv6 – A 128-bit Internet Protocol version 6 address, typically provided with a CIDR based mask.

Unit – Any organization, sub-organization, or entity described in Section, including any departments or divisions not explicitly defined in the Maryland manual.

5.2 RFC 2119 Definitions

MUST - This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

MUST NOT - This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

SHOULD - This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT - This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behavior described with this label.

MAY - This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein, an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

Appendix A – File Formats

Table 1 – IP Address Reporting

Unit	Sub-unit (if applicable)	IPv4 or IPv6	Network Address	Network Mask	Network connections (AWS/Cloud/3rd party/networkMaryland/Other)	Description

Table 2 – DNS Reporting

Agency/Unit	Sub-unit (if applicable)	DNS Name	Description