NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer

P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212

www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 184-01 Information Security Vulnerability Management Procedure and Standard	**POLICY NO:** 12-04-P1-S1-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 09/10/2012
	VERSION: 2.1	**LAST REVIEWED:** 12/11/2014

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this circular is to define the necessary requirements and specifications to apply to the Executive Branch of State Government's information assets in compliance with 12-04-NJOIT, - *184 -Information Security Vulnerability Management Policy*.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This policy defines New Jersey Office of Information Technology's (NJOIT) role with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

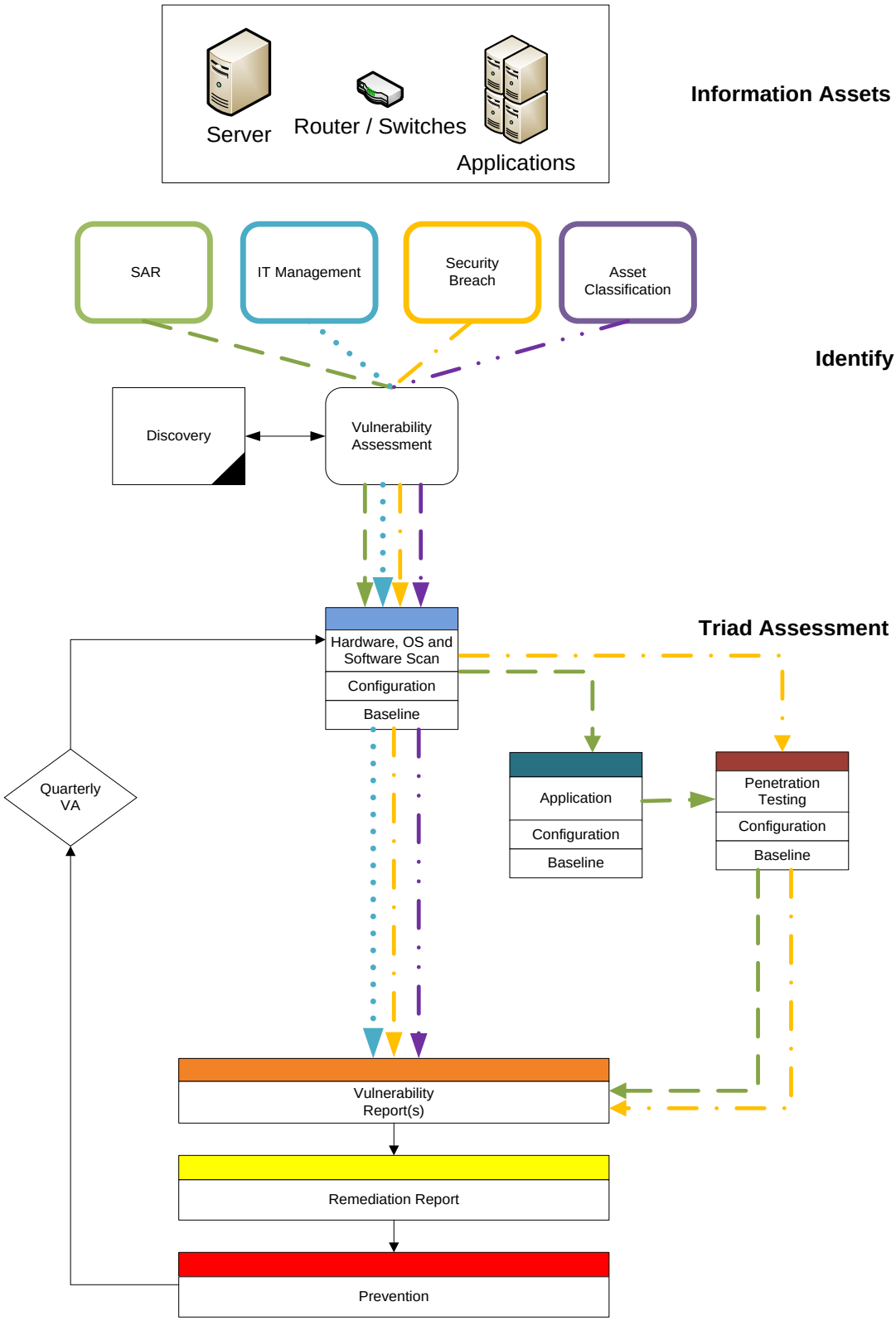
3 SCOPE

This circular applies to employees, contractors and others, who develop, administer and maintain information systems, networks, software applications, and resources for New Jersey State Government enterprise environment, the Office of Information Technology and their clients.

4 STANDARD/PROCEDURE

The Statewide Office of Information Security has made available a set of Information Security Vulnerability Assessment tools to departments and agencies to reduce the risk of threats or attacks to the State's Information Assets. Departments and agencies are

required to work with OIT to leverage these tools to ensure that the Information Security Vulnerability Management Program is effective.



Department and agencies may also use comparable Information Security Vulnerability Management products in conjunction with, but not in place of the provided enterprise tool set. No additional scanning products will be approved for new purchases.

A Systems Architecture Review (SAR) would trigger the Triad Assessment. All four-identity methods could trigger the Triad Assessment, depending on the event and asset type.

A vulnerability assessment can occur when:

- A Department or agency presents a new project, enhancement, application, or information asset during an OIT (SAR).
- Requested by OIT management, department or agency management and/or the OIT Statewide Office of Information Security to determine if new vulnerabilities and/or weak or insecure coding practices have been identified.
- The Information asset has had a security breach or compromise.
- A department or agency adds or changes an Information asset in their asset classification report.

The Vulnerability Assessment Program will identify, remediate, and prevent additional vulnerabilities. The program uses the following set of assessment tools:

- Discovery Scan
- Triad Assessment
- Vulnerability Report
- Risk Remediation Report
- Prevention

4.1 Discovery Scan

In order to identify Information assets, a department or agency can conduct a discovery scan. There are two methods for creating a discovery scan. The first method involves using the default Asset Discovery Scan template provided as part of the information security management toolset. The second method involves modifying the default Asset Discovery Scan template to meet specific needs of the department or agency.

Either method requires IP address information and the selection of network protocols and services for discovery such as ICMP, UDP, or TCP. Selecting the advanced host discovery option will provide host name resolution and Operating System (OS) identification. Unlike the vulnerability scan, asset discovery scans are not constructed to utilize, nor rely upon, vulnerability checking against the information asset.

Upon completion of a discovery scan of an information asset, hardware, operating system and software, you can then proceed to the triad assessment.

4.2 Triad Assessment

The triad assessment consists of three independent vulnerability assessments.

- Hardware, Operating System and Software
- Application
- Penetration Test

4.2.1 Hardware, Operating System and Software

The hardware, operating system and software scan will identify the operating system, software and services running on the physical asset. This scan will identify and report on known vulnerabilities.

All departments and agencies are required to have training on the use of the information security vulnerability assessment and remediation tools. If additional access is required for IP ranges, subnets, licenses, and/or user accounts on the information security vulnerability assessment tools, a written request for such access should be made at least one week prior to conducting any scans and assessment.

The scanning process covers five events:

- Scan Configuration
- Baseline Vulnerability Assessment
- Scheduling of Vulnerability Assessment Scans
- Monthly Vulnerability Assessment
- Cross Agency Assessment

4.2.1.1 Scan Configuration

4.2.1.1.1 Unlike information asset discovery scans, vulnerability scans require defined configurations constructed to include vulnerability checking. The Statewide Office of Information Security shall ensure the availability of at least one custom, multi-platform vulnerability scan template, with the minimum-security configuration.

4.2.1.1.2 Templates are available to assist departments and agencies to meet their mandated compliance and/or information technology requirements (e.g. HIPAA, PCI, SOX, and PII). At a minimum, departments and agencies should include the predefined regulatory templates as part of their tool set in order to meet regulatory compliance for any Information Asset that has a regulatory classification.

4.2.1.1.3 Departments and agencies can perform a regulatory compliance or a custom IT requirement scan independently by following the procedures used for conducting baseline scans with the exception of scheduling.

4.2.1.2 Baseline Vulnerability Assessment

Departments and agencies are responsible for scheduling and performing baseline vulnerability assessment scans of their assigned information assets at a minimum once a year. The purpose of the baseline scan is to determine the overall security health of a department or agency's assigned Information assets. This will also establish informational reports on vulnerabilities for use in planning, budgeting, and staffing needs as it relates to remediation.

Procedure for conducting a baseline scan:

4.2.1.2.1 A department or agency can use the results of a discovery scan or asset classification report to identify their assigned information assets and schedule the scan for the baseline vulnerability assessment.

4.2.1.2.2 Baseline scanning will occur at such time to minimize the impact on time-sensitive system functions (i.e. tax filing season).

4.2.1.2.3 Advance planning is required for baseline scanning to ensure necessary licenses are available.

4.2.1.2.4 Prior to conducting any scan, notify IT management and any affected staff along with the Statewide Office of Information Security to minimize any disruption to an active Information Asset.

4.2.1.2.5 Follow change control processes.

4.2.1.3 Scheduling Vulnerability Assessment Scans

4.2.1.3.1 New Information Assets require departments and agencies to conduct full intrusive vulnerability scans on all new and/or replacement equipment connecting to any State network during installation. A scan of the new Information Assets will occur independently at the Agency, but must follow the procedures used for conducting baseline scans.

4.2.1.3.2 Ad hoc scanning addresses perceived problems such as the existence of unapproved systems, devices or malware. Additional scans may be conducted to address configuration changes or for assessing classified and non-classified information assets. An ad-hoc scan or the usage of temporary licenses will follow the above procedure listed above for conducting new equipment scans.

4.2.1.4 Monthly Vulnerability Assessment

4.2.1.4.1 Departments and agencies are required to conduct vulnerability assessments every month on Internet public accessible Information assets. The purpose of the monthly scans is to measure a department or agency's success in reporting and remediating vulnerabilities.

4.2.1.5 Cross Agency Assessments

4.2.1.5.1 Department or agency vulnerability assessments are limited to the local agency networks and/or subnets.

4.2.1.5.2 The Statewide Office of Information Security will coordinate the following vulnerability scans:

4.2.1.5.2.1 Any vulnerability scans outside of a department or agency's jurisdiction or local network.

4.2.1.5.2.2 Any scans conducted on information assets hosting multiple department or agency applications.

4.2.2 Application

The application scan will identify and report on known software code vulnerabilities.

- Scan Configuration (the scanning process covers three events)
- Baseline Vulnerability Assessment
- Application Modification

4.2.2.1 Scan Configuration

An application scan requires a defined configuration. OIT Statewide Office of Information Security will work with the department or agency to define the configuration and schedule the scan. The department or agency will provide Statewide Office of Information Security the URL and credentials to perform an effective scan.

4.2.2.2 Baseline Vulnerability Assessment

Procedure for conducting a baseline scan:

4.2.2.2.1 Baseline scanning is to be conducted at such times as to minimize the impact on time-sensitive system functions (i.e. tax filing season).

4.2.2.2.2 Prior to conducting any scan, the Statewide Office of Information Security will notify the department or agency to minimize any disruption to an active information asset.

4.2.2.2.3 The Statewide Office of Information Security will follow the OIT change control processes.

4.2.2.3 Application Modification

Departments and agencies must contact the Statewide Office of Information Security to schedule an application scan when a software application is enhanced, upgraded or modified prior to any deployment to production.

4.2.3 Penetration Test

The penetration test scan will evaluate the security controls of an information asset by simulating an attack.

The scanning process covers three events:

- Scan Configuration
- Baseline Vulnerability Assessment
- Application Modification

4.2.3.1 Scan Configuration

A penetration test scan requires a defined configuration. The Statewide Office of Information Security will work with the department or agency to define the configuration and schedule the scan. The department or agency will provide Statewide Office of Information Security the URL to perform an effective scan.

4.2.3.2 Baseline Vulnerability Assessment

Procedure for conducting a baseline scan:

- Baseline scanning will be conducted at such times to minimize the impact on time-sensitive system functions (i.e. tax filing season).
- Prior to conducting any scan, the Statewide Office of Information Security will notify the department or agency to minimize any disruption to an active information asset.
- The Statewide Office of Information Security will follow the OIT change control processes.

4.2.3.3 Application Modification

Departments and agencies will contact the Statewide Office of Information Security to schedule a penetration scan when a software application is enhanced, upgraded or modified prior to any deployment to production.

4.3 Vulnerability Report

The vulnerability scans will produce reports indicating the vulnerabilities' severity levels. The severity levels will allow departments and agencies to prioritize remediation efforts and take the necessary steps to protect the integrity of the information asset. The Statewide Office of Information Security will establish and oversee overall vulnerability severity levels and risk scores attributed to vulnerability scans.

The severity level of 'Low' or the equivalent is acceptable for all vulnerability scans.

4.4 Remediation Report

Each scan will produce a vulnerability report. Departments and agencies are responsible for conducting a review of the vulnerabilities and formulating strategies for remediation. The reviews should involve the agency IT Leader, department or agency technical staff and if necessary, the affinity Deputy CTO, and the Statewide Information Security Officer when applicable. The goal is to complete the review, establish a remediation plan, and execute the plan within a 90-day Vulnerability Mitigation Cycle. Departments and agencies will use the Risk Management Remediation Report (Appendix A) to document and plan for the remediation. Departments and agencies are required to submit the Risk Management Remediation Report to the Statewide Office of Information Security for review.

A department or agency IT Leader or the Statewide Information Security Officer may request an update on the status of the remediation plan.

The remediation report identifies the risk, rating of the risk, mitigation and prioritization according to the severity level.

The severity of the vulnerability may require a more immediate mitigation action.

4.5 Prevention

Mitigation could include software patching and testing, rescanning (where necessary), and reporting in order to address reported vulnerabilities. The mitigation cycle will commence upon development of the remediation plan and shall not require longer than, nor exceed 90 consecutive calendar days to complete.

Patch Management Program – as part of the effort to keep vulnerabilities to a minimum and reduce exploitable weaknesses for information assets, departments and agencies must adopt a patch management process consisting of:

4.5.1 Formalizing a Software Patch Management methodology that includes best practices and/or industry standards such as prioritizing patch deployment, planning and testing (where necessary) for applying patches and timely deployment of new patches, using a phased approach as appropriate.

4.5.2 A notification process and/or service for new patch availability according to a department or agency's specific environment, systems or vendor specific firmware versions or levels.

4.5.3 Implementing a local process with the ability to obtain and store patch information within a centralized system.

5 EXCEPTIONS AND NON-COMPLIANCE

An exception request must be filed for any high or medium vulnerability that has not been remediated at the end of the 90-day Vulnerability Mitigation Cycle. An Exception Request Form or Risk Management Remediation Report is acceptable.

A compliance exception must be requested if there is an inability to comply with any portion of this policy. Exceptions and non-compliance shall be managed in accordance with Enterprise Policy 08-02-NJOIT, *111 - Information Security Managing Exceptions.*