NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	**No:** NYS-S15-002
IT Standard: **Vulnerability Management**	**Updated:** 05/04/2021
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

New York State (NYS) utilizes automated tools to scan systems, computing and network devices, web applications, and application code. The results of these scans help inform management and system administrators of known and potential vulnerabilities.

Vulnerability scanning is a process by which vulnerabilities are identified. Vulnerability management is a process by which the vulnerabilities identified through scanning are tracked, evaluated, prioritized, and managed until the vulnerabilities are remediated or otherwise appropriately resolved. Managing the remediation of vulnerabilities identified during scans ensures that appropriate actions are taken to reduce the potential that these vulnerabilities are exploited and thereby reduce risk of compromise to the confidentiality, integrity, and availability of NYS information assets.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117*, established January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

3.0 Scope

This standard applies to all "State Entities" (SE), defined as "State Government" entities as defined in Executive Order 117, established January 2002, or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any IT resource for which the SE has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. While an SE may adopt a different standard, it must include the requirements set forth in this one.

This standard applies to all systems, web applications, and application source code developed, maintained, or operated by, or on behalf of, all SEs.

4.0 Information Statement

As per the NYS-P03-002 Information Security Policy, all systems must be scanned for vulnerabilities. In addition, each system must be inventoried and have an individual or group assigned responsibility for maintenance and administration.

4.1 Types of Scans

The type of vulnerability scan appropriate for a given asset depends on the asset type (i.e., hardware, software, source code) and the asset's location (i.e., internal or external to the SE's network). The table below lists the types of vulnerability scans required by this standard.

Type	Description
External Infrastructure Scan	Scans of the perimeter of SE networks or any externally available hosted infrastructure to identify potential vulnerabilities in Internet accessible IT infrastructure.
Internal Infrastructure Scan	Scans of IT infrastructure on SE protected networks or any hosted infrastructure to identify potential vulnerabilities.
Unauthenticated Web Application Scan	Unauthenticated scans of SE externally facing production web applications identify security vulnerabilities that can be found without authenticated credentials.
Authenticated Web Application Scan	Authenticated scans of SE web applications identify security vulnerabilities for each level of access available within the web application.
Application Source Code Analysis	Scans of application source code run during development, or when necessary for change control, to identify problems in the code that could cause potential vulnerabilities.

4.2 Scanning

SEs are responsible for confirming that vulnerability scans are conducted and successfully completed. SEs must use a scanning tool approved by the SE ISO/designated security representative. Approved scanning tools must be able to provide remediation suggestions and be able to associate a severity value to each vulnerability discovered based on the relative impact of the vulnerability to the affected system.

As per the NYS-S14-002 Information Classification Standard, scan reports are classified with a minimum of moderate confidentiality and moderate integrity and should be protected as such.

SEs are required to provide all external IP addresses and Uniform Resource Locators (URLs) for all externally facing web applications to the SE ISO/designated security representatives and the Chief Information Security Office.

Network and system administrators must provide sufficient access to allow the vulnerability scanning tool to scan all services provided by the system. No devices connected to the network shall be specifically configured to block vulnerability scans from authorized scanning tool.

Scans must be performed within the system development life cycle (see NYS-S13-001 SSDLC Standard) while in pre-production environments, when deployed to the production environment, and periodically thereafter as specified below:

a. Pre-production scans occur prior to the move of the system, source code, or web application to the production environment:

   1. All systems must undergo an authenticated internal infrastructure scan, where technically feasible, before being deployed to the production environment. Any infrastructure vulnerability discovered must be remediated determined to be a false positive, or deemed an insignificant risk, by the SEISO/designated security representative, prior to the system being deployed for intended use.

   2. When source code is available, scan of the source code should be conducted throughout the development process. Applications must undergo source code scanning before the application moves to production and between environments if there has been a change to application code.

   3. Web applications that require authentication must undergo an authenticated scan before being deployed to the production environment or into an environment that is externally accessible. When authentication is required to access the application, scans must be run with authenticated access at each access level (e.g., user, admin) supported by the application, except where limitations in the scanning tool and/or application prevent authenticated scanning, in order to determine if vulnerabilities exist in the different functionality of the applications accessible by each access level Any web application vulnerability discovered must be remediated or determined to be a false positive

or insignificant risk by the SE ISO/designated security representative, prior to the web application being placed into the production environment.

4. Any system, source code, or application deployed to its production environment with un-remediated vulnerabilities must have a formal remediation plan and the documented approval of the SE executive responsible for risk management or their designee.

b. Implementation scans occur the first time a system or web application is moved to its production environment:

1. Systems must be scanned immediately upon being placed into the production environment with an authenticated internal infrastructure scan, where technically feasible. If the system is accessible from the internet or an external network, then the system must be scanned with an external infrastructure scan.

2. Web applications must be scanned within the first month of being placed into the production environment. An authenticated web application scan is required if feasible, but at minimum an unauthenticated web application scan is required. Sensitivity and criticality of the application must be considered when determining the schedule for the initial implementation scan.

c. Recurring Scans: After the initial scan in the production environment, the frequency of scans must occur according to the system or application's risk rating (see Table 2).

1. When performing internal infrastructure scans on systems built using a shared image, such as workstations, scans may be run on a sampling of systems, but the sample set must vary from scan to scan.

2. Web applications in production are required to undergo recurring scans. At minimum, web applications in production are required to undergo recurring unauthenticated application scans.

3. All vulnerabilities found during scans must be addressed as per the remediation section below.

4.3 Determine Risk Rating and Frequency of Scans

The risk that vulnerabilities pose to systems and applications is based on the likelihood of a vulnerability being exploited and the impact if the confidentiality, integrity, or availability of the SE's information assets were compromised. The likelihood of a vulnerability being exploited increases in direct relation to the system's or application's accessibility from other systems.

The impact of a vulnerability to a SE's information asset is based on that asset's information classification (see NYS-S14-002 Information Classification Standard). The SE must consider the impact (i.e., high, moderate, or low) of a compromise to the confidentiality, integrity, and availability of that asset. The highest impact level identified must be used when determining the overall risk rating, per the table below.

Table 2: RISK RATING			
Impact **(Confidentiality, Integrity, Availability)**	**Exposure**		
	Systems with no network connectivity to production data	**Systems with network connectivity to production data (not internet facing)**	**System that is publicly available from the internet**
High	**Moderate**	**High**	**High**
Moderate	**Low**	**Moderate**	**High**
Low	**Low**	**Low**	**High**

Minimum frequency of scans is dependent on the risk rating. All systems that are publicly available from the internet are considered High risk regardless of their impact rating because they represent a potential entryway to an SE's internal network. Systems without a risk rating must be scanned as if they had a risk rating of "High" until they are rated.

TABLE 3: FREQUENCY OF SCANS	
Risk Rating	**Frequency**
Infrastructure scans	
High	Monthly
Moderate	Quarterly
Low	Semi-annually
Web Application Scans	
High	Monthly or after significant change
Moderate	Quarterly

Low	Semi-Annually

4.4 Remediation

Vulnerabilities discovered during scans must be remediated based on risk rating (see Table 2) and vulnerability severity identified by the scanning tool as per the table below.

	TABLE 4: REMEDIATION TIMEFRAMES			
Risk Rating (from Table 2)	**Vulnerability Severity**			
	Critical	**High**	**Moderate**	**Low**
High	Resolved in 15 calendar days	Resolved in 30 calendar days	Resolved in 3 months	At the discretion of the SE ISO/designated security representative
Moderate	Resolved in 30 calendar days	Resolved in 3 months	Resolved in 6 months	At the discretion of the SE ISO/designated security representative
Low	Resolved in 4 months	Resolved in 6 months	At the discretion of the SE ISO/designated security representative	At the discretion of the SE ISO/designated security representative

Individuals performing vulnerability scans are required to notify the SE ISO/designated security representative within 1 business day of scan completion of new vulnerabilities discovered and at least monthly of un-remediated vulnerabilities on systems or applications that are running in production. Validation testing must be done to verify the remediation was successful.

SE ISOs/designated security representatives must notify SE management of any un-remediated vulnerabilities not addressed in the timeframes prescribed in this standard, so that risk is communicated to the appropriate parties, which should include ITS when the vulnerability directly or indirectly impacts the ITS-managed state network or data center, and risk review can be initiated.

5.0 Compliance

This standard shall take effect upon publication. Compliance is required with all ITS policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities shall request an exception through the Chief Information Security Office exception process.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

Term	Definition
Authenticated scan	A credential-based scan that provides sufficient access to allow the vulnerability scanning tool to scan the operating system and all applications running on the system.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-S15-002
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12242
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
01/16/2015	Original Standard Issued	Deborah A. Snyder, Deputy Chief Information Security Officer

03/10/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
05/04/2021	Updated remediation timelines, Scope and Authority, and minor wording changes	Karen Sorady, Chief Information Security Officer
05/19/2021	Updated Scope language	Karen Sorady, Chief Information Security Officer

9.0 Related Documents

NYS-S15-001 Patch Management Standard

NYS-S14-002 Information Classification Standard

US Department of Homeland Security Binding Operational Directive 19-002