



# Office of Information Technology Services

State Capitol P.O. Box 2062  
Albany, NY 12220-0062  
[www.its.ny.gov](http://www.its.ny.gov)

<b>New York State Information Technology Standard</b>	<b>No:</b> NYS-S15-002
<b>IT Standard:</b>  <b>Vulnerability Scanning</b>	<b>Effective:</b> 01/16/2015
	<b>Issued By:</b> NYS ITS  <b>Standard Owner:</b> Enterprise Information Security Office

## 1.0 Purpose and Benefits of the Standard

---

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 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 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 Enterprise IT Policy/Standard Statement

---

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), 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 (IT) Policy, Standards and Guidelines.

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

### 3.0 Scope

---

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

### 4.0 Information Statement

---

As per the [NYS 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 target depends on the target type (i.e., hardware, software, source code) and the target's location (i.e., internal or external to the State Entity's (SE) network). The table below lists the types of vulnerability scans required by this standard.

Type	Description
<b>External Infrastructure Scan</b>	Scans of the perimeter of SE networks or any externally available hosted infrastructure to identify potential vulnerabilities in Internet accessible IT infrastructure.
<b>Internal Infrastructure Scan</b>	Scans of IT infrastructure on SE protected networks or any hosted infrastructure to identify potential vulnerabilities.
<b>"Lite" Web Application Scan</b>	Cursory unauthenticated scans of SE externally facing production web applications to identify security vulnerabilities.
<b>In-depth Web Application Scan</b>	In-depth scans of SE web applications to identify security vulnerabilities.
<b>Application Source Code Analysis</b>	Scans of application source code run during development to identify problems in the code that could cause potential vulnerabilities.

#### 4.2 Scanning

SEs are responsible for confirming that vulnerability scans are conducted. SEs must use a scanning tool approved by the SE ISO/designated security representative. Any approved scanning tool 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 Information Classification Standard](#), scan reports are classified with high confidentiality and high integrity and should be protected as such.

SEs are required to provide all external IP addresses and URLs for all externally facing web applications to the SE ISO/designated security representatives and the Enterprise Information Security Office.

Network and system administrators must provide sufficient access to allow the vulnerability scan engine 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 engines.

Scans must be performed within the system development life cycle (see [NYS SSDLC Standard](#)) while in pre-deployment environments, when deployed into the target implementation environment, and periodically thereafter as specified below:

**a. Pre-deployment scans** occur prior to the move of the system or web application to the target implementation environment:

1. All systems must undergo an authenticated internal infrastructure scan before being deployed to the target implementation environment. Any infrastructure vulnerability discovered must be remediated, or determined to be a false positive or insignificant risk, by the Information Security Officer (ISO)/designated security representative, prior to the system being deployed for intended use.
2. When source code is available, applications must undergo source code scanning before the application moves between environments if there has been a change to application code.
3. Web applications must undergo an in-depth web application scan before being deployed into the target implementation 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 tool prevent authenticated scanning. Any web application vulnerability discovered must be remediated, or determined to be a false positive or insignificant risk by the ISO/designated security representative, prior to the system being placed into the target implementation environment.
4. Any system or application deployed to its target implementation environment with un-remediated vulnerabilities must have a formal remediation plan and the documented approval of the SE executive responsible for risk management.

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

1. Systems must be scanned immediately upon being placed into the target implementation environment with an internal infrastructure scan. 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 target implementation environment. An in-depth web application

scan is required if feasible, but at minimum a “lite” 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 target implementation environment, the frequency of scans are to 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 in-depth recurring scans for each access level supported by the application to the extent feasible. At minimum, web applications in production are required to undergo recurring “lite” 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 is increased in direct relation to the system’s or application’s accessibility from other systems.

The impact to the SE’s information assets is based on the asset’s information classification (see [NYS Information Classification Standard](#)). Impact (i.e., high, moderate or low) if the confidentiality, integrity or availability is compromised must be considered and the highest individual impact rating for confidentiality, integrity or availability utilized within 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 publically available from the internet
High	Medium	High	High
Moderate	Low	Medium	High
Low	Low	Low	Medium

Minimum frequency of scans is dependent on the risk rating. 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
<b>Infrastructure scans</b>	
High	Monthly
Medium	Quarterly
Low	Semi-annually
<b>Web Application Scans</b>	
High	Quarterly or after significant change
Medium	Semi-annually
Low	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 <a href="#">Table 2</a> )	Vulnerability Severity		
	Low/Informational/Minimal	Medium or Above	Highest Severity Rating
<b>High</b>	At the discretion of the ISO/designated security representative	Action Plan in 1 Week, Resolved in 1 Month	Action Plan in 1 Day, Resolved in 1 Week
<b>Medium</b>	At the discretion of the ISO/designated security representative	Action Plan in 2 Weeks, Resolved in 6 Months	Action Plan in 1 Week, Resolved in 1 Month
<b>Low</b>	At the discretion of the ISO/designated security representative	At the discretion of the ISO/designated security representative	Action Plan in 2 Weeks, Resolved in 6 Months

The ISO/designated security representative may review vulnerabilities to adjust the severity rating if necessary. Testing must be done to verify that remediation has been completed.

Individuals managing vulnerability scans are required to notify the ISO/designated security representative within 1 business day of scan completion for new vulnerabilities and at least monthly of un-remediated vulnerabilities on systems or applications that are running in production.

ISOs/designated security representatives must notify SE management of any unremediated vulnerabilities not addressed in the timeframes prescribed in this standard, so that risk is accepted by the appropriate party.

## 5.0 Compliance

---

This standard shall take effect upon publication. The Policy Unit shall review the standard at least once every year to ensure relevancy. The Office may also assess agency compliance with this standard. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, SEs shall request an exception through the Enterprise Information Security Office [exception process](#).

## 6.0 Definitions of Key Terms

---

**Authenticated scan** – a credential based scan that provides sufficient access to allow the vulnerability scan engine to scan the operating system and all applications running on the system.

**Target Implementation Environment** – the deployment environment in which the new or modified system is installed or fielded for use by a defined set of users after system acceptance has been completed. This is often referred to as the “production” environment.

## 7.0 ITS Contact Information

---

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

**Standard Owner**  
**Attention: Enterprise Information Security Office**  
**New York State Office of Information Technology Services**  
**State Capitol, ESP, P.O. Box 2062**  
**Albany, NY 12220**  
**Telephone: (518) 242-5200**  
**Facsimile: (518) 322-4976**

Questions may also be directed to your ITS Customer Relations Manager at:  
[Customer.Relations@its.ny.gov](mailto:Customer.Relations@its.ny.gov)

The State of New York Enterprise IT Policies may be found at the following website:  
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

## 8.0 Review Schedule and Revision History

---

Date	Description of Change	Reviewer
01/16/2015	Original Standard Issued	Deborah A. Snyder, Deputy Chief Information Security Officer
01/16/2016	Scheduled Standard Review	

## 9.0 Related Documents

---

- [NYS Patch Management Standard](#)