

STATE OF ALABAMA

Information Technology Standard

STANDARD 675S1-00: VULNERABILITY SCANNING

Periodic vulnerability scanning, following a specific but flexible schedule, is part of the continual evaluation process of risk and vulnerability management. Vulnerability scanning is an information gathering process, the process of identifying all known vulnerabilities of computing systems on the network. Vulnerability scanning identifies specific weaknesses in the operating system or application software that can be used to compromise the information system.

OBJECTIVE:

Direct the performance of periodic information security vulnerability scanning for the purpose of ensuring the integrity, confidentiality, and availability of critical information and computing assets, determining areas of vulnerability, and initiating appropriate remediation.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) Special Publication 800-53: Recommended Security Controls for Federal Information Systems, and other best practices, State of Alabama vulnerability scanning processes shall comply with the following requirements.

VULNERABILITY SCANNING PROCESS

Preparation:

Organizations shall document vulnerability scanning procedures and ensure adequate scan coverage, both in terms of vulnerabilities checked and information system components scanned.

Organizations shall train selected personnel in the use and maintenance of vulnerability scanning tools, techniques, and procedures.

Schedule:

Using appropriate vulnerability scanning tools and techniques, organizations shall scan for vulnerabilities in information systems follow a specific schedule (see Table below) or when significant new vulnerabilities affecting the system are identified and reported.

Table: Scanning Schedule

Requirement	Schedule	What to Look for:
Specific vulnerabilities and remediation	Immediately upon identification	Identify assets requiring remediation; validate remediation
Policy Enforcement	Monthly on a rotational schedule or as directed	Specify in scanning procedures to identify individual requirements
Password Compliance	Monthly on a rotational schedule or as directed	Blank or "out of the box" passwords, default administrator and guest accounts.
Unauthorized and approved software installation	Monthly on a rotational schedule or as directed	Specify in scanning procedures to identify individual requirements
Patch Compliance	Monthly on a rotational schedule or as directed	Required patches, service packs, etc.
Wireless VPN RAS	Monthly	Unauthorized or mis-configured connectivity, configuration, poor security, non-compliance, policy enforcement, changed requirements, etc.
Enclave Assessment	Quarterly	Identify application, network, and operating system vulnerabilities, configuration errors, and unauthorized access points.
Infrastructure Systems and Devices	Quarterly	Configuration, poor security, non-compliance, policy enforcement, changed requirements, unauthorized devices and connections, etc.
Comprehensive Vulnerability Assessment	Semi-annually	100% asset inventory. Configuration, poor security, non-compliance, policy enforcement, etc.
Web Sites	Semi-annually	Configuration, poor security, non-compliance, policy enforcement, changed requirements, etc.

Vulnerability scanning schedule shall also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment or changes resulting from new technologies and policy changes.

Vulnerability scanning shall also be performed on all new systems and significantly modified existing systems. Vulnerability scanning should be completed as early as feasible in the system development lifecycle and must be completed prior to the application or system being placed on the State network.

Vulnerability scanning of custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, static code analysis, source code reviews, etc.).

Findings:

Vulnerability scan findings shall be reported to the State IT Planning and Standards Office and the CIO. Findings and recommendations will be provided back to the organization Director, Assistant Director, and/or IT Manager

Results of a vulnerability scan determine appropriate priorities and actions to be taken to secure the application/system. Development and implementation of remediation programs is the responsibility of the agency responsible for the system or application being scanned.

Withholding assessment information is detrimental to risk mitigation strategies. As such, the results of vulnerability scanning and assessments shall be freely shared with appropriate personnel throughout the organization.

Results from vulnerability scans should be considered at a minimum as sensitive information (Confidential if the scanned system is confidential) and protected in accordance with applicable State standards. Scan data shall contain no protected or personally identifiable information (PII).

AUTHORITY TO SCAN

The Information Services Division (ISD) of the Department of Finance may perform internal (inside the network perimeter) scans of applications, servers, and devices for all organizations supported by ISD.

State organizations who control their own network segment may be internally scanned by ISD (or other authorized organization) by agreement.

All State organizations are subject to external scans of their Internet accessible segments (IAS).

External scans shall not require the system owner to expose their system to additional risk; conversely however, system owners shall not implement measures to prevent authorized scanning activity. External scanning of IAS is only effective when the enclave protection strategies reflect normal operations. If enclave and systems owners block the individual source of an authorized organization's scanning activity then an inaccurate representation of that network's enclave protections may result, while scanning efforts originating from other unidentified or "unknown" networks remain unhindered (vulnerability scanning, when performed by unauthorized individuals, is considered a prelude to attack). If the system owner and the scanning organization cannot reach a compromise on the scanning methodology, then it shall be resolved by the CIO.

ADDITIONAL INFORMATION:

Information Technology Policy 675: Vulnerability Management

http://cybersecurity.alabama.gov/documents/Policy_675_Vulnerability_Management.pdf

Information Technology Dictionary

http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
670-01S3	12/12/2006	Original document
675S1-00	09/01/2011	New number and format