STATE OF ALABAMA

Information Technology Policy

POLICY 672-00: VULNERABILITY SCANNING

Vulnerability scanning is an information gathering process, the process of identifying weaknesses in information system components that could be used to compromise the system. Vulnerability scanning includes, for example, scanning for patch levels, scanning for functions, ports, protocols, and services that should not be accessible to users or devices, and scanning for improperly configured or incorrectly operating information flow control mechanisms. Periodic vulnerability scanning, following a specific but flexible schedule, is part of the continual evaluation process of risk and vulnerability management

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:

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

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

Organizations shall scan for vulnerabilities in information systems and Web/Internet-accessible applications following a defined schedule and/or periodically in accordance with organization-defined procedures and when new vulnerabilities potentially affecting systems/applications are identified and reported.

Employ vulnerability scanning tools, techniques, and standards that automate parts of the vulnerability management process and promote interoperability. Consider using tools that:

- Automatically update their information system vulnerability database
- Express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention
- Use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities
- Express vulnerability impact using the Common Vulnerability Scoring System (CVSS)

The Open Web Application Security Project (OWASP) provides a list of vulnerability scanning tools at https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools.

Train selected personnel in the use and maintenance of vulnerability scanning tools, techniques, and procedures.

Document vulnerability scanning procedures.

Analyze vulnerability scan reports and determine appropriate priorities and actions to be taken to secure the system/application in accordance with an organizational assessment of risk.

Withholding vulnerability information can be detrimental to risk mitigation strategies. As such, the results of vulnerability scanning and assessments should be shared with security personnel (both within and external to the organization as appropriate) to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Information Services Division (ISD):

ISD shall vulnerability-scan:

- Any systems using IP address space assigned to ISD by an Internet Service Provider for which ISD is responsible
- Any systems (regardless of IP address space used) which provide functions related to an official presence and/or recognized as official systems of an agency of the Alabama State Government

Third-Party Non-State Entities:

Third-party (e.g. contracted service provider) may scan systems/applications to independently verify the results of a prior scan or to perform periodic independent compliance checks.

External entities may scan State systems only when all of the following conditions are met:

- When requested and authorized by ISD or by the owning/hosting State organization
- When covered by appropriate written agreement (contract, non-disclosure agreement, etc)
- When scheduled in advance, in sufficient time to affect required notifications
- When the source of the scanning activity is made known in advance to ISD Security personnel and/or the appropriate monitoring authority

Scanning activities not meeting all of the above conditions shall be treated as an attack (or precursor to an attack) and handled accordingly.

ADDITIONAL REQUIREMENTS:

Network/Application Safeguards:

Some network safeguards, such as intrusion prevention systems, will prevent scanning activity. These safeguards may need to be temporarily disabled to enable scanning. Scan the application twice, once with safeguards in place and once with safeguards disabled and compare the results to validate network and system protection mechanisms. Ensure safeguards are re-enabled when scan activity is complete.

Some applications may require log-in credentials in order to access program functionality. Conduct multiple scans of such applications using valid log-in credentials, invalid credentials, and anonymous access. Compare the results to (partially) validate authentication mechanisms (this technique is not as thorough as penetration testing). Ensure log-in accounts used for scanning are disabled when no longer required.

Vulnerability analyses of custom software applications may require additional approaches such as static analysis (such as source code reviews), dynamic analysis (such as code coverage tests), binary analysis, or a hybrid approach.

Scanning Schedule:

Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans; however, scanning must be conducted throughout the system lifecycle.

Application Development personnel shall ensure that systems/applications in development are vulnerability-scanned prior to placing them into production in accordance with a defined software development lifecycle.

Security personnel shall scan production systems/applications following a prescribed schedule (required minimum intervals shown in the table below) or randomly as deemed necessary or beneficial.

Whenever possible, scanning activities will be conducted in a staging or QA environment.

Table: Scanning Schedule

SCAN WHAT	WHEN	FOR
Remote Access Wireless VPN	Monthly	Unauthorized devices, unauthorized or mis-configured connectivity, configuration, poor security, non-compliance, default administrator and guest accounts, policy enforcement, changed requirements, etc.
Network Enclave	Quarterly	Application, network, and operating system vulnerabilities, configuration errors, unauthorized access points
Infrastructure Systems and Devices	Quarterly	Configuration, poor security, non-compliance, policy enforcement, required patches/service packs, changed requirements, unauthorized devices and connections, password compliance (blank or "out of the box" passwords), default administrator and guest accounts, etc.
Software	Semi-annually	Unauthorized software; patch compliance
Web Sites	Semi-annually	Configuration, poor security, non-compliance, policy enforcement, changed requirements, etc.
Applications Databases	Semi-annually	Known and common vulnerabilities, patch compliance, password compliance
Comprehensive Vulnerability Assessment	Semi-annually	Configuration, poor security, non-compliance, policy enforcement, etc. 100% asset inventory; ensure potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked.

Notifications:

Because scanning activities occasionally have unintended consequences, such as a temporary denial of service or other adverse effect, the scanning entity shall send a Notification of Scan e-mail to the appropriate monitoring authority prior to commencing a scan on a production system or application.

Findings:

If the results of vulnerability scanning indicate that the system poses a critical or high risk to other state systems or data, that system shall be isolated or taken off-line until the vulnerability is corrected.

Results from vulnerability scans should be considered sensitive information and protected in accordance with applicable State standards.

Retain scan data for no less than 2 years (for trending purposes).

SUPPORTING DOCUMENTS:

- Information Technology Policy 675: Vulnerability Management
- Information Technology Standard 681S1: Information Protection

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
670-01S3	12/12/2006	Original document
675S1-00	09/01/2011	New number and format
675S1-01	09/10/2012	Added information on scanning tools and modified schedule table
672-00	04/15/2013	Completely revised and reissued as a policy; replaces Standard 675S1.