State of New Mexico Statewide Architectural Configuration Requirements Title: Network Security Standard S-STD005.001 Effective Date: April 7, 2005

1. Authority

The Department of Information Technology (DoIT) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) including the adoption of statewide technical, coordination, and security standards per the Department of Information Technology Act, 9-27-1 et. seq. (1978).

2. Purpose

The purpose of this standard is to coordinate Agency and State efforts to provide a multi-layer protection strategy for secure and seamless interconnections of the State's heterogeneous systems and communications networks, including modems, routers, switches, and firewalls while protecting the State's computing resources and information from the risk of unauthorized access from external sources.

3. Scope

This applies to all Agencies. Agency is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches.

The Department Secretary, working in conjunction with the Department Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each agency.

4. Standard

The following network security standards provide the minimum requirements for providing secure and seamless interconnection of communications networks and systems while protecting the State's computing resources and information. Multi-layered protection shall be deployed at the Internet gateway, the network server, and the desktop levels to prevent introduction of malicious code or unauthorized access into the State's information systems.

4.1. NETWORK PERIMETER SECURITY**:** Firewall technology shall be employed at the edge of an agency's network including the Internet Gateway, to protect sensitive internal information assets and infrastructure from unauthorized access. External (inbound and outbound) traffic shall be routed through secure gateways, such as firewalls.

4.1.1. Any source routed packets or any packets with the IP options field set shall be blocked.

4.1.2 Inbound or outbound traffic containing source or destination addresses of 127.0.0.1 or 0.0.0.0, or directed broadcast addresses should be blocked.

4.1.3 Firewall technologies shall have security logging turned on. Logs should be reviewed, on a frequency determined and documented by the agency, by agency authorized personnel and all incidents, violations, etc. reported and resolved.

4.1.4 Firewall policies should be reviewed, tested, and audited, on a frequency determined and documented by the agency.

4.1.5 Remote management of firewall technologies should be via encrypted communications.

4.1.6 Unneeded services shall be turned off and unused ports disabled.

4.1.7 When required to allow converged services, such as voice (VoIP), instant messaging, presence, mobility services, multimedia (MoIP), etc., to securely traverse network borders and NAT functionality, firewall technologies shall use an approved, defined configuration in accordance with Firewall Standard N-STD-004.

4.1.8 Agencies may collectively establish joint power agreements (JPAs) or memorandums of understanding (MOUs) to implement and maintain a “trusted peer” relationship among multiple participants. Each participant in the agreement shall agree to conform to all applicable requirements set forth in the agreement to ensure sufficient and acceptable security protection for all other participating entities.

4.2. <u>END POINT SECURITY</u>**:** Client platform devices, including State-owned assets, client devices used by remote workers and telecommuters, as well as third-party entities, connected to the agency’s internal network should be protected from sending or receiving hostile threats from unauthorized network traffic or software applications.

4.2.1. Client platform devices shall utilize virus-scanning software in accordance with Virus and Malicious Code Standard S-STD-006.

4.2.2. Client platform devices externally connecting to agency internal networks shall encrypt all traffic in accordance with paragraph 4.6.

4.2.3. Individual firewalls deployed on client platform devices provide protection against network-borne threats by providing traditional firewall services blocking network traffic based on protocol, ports, and software applications, content filtering of packets, as well as controlling the behavior of software applications deployed and executed on the client platform device. Individual firewalls deployed on agency IT assets should be centrally administered and managed to ensure agency policy-based security is applied and updated.

4.3. <u>ACCESS TO INTERNETWORKING DEVICES AND SHARED PLATFORMS</u>**:** Internetworking devices (including routers, firewalls, switches, etc.) and shared platforms (including mainframes, servers, etc.) provide both access to equipment and information about networks. They shall be controlled to prevent unauthorized access.

4.4. PATCH MANAGEMENT: Agencies shall develop and implement written procedures that identify roles and responsibilities for implementing patch management that include the following activities:

4.4.1. Designated agency employees or contractors shall proactively monitor and address software vulnerabilities of all internetworking devices in their network (routers, firewalls, switches, etc.) by ensuring that applicable patches are acquired, tested, and installed in a timely manner. IT device manufacturers, security organizations, security vendors, and the Statewide Security Program Office (home of the Computer Security Incident Response Team, or CSIRT) provide various tools and services to assist in identifying vulnerabilities and respective patches.

4.4.2. Where practical and feasible, agencies shall test patches in a test environment prior to installing the patch. Testing exposes detrimental impacts to internal/external enterprise-wide application software systems, community-of-interest application software systems, and other third-party application software systems.

4.4.3. Agencies shall query the CSIRT prior to installing patches in production to determine if other State agencies have experienced problems during testing or post-installation. Agencies shall report testing and production problems discovered with patches to the CSIRT.

4.4.4. Patches shall be installed (use of an automated tool is recommended) on all affected internetworking devices. Designated employees or contractors shall monitor the status of patches once they are deployed.

4.4.5. Patches make changes to the configuration of an internetworking device designed to protect and secure internetworking devices and attached IT devices and systems from attack, and shall be controlled and documented in accordance with Statewide Standard Configuration Management S-STD-002.

4.5. DEMILITARIZED ZONE: Services provided through the Internet (Web-enabled applications, FTP, Mail, DNS, VoIP, etc.) shall be deployed on a Demilitarized Zone (DMZ) or proxies from the DMZ.

4.5.1. All communication from servers on the DMZ to internal applications and services shall be controlled.

4.5.2. Remote or dial-in access to networks shall be authenticated at the firewall, or through services placed on the DMZ.

4.5.3. The DMZ is the appropriate location for web servers, external DNS servers, Virtual Private Networks (VPNs), and dial-in servers.

4.5.4. Agency external DNS servers should neither be primary servers nor permit zone transfers to DNS servers outside of the agency.

4.5.5. All remote access users shall be considered external and therefore should be subjected to the firewall rule set. VPNs should terminate on the external segment or outside of the firewall.

4.5.6. Devices with multiple interfaces that reside in the DMZ shall conform to all State Security Architecture Standards.

4.6. EXTERNAL CONNECTION TO NETWORKS: External connections are entities that have contractual obligations that require connection to state resources. Those organizations that do not conform to any and all state standards must be required to use an external connection. External connections to networks shall be routed through secure gateways (as required above) and protected by at least one of the following encryption methods, as appropriate:

4.6.1. Transport Layer Security (TLS) or Secure Socket Layer (SSL) shall be employed between a web server and browser to authenticate the web server and, optionally, the user's browser. Implementations of TLS and SSL shall allow for client authentication support using the services provided by Certificate Authorities.

4.6.2. Wireless Transaction Layer Security (WTLS) with strong authentication and encryption shall be used between a web server and the browser of a wireless mobile device, such as a cellular telephone, PDA, etc., to provide sufficient levels of security during data transmission. WTLS currently supports X.509, X9.68 and WTLS certificates.

4.6.3. IP Security (IPSec) shall be used to extend the IP communications protocol, providing end-to-end confidentiality for data packets traveling over the Internet. The appropriate mode of IPSec shall be used commensurate with the level of security required for the data being transmitted: sender authentication and integrity without confidentiality or sender authentication and integrity with confidentiality.

4.6.4. VPNs shall be used to connect two networks or trading partners that must communicate over insecure networks, such as the public Internet, by establishing a secure link, typically between firewalls, using a version of the IPSec security protocol. VPNs are recommended for use in remote access.

4.6.5. Remote Authentication Dial-In User Service (RADIUS) which is a client/server protocol and software that enables network access servers to communicate with a central server to authenticate remote users and authorize their access to the requested system or service, and strong authentication shall be used for dial-up modem systems.

4.6.6. Dial-up desktop workstation modems should be disabled and removed. Use hardware and inventory scanning tools to verify the presence and configuration of dial utilities and modems. Agencies using dial-up modem systems shall establish modem use policies which include:

- A complete, current list of all authorized personnel having modem access privileges.
- Automatic disconnection after a specified period of inactivity. Inactivity parameters shall be determined by the agency.
- The recommended use of security tokens.
- Immediate termination of modem access privileges upon employment transfer, re-assignment, or termination.

4.6.7. Strong authentication, such as challenge/response devices, one-time passwords, tokens, Kerberos, and smart cards, shall be used once permission to connect has been granted.

4.6.8. External connections shall be removed promptly when no longer required. Key network components shall be disabled or removed to prevent inadvertent reconnection.

4.7. INTER-NETWORK TRANSPORT SERVICES**:** Generally and commercially available transport services, commonly referred to as carrier services. Based on agency business requirements, these services should be configured and implemented to allow for automatic re-routing of communications when critical nodes or links fail, or fall- back to alternate transport services, including the provision of duplicate or alternate secure gateways and external exchanges or switching centers.

4.8 WIRELESS NETWORK ACCESS: Wireless Access will conform to Authentication and Directory Services Standard S-STD-001.

4.9. INTRUSION DETECTION/PREVENTION**:** Intrusion detection mechanisms or intrusion prevention tools should be incorporated into all servers connected to WANs and to all internetworking devices that serve as gateways between WAN network segments. Caution should be taken to stay abreast of emerging technologies.

4.9.1. When used, intrusion detection systems shall be installed both external and internal to firewall technology protecting the network to monitor, block, and report unauthorized activity. Logs should be reviewed by agency authorized personnel and all incidents, violations, etc., reported and resolved.

4.9.2. Intrusion detection mechanisms for servers shall include the use of software and review procedures that scan for unauthorized changes to files, including system files.

4.9.3. Software and review procedures shall examine network traffic for known, suspicious attack signatures or activities and look for network traffic indicative of devices that have been mis-configured.

4.9.4. Violations of set parameters shall trigger appropriate notification to security administrators or agency staff, allowing a response to be undertaken.

4.9.5. Intrusion prevention tools combine user-defined security parameters with the ability to learn how software applications and operating systems should perform in their normal states to generate an appropriate set of security policies. Violations of these security policies produced through network penetration and changes in the normal state result in recognition of an attack with corresponding adjustments to stop it.

4.9.6. Application Vulnerability Description Language (AVDL) is a security interoperability standard being proposed as an OASIS standard. AVDL creates a uniform way of describing application security vulnerabilities using XML. The XML-based technology will allow communication between products that find, block, fix, and report application security holes.

4.9.7. Intrusion prevention technologies reduce the number of false alarms by focusing on real-time behavior rather than using signature-matching technology to identify a potential network attack. Intrusion prevention technologies can also prevent “zero-day” attacks, which exploit previously unknown weaknesses, because they respond to a change in the normal state of operation.

4.10. VULNERABILITY SCANNING: Network and host vulnerability scanners should be used to test for the vulnerabilities of internal systems and of network perimeter defenses, as well as adherence to security policy and standards. Vulnerability scanners should be components of the State’s comprehensive network security solutions. Such components allow security administrators to measure security, manage risk, and eliminate vulnerabilities, providing a more secure network environment. Notification of vulnerability scans shall be in compliance with CSIRT protocol, standards, policies and procedures. Scanners should have the ability to do the following:

4.10.1. Map the network or inventorying systems and services on the agency’s network,
4.10.2. Identify security holes by confirming vulnerabilities
4.10.3. Provide effective analysis if vulnerability data using browsing techniques, and enforcing valid security policies when used during security device installation and certification.
4.10.4. Provide comprehensive reports and charts for effective decision making and improved security, and
4.10.5. Define and enforce valid security policies when used during security device installation and certification.

4.11. DESTRUCTION OF NETWORK DOCUMENTATION: Hardcopy and electronic documentation of network device configurations, network diagrams, etc., shall be destroyed, as appropriate, when superseded, or no longer needed.

5. Definitions

Refer to the N-DEF001.001 Glossary of Terms located on the DoIT website: http://www.doit.state.nm.us/standards.html

6. References

S-STD-004 Firewall Standard

7. Attachments

None

8. Version Control

S-STD-00.001

9. Revision History

Original 04/07/05
Format Updated 09/18/13