State of New Mexico Statewide Architectural Configuration Requirement Title: Wireless Access Point Hardware Standard NDT-STD008.001 Effective Date: October 18, 2005

1. Authority

The Department of Information Technology (DoIT) in coordination with the Information Technology Commission, 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 NMSA, 9-27-1 et. seq. (1978).

2. Purpose

This standard provides guidelines for the hardware procurement and secure deployment of wireless access points for “Hot Spot” Wi-Fi coverage and Point-to-Point LAN communications links covering IEEE specifications 802.11a, 802.11b, 802.11g and 802.11i.

3. Scope

This applies to all Executive Agencies and to any other Agency or Entity utilizing Executive Agency infrastructure.

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

This standard will apply to all State of New Mexico Executive Agencies looking to deploy wireless networking to the Desktop and in Point-to-Point 802.11 WAN links.

Wireless networking is the largest growth area of networking since its introduction in 1998. Many security concerns developed since the original specification of IEEE 802.11, 802.11b and the WEP or RC4 encryption standard. Since that time, many changes and enhancements have been introduced into the firmware and hardware of wireless devices that have allowed more secure implementations and backwards compatibility with legacy devices allowing compatibility with the newer specifications. Best Practices in wireless AP deployments have now emerged. This standard is not intended to limit but to standardize the use and architecture to allow for wireless and Point-to-Point implementations within the State of New Mexico’s network architecture.

Wireless networks can allow for discounted network deployments in leased, difficult installations for older buildings and temporary sites. They can allow network access in conference rooms and public meeting sites. Emergency repairs to WAN links are also available with Point-to-Point solutions.

4. Standard

Agencies implementing wireless technologies must maintain a centralized record of all wireless installations and their configurations. At a minimum, records must contain the following specifications; hardware, firmware, location, antenna type, contact information. For audit purposes, agencies must maintain all records on a regular basis and must be made available upon request.

Commercial Grade Wireless Access Points (APs) must have the following features and minimum characteristics for deployment into the State of New Mexico and its Executive Agencies infrastructures.

1) Modes of Operation. APs will be capable of operating in the following modes as defined herein:
   a. Personal Mode: For small-scale deployments of a WLAN for remote operations and offices where document sensitivity is low and there are less than 25 stations utilizing a single access point. This mode features a shared key authorization for association. Encryption options may be selectable between WPA, WPA2, Vendor specific and/or the AES encryption standards.
   b. Enterprise Mode: For larger enterprise deployments of WLANs at central offices and facilities. Document sensitivity is moderate to low. Enterprise mode allows for large scale deployments with multiple AP's and more than 25 stations. This mode features associations only after a successful EAP authorization under IEEE 802.1x. Encryption options may be selectable between WPA, WPA2, Vendor specific and/or the AES encryption standards.
   c. Point-to-Point: As the installation of an Ethernet link.

2) Access Points must include as the minimum features and characteristics support for the following:
   a. Multiple VLANs;
   b. On Board Hardware Encryption supporting AES;
   c. Internal Memory to allow for upgradeable firmware;
   d. The manufacture should provide a Plenum rated model for location options;
   e. Capable of a diversity of antennae options for multiple installation variables;
   f. A minimum of 80mw RF power;
   g. Output power selectable;
   h. Multiple channel selection;
   i. Be equipped for inline power per IEEE 802.3af;
   j. Manageable through SSH and HTTPS.

Security Guidelines – As WLAN products have evolved and specifications have matured, the latest security principles must be observed when implementing these networks. Due diligence indicates that wireless networks may include a more involved administrative burden than normal wired networks. It is assumed the state agency interested in implementing wireless LAN technologies will have implemented a strong security template for their traditional wired network before implementing wireless technologies. The security template should already include:

- In Place Access policies;

- Meets official State Password Policy;
- Password Rotation;
- Key Rotation Plan;
- VLAN implementation;
- Physical Security Plan;
- Scheduled Firmware Update Rotation Cycles for Network Devices;
- Penetration Testing.

In addition to the traditional security plan, implementation of security features of wireless devices must be strictly adhered to.

Which Wireless security features are implemented will depend on the mode of operation and in some cases where vendor specific features are used, the vendor of the equipment:

1) Personal Mode: Personal mode installations are suggested for remote and temporary sites where WLANs are the preferred connection method and Document sensitivity is low. Specific security options will include:
   a. Complex Key Strings with no repeating members;
   b. Regular Static Key Rotations;
   c. SSID will not be broadcast;
   d. Strong encryption will be enabled using:
      i. WPA
      ii. WPA-2
      iii. AES
      iv. Vendor Specific
   e. Physical location of the AP must be considered;
   f. Wireless VLANs are recommended.

2) Enterprise Mode: Enterprise mode installations are for larger enterprise deployments of WLANs at central offices and other facilities. Document sensitivity is moderate to low. Enterprise mode allows for large-scale deployments with multiple APs and more than 25 subscribers.
   a. Wireless segments will be implemented using VLANs.
   b. A client authentication server conforming to IEEE 802.1x using any appropriate form of EAP will be required for client authentication prior to association with the AP.
   c. Authentication of the subscriber through Active Directory and Kerberos is encouraged.
   d. Dynamic key rotation will be enabled via the 802.1x server.
   e. Guests may be allowed access to Internet only via the appropriate VLAN.
   f. Strong encryption will be enabled using:
      i. WPA
      ii. WPA-2
      iii. AES
      iv. Vendor Specific
   g. A wireless management suite is encouraged that promotes Rogue AP and intrusion detection.

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

None

7. Attachments

None

8. Version Control

N-STD-008.001

9. Revision History

Original 10/18/05
Format Updated 09/18/13