Idaho Technology Authority (ITA)

ENTERPRISE STANDARDS – S3000 NETWORK AND TELECOMMUNCATIONS

Category: S3530 – NETWORK CONNECTIVITY AND TRANSPORT – WIRELESS LAN

CONTENTS:

I. DEFINITION

A Wireless Local Area Network (WLAN) is a Local Area Network (LAN) or LAN segment that uses radio waves, instead of physical cables, to transfer data between networked devices.

II. RATIONALE

Idaho State government must be able to easily, reliably, and economically communicate data and information to conduct State business. Wireless communications are approved by ITA for use in State government local area networks. The standards recommended by the Institute of Electrical and Electronics Engineers (IEEE) are recognized as the primary standards for Wireless Local Area Networks and Federal Information Processing Standard (FIPS) validated cryptographic algorithms are the recognized standard for encryption of the signals.

III. APPROVED STANDARD(S)

Enterprise-level standard equipment which conforms to the following standards are approved:

1. IEEE 802.11g with 802.11i encryption standards; and

2. IEEE 802.11n (when ratified).

IV. APPROVED PRODUCT(S)

Standards-based products and architecture.

V. JUSTIFICATION

Products and wireless LAN implementations must conform to approved IEEE standards and ITA Standard 3510 – Network Connectivity and Transport - Local Area Network. Wireless networks enable wireless-capable computers and devices to connect more easily to networks or other computers; however, this ease of access creates security risks which must be mitigated through specific actions. This standard identifies the minimum technical and security requirements agencies must follow in order to ensure the confidentiality, integrity and availability of wireless communications information on the network as well as to help prevent unauthorized access to official and sensitive information which resides on the State Network.

VI. TECHNICAL AND SECURITY IMPLEMENTATION CONSIDERATION

The deployment of a WLAN is a complex task that requires skilled resources. The 802.11i product standard was added to later 802.11g products; however, only 802.11i capable systems should be used for new installations. No 802.11b equipment should be on the state network within the implementation time requirements. When the 802.11n standard is ratified, new installations of those products who meet that standard should be used for new installations.

Agencies must carefully consider the security implications of the deployment, administration, and operation of a Wireless LAN. IEEE 802.11i addresses the security flaws in the original IEEE 802.11 standard with built-in features providing robust wireless communications security, including support for Federal Information Processing Standard (FIPS) standards for encryption. If agencies maintain their use of older legacy IEEE 802.11g, they should follow the accepted security recommendations to compensate for the security weaknesses inherent in legacy WLANs. To assist with this process, agencies may refer to the ITA Wireless Local Area Network (LAN) Security Guideline (G530 – Wireless Local Area Network [LAN] Security) and the National institute of Standard and Technology (NIST) Special Publication SP 800-48 entitled Wireless Network Security, Revision 1, dated July 2008 (http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf).

The IEEE 802.11i standard is sometimes referred to as the Advanced Encryption Standard (AES) or Wireless Protected Access 2 (WPA 2) standard. It addressed security concerns within earlier 802.11 standards and adds the ability to use the Advanced Encryption Standard (AES) for encryption of data including support for Federal Information Processing Standard (FIPS) validated cryptographic algorithms. It is included in some wireless products shipped as 802.11g. To identify these products, look for AES or WPA2 in the technical specifications. Agencies implementing new WLAN's or requiring an increased level of security for their WLAN should consider using products containing IEEE 802.11i. Upgrading an existing wireless network to include IEEE

802.11i security elements, such as AES, may require upgrading all associated WLAN hardware.

VII. EMERGING TRENDS AND ARCHITECTURAL DIRECTIONS

The development of the 802.11n standard is particularly noteworthy, as 802.11n wireless networks will have significantly higher data throughput than existing wireless networks. Agencies planning to adopt 802.11n when it is finalized by IEEE should review their Local Area Network (LAN) backbone, as agencies using 100BaseT for their LAN backbone will not realize the speed benefits available with 802.11n technology. ITA will follow these developments and make updates to the state approved standards as appropriate.

VIII. PROCEDURE REFERENCE

Network Connectivity and Transport – Wireless LAN used on the State of Idaho's Wide Area Network must comply with the Department of Administration's "*P3020 – Connectivity and Transport Protocols* and *P4540 – Wireless Security for State Local Area Networks*"

IX. REVIEW CYCLE

Six (6) Months

X. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876.

XI. SECURITY SPECIFIC REQUIREMENTS

As required in ITA Policy, P4540 – Wireless Security for State Local Area Networks, the following are required for wireless LAN security.

1. Physical Access – All wireless devices shall be protected against theft, unauthorized use and damage. The following physical access requirements are essential for providing this protection:

   A. All network access points and related equipment such as base stations and cabling supporting wireless networks shall be secured with locking mechanisms or kept in an area where access is restricted to authorized personnel.

   B. The reset function on access points shall be accessible only to authorized personnel.

2. Network Access – Network access to State of Idaho information resources should be restricted only to those authorized. The following are required for securing wireless network access:

A. Access points shall be segmented from an internal, wired LAN using a gateway or similar device or control.

B. The service set identifier (SSID), administrator user ID, password and WEP key shall be changed from the default value. Also, the SSID shall be configured such that it does not contain any identifying information about the organization.

C. The SSID shall not contain characters that indicate the location of the wireless LAN access point or any other identifying name.

D. The SSID broadcast function shall be disabled, except where technology does not permit. In cases where the broadcast SSID function cannot be disabled, the network administrator shall notify the Office of the CIO Security Team.

E. A device shall not be connected to a wireless network unless it can provide the valid SSID.

F. Devices used to access the state's network over an IEEE 802.11 wireless connection shall have anti-virus software. Devices incapable of running anti-virus or firewall software such as radio frequency identification (RFID) tags, voice telephony systems, or some personal digital assistants are exempt from this requirement.

3. Administrative Access – only authorized agency system administrators will be allowed administrative access to the wireless access points and network systems.

A. All access points shall require a password to access the administrative features. This password shall be stored and transmitted in an encrypted format.

B. The ad-hoc mode for 802.11 communications (referred to as peer-to-peer mode or Independent Basic Service Set) shall be disabled by the network administrator. The ad-hoc mode shall be allowed only when an emergency, temporary network is required.

C. Every device used to access the state's network over a 802.11 wireless connection shall, when not in use for short periods of time, be locked (via operating system safeguard features) and shall be turned off when not in use for an extended period of time unless the design of the device is to provide or utilize continuous network connectivity. Such items might include wireless cameras, RFID tag readers and other portable wireless devices.

D. If supported, auditing features on wireless devices shall be enabled and resulting logs shall be reviewed periodically by designated staff and/or sent to the OCIO Security Team's Security Information and Event Management (SIEM) device.

E. All wireless access to the state's network via an 802.11 wireless network shall be authenticated using USERID and Password which meet the standards of the Idaho Consolidated Services Policy. Any employee's or other authorized user's account

will be disabled within 24 hours of notification of employee status change (such as agency change or dismissal), either automatically via Active Directory or LDAP disabling, or specifically deactivating the 802.1X credentials.

4. Encryption – All wireless networks which provide access to or through the state network shall be encrypted.

A. At a minimum, public information requires at least WPA encryption until 802.11i (WPA2) compliant AES encryption-capable or better equipment can be acquired and deployed. Portions of the network known to handle Privacy, HIPAA or other sensitive information require WPA2 encryption. All agencies must move to FIPS approved encryption algorithms, or WPA2/AES because of the increasing risk of sensitive data traversing any portion of the state network. Please note that only Counter Mode with Cipher Block Chaining MAC Protocol (CCMP) RSN, which is used by IEEE 802.11i, has a cryptographic algorithm that is FIPS-validated.

B. When using WPA2, AES encryption shall be enabled and shall be no less than 128-bits.

C. When using WPA, the highest level of encryption supported on the device shall be enabled.

D. WPA encryption must use the temporal key integrity protocol (TKIP) or other IEEE or NIST-approved key exchange mechanism.

E. WPA2 encryption must use Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) or other IEEE or NIST-approved key exchange mechanism.

F. WEP encryption in no longer considered secure because it has been cracked and it is not an approved standard for State of Idaho wireless security.

5. Wireless System Management - The following wireless system management requirements will be followed for wireless networks that provide access to or through the state network:

1. SNMP shall be disabled if not required for network management purposes.

2. If SNMP is required for network management purposes, SNMP will be read-only with appropriate access controls that prohibit wireless devices from requesting and retrieving information.

3. If SNMP is required for dynamic reconfiguration of access points to address AP failures and rogue access points, the SNMP protocol used shall adhere to SNMP Version 3 or better standards and only take place on the wired side of the network.

4. Pre-defined community strings such as “public” and “private” shall be removed.

5. The latest version of the SNMP protocol supported by both device and management stations shall be implemented and support for earlier versions of SNMP disabled.

6. IEEE 802.11 wireless devices shall not be used to manage other systems on the network except in temporary, ad-hoc emergency situations or by use of end-to-end encryption with authentication.

REVISION HISTORY

07/01/13 – Changed “ITRMC” to “ITA”.

6/5/12 – WEP encryption updated to WPA2.

6/16/09 – Added Procedure Reference, changed the layout and deleted Timeline.

2/25/09 – Removed 802.11b as a standard. Added encryption standards and reference to ITRMC Policy P4540. Added specific security requirements and reference to FIPS standards.

3/7/07 – Updated Emerging Trends and Architectural Directions to include information on 802.11n standard development. Removed reference to ‘Recent trends’ for 802.11g.

9/13/06 – Corrected minor typo in Section VII. Added information to Section VII to acknowledge other subsets of IEEE 802.11 in development.

4/25/05 – Added information about IEEE 802.11i.

8/25/04 – Added reference to ITRMC Guideline G530 (Wireless LAN Security) and revised emerging trends to acknowledge the future benefits and impact of 802.11i-based products.

Effective Date: April 24, 2002