DRAFT Standard Statement – Wireless Security

Title: Wireless Security

Document Number: SS-70-010

Effective Date: xx/xx/2011

Published by: Department of Information Systems

1. Purpose

Wireless technology gives users the ability to access data and applications from more locations in a cost effective manner, but wireless technology also presents problems in terms of security. All information assets handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. For these reasons, appropriate security measures are essential when deploying wireless technology with access to the state network. This standard addresses commonly used networking and end user technologies.

2. Scope

This standard statement applies to all state agencies, boards, commissions, and administrative sections of institutions of higher education.

3. Background

Arkansas Code Ann. Section 25-4-105(13) and (15)(Supp. 2007) gives the Department of Information Systems the authority to define standards, policies and specifications for state agencies and ensuring agencies' compliance with those policies, procedures and standards. In addition, the department develops information technology security policy for state agencies.

The State Security Working Group, made up of representatives of state agencies and higher education, wrote the Wireless Security Standard.

4. References

4.1 Arkansas Code Ann. Section 25-4-105(13) and (15) (Supp. 2007) authorized the Department of Information Systems to develop statewide information technology security policies

4.2 Encryption Standard (SS-70-006)

4.3 Remote Access Standard (SS-70-009)

4.4 Warning Banner Standard (SS-70-003)

4.5 Data and System Security Classification Standard (SS-70-001)

5. Standard

5.1 All configuration parameters (such as Service Set Identifier (SSID), keys, passwords, etc.) of Wi-Fi access points or bridges that can be changed from default manufacturer settings shall be changed from the default. Where applicable, the new security setting should be complex.

5.2 Open Wireless Networks on the state network

5.2.1 Entities shall not offer open wireless networks without requiring authentication through a secure method (such as the use of hotspot café type software or a captive web portal) to identify and authenticate users of the hotspot environment.

5.2.2 Warning banners shall be utilized to inform users of the acceptable use of the network and the possibility of monitoring

5.2.3 Entities offering open wireless networks shall contact the DIS network section to secure a private IP range to establish the network.

5.2.4 Service Set Identifier shall be changed to one which appropriately identifies the wireless network as a hotspot environment.

5.2.5 Appropriate audit logs containing IP address login id, and logon/logoff date and time stamps should be maintained based on the organization’s data retention policy.

5.2.6 Access control support (such as timeout and logout mechanisms) should be implemented.

5.3 Wireless Managed Networks may exist on the state network if and only if the following requirements are met:

5.3.1 An appropriate warning banner is presented to authorized and unauthorized users of the managed wireless environment in accordance to the SS-70-003 Warning Banner Standard. Wireless users must be given the opportunity to view any appropriate acceptable use policy as a part of authenticating via some mechanism such as a captive portal.

5.3.2 The Service Set Identifier is changed to one which appropriately identifies the wireless managed network.

5.3.3 Appropriate audit logs containing IP address, login id, and logon/logoff date and time stamps should be maintained based on the organization’s data retention policy.

5.3.4 Systems or applications which contain data which is classified by the SS-70-70-001 Data and System Security Classification Standard as being Level B – Sensitive, Level C – Very Sensitive or Level D – Extremely Sensitive must have appropriate access controls (firewall rules, router access control lists, and similar measures) that disallow wireless users from directly accessing the system or application. Users of a managed wireless environment which require access to these systems or applications must use appropriate technology such as encrypted VPN, SSL/TLS, encrypted web pages, or similar authenticated and encrypted technologies to access these resources. This is in accordance to SS-70-009 Remote Access Standard and the SS-70-006 Encryption Standard.

5.4 Covered entities which use wireless networking in a non-hotspot environment must adhere to the following.

5.4.1 The Service Set Identifier must not contain information relative to agency location, mission, or name, except for open wireless networks.

5.4.2 Wi-Fi equipment shall be configured for infrastructure mode only.

5.4.3 All wireless transmissions between a state network entity's managed wireless access point or bridge and clients shall be encrypted utilizing the WPA protocol at a minimum to prevent unauthorized access to the state network. WEP (wireless encryption protocol) shall NOT be utilized due to its multiple security flaws.

5.4.4 Wirelessly transmitted data and credentials granting access to state resources are subject to the SS-70-009 Remote Access Standard and the SS-70-006 Encryption Standard.

5.4.5 Covered entities will search for and disable rogue Wi-Fi access points to the state network at least quarterly.

5.4.6 Covered entities utilizing wireless technologies shall establish a policy to ensure compliance with the state wireless security standard.

5.5 Wireless networks (Including Bluetooth, Wi-Fi, etc.) that covered entities may use that are separate from the state network are not subject to this standard. Clients however must still adhere to the SS-70-009 Remote Access Standard and the SS-70-006 Encryption Standard when accessing Level B, C, or D data from these outside environments.

5.6 Bluetooth wireless devices must be secured to the extent configurable between the devices involved.

5.7 Use of Bluetooth devices for accessing network should follow the SS-70-009 Remote Access standard and the SS-70-006 Encryption standard.

6 Procedure

The State Cyber Security Office reserves the right to audit for compliance with this standard. Furthermore, the State Cyber Security Office has the right to grant an exception or exclusion to any part of this standard. The Arkansas Division of Legislative Audit also audits for compliance with this standard.

7 Revision History

Date	Description of Change
x/x/2010	Original Standard Statement Published

8 Glossary

8.1 Bluetooth A computing and telecommunications industry specification that describes how mobile phones, computers, and personal digital assistants (PDAs) can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection.

8.2 Hotspot A public or semi-public wireless local area network (WLAN) that provides Internet access to subscribers

8.3 Rogue Access Point Unauthorized wireless device allowing access to the state network

8.4 SSID (Service Set Identifier) A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN). This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.

8.5 State Network The state core information technology infrastructure serving Arkansas agencies, boards, commission, public schools, institutions of higher education, libraries, and other public organizations with Internet connectivity, data processing and transmission, video conferencing and telecommunications.

8.6 WEP (Wired Equivalent Privacy)– WEP is an optional privacy protocol originally specified in the IEEE 802.11 (802.11 legacy) standard that is designed to provide a level of security and privacy comparable to what is usually expected of a wired LAN. Weakness in the design makes this protocol unsuitable for use in environments which must protect sensitive data.

8.7 Wi-Fi A term used to describe the underlying technology of wireless local area networks (WLAN) based on the IEEE 802.11 set of specifications and is used interchangeably with the term wireless. Wi-Fi refers to any individual standard or the collection of all standards within the 802.11 family such as 802.11a, 802.11b/g, 802.11i, or 802.11n.

8.8 Wireless Wireless LAN (local area network) data access technology including the following protocols: 802.11 series and Bluetooth that accesses state information technology resources

8.9 WLAN (wireless local area network) A communication system that enables mobile users to connect to a wired network through a wireless (radio) connection, often implemented as an extension to wired LAN. WLAN'S are typically found within a small client node, dense locale (e.g. a campus or office building), or anywhere a traditional network cannot be deployed for logistical reasons.

8.10 WPA (Wi-Fi Protected Access) WPA is a security standard for users of computers equipped with Wi-Fi wireless connection. It is an improvement on and is expected to replace the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). WPA provides more sophisticated data encryption than WEP and also provides user authentication.

9. Related Resources

9.1 FCC Wireless website: http://wireless.fcc.gov/

9.2 SANS website: www.sans.org

9.3 Bluetooth website: www.bluetooth.com

9.4 Wi-Fi Alliance website: www.wifialliance.org

9.5 NIST website: http://www.nist.gov/index.html

9.6 Payment Card Industry:
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml