Technical Panel
of the
Nebraska Information Technology Commission

Draft Document
30-Day Comment Period

Title: Wireless Local Area Network Standard

Notes to Readers:

1. The following document is a draft standard under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is available in both PDF and Word versions at http://www.nitc.state.ne.us/standards/index.html.
2. If you have comments on this document, you can send them by e-mail to rick.becker@nitc.ne.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on May 22, 2006.
4. The Technical Panel will consider this standard and the comments received at their meeting currently scheduled for June 13, 2006. Final approval of the standard would be considered by NITC at their next meeting following the Technical Panel review. Information about these meetings will be posted on the NITC web site at http://www.nitc.state.ne.us/.
5. Comments may also be submitted on two related documents: Wireless Access Point Approval Process and Wireless LAN Security Checklist. These documents are posted at http://www.nitc.state.ne.us/standards/index.html.

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Wireless Local Area Network Standard

Category	**Security Architecture**
Title	**Wireless Local Area Network Standard**
Number	

Applicability

☑ **State Government Agencies**
- ☐ All.....**Not Applicable**
- ☑ Excluding higher education institutions..... **Standard**

☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document.....**Not Applicable**

☑ **Other:** All Public Entities.....**Guideline**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 4.1).
Guideline - Adherence is voluntary.

Status	☐ Adopted	☐ Draft	☑ Other: Reviewed
Dates	Date: March 17, 2006 (Draft Revisions) Date Adopted by NITC: September 30, 2003 Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

Executive Summary

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs.

In additional to the inherent risks associated with any wired network, wireless technology introduces several unique vulnerabilities. Since wireless signals are radio transmissions, they can be intercepted by suitable radio receiving devices, sometimes even devices operating outside the intended service area. If data transmissions are not encrypted or are inadequately encrypted, the intercepted data can be read and understood in a matter of seconds. Any data transmission sent through the wireless network is at risk, including correspondence, usernames and passwords, financial data, and other sensitive information. Because wireless transmissions circumvent traditional perimeter firewalls, those existing protections established to prevent unauthorized access are ineffective. Advances in wireless signaling technology may increase transmission distances, further exacerbating the problem of unauthorized reception. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

Also, since wireless network devices operate using radio signals, their proliferation within an area can lead to Radio Frequency Interference (RFI) among these devices and other radio devices using the same frequency bands.

The purpose of this standard is to ensure that only registered and secure WLANs are deployed by state government agencies. This standard provides the following:

1. State agencies must register WLANs, including each Access Point (AP) that connects to the state private network, with the Division of Communications (DOC). [Section 1.1]

2. State agencies must provide for proper management and security of WLANs. [Section 1.2]

3. Provides for resolution of conflicts between wireless devices. [Section 1.3]

4. Requires compliance with other network standards. [Section 1.4]

5. Provides a list of general recommendations for agencies implementing WLANs. [Section 1.5]

Source Notes: A source for portions of the original version of this document and the Division of Communication's Wireless Access Point Checklist was *Special Publication 800-48, "Wireless Network Security 800.11, Bluetooth and Handheld Devices,"* November 2002 published by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. A full copy of that publication is available at http://csrc.nist.gov/publications/nistpubs/index.html. NIST Special Publication 800-48 provides a detailed overview of wireless technology, wireless LANs, wireless personal area networks ("Bluetooth" technology), and wireless handheld devices. Anyone implementing any of these types of wireless systems should read the entire report. Parts of the document were also based on the National Institutes of Health, Wireless Network Policy.

1.0 Standard

This standard applies to state agencies which deploy a Wireless Local Area Network (WLAN).

Wireless services that fall within the definition of Campus Connection, Metropolitan Area Network (MAN), or Wide Area Network (WAN) must be purchased through DAS Information Technology Services (ITS) to comply with state statutes.

1.1 Registration of Wireless Devices

State agencies must register WLANs, including each Access Point (AP) that connects to the state private network, with the Division of Communications (DOC).

1.1.1 Registration

Self-registration is available through a DOC form on the ITS website (See Section 7.1). The registration process will identify: contact information; WLAN device information, including the manufacturer, model, and physical location; and the security/firewall technologies being deployed. Registration should occur prior to deployment.

1.1.2 Review and Approval

The DOC will contact the registering agency after reviewing the registration information.

1.1.3 Naming Convention

Final device names are assigned by the DOC during the registration process to avoid conflicts and confusion, and to aid in incident response and in identifying and locating wireless devices. If technology allows for the broadcast of a device name, standardized names should appear in the broadcast description, along with any unique identifiers assigned to the unit.

1.1.4 Unregistered (Rogue) and Unsecured Devices

Only approved WLANs and access points will be deployed within state agencies. Unregistered (rogue) devices will be removed from service.

Network managers for the DOC will incorporate procedures for scanning and detecting unregistered (rogue) wireless devices and access points. This requires a full understanding of the topology of the network. It also requires performing periodic security testing and assessment, including randomly timed security audits to monitor and track wireless and handheld devices. ITS reserves the right to disable network access for a device, server or LAN if adequate security is not in place.

1.2 Management and Security

1.2.1 Physical Security

Access points must be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices will not be placed in easily accessible public locations.

1.2.2 Configuration Management

All wireless access points must be secured using a strong password. Passwords will be changed at least every six months. Administrators must ensure all vendor default user

names and passwords are removed from the device. Administration of the device will be prohibited from the wireless network.

1.2.3 Authentication and Encryption

Authentication and encryption is required on all WLANs (see options listed on the registration form for details).

1.2.3.1 Access to Systems and Data

- Agencies and other entities connected to the state's network must employ adequate security measures to protect other systems and data connected to the state's network.
- Once authenticated to an access point, users will either be routed outside the state's firewall(s), or authenticated to the network. Just as with a wired network, state network authentication--whether enterprise-wide or agency-specific-- must satisfy prescribed login/password combinations prior to using enterprise or agency-specific resources that are not normally accessible by nodes outside the state's firewall(s).
- Access control mechanisms such as firewalls must be deployed to separate the wireless network from the internal wired network.
- As the technology permits, wireless networks will employ a combination of layered authentication methods to protect sensitive, proprietary, and patient information.

1.2.4 Risk Management

Agencies using wireless systems must develop general risk mitigation strategies for access points, users, and client devices such as virus protection, password standards, and other preventative measures.

1.3 Disruption and Interference

For state agencies, the DOC will resolve any conflicts between wireless devices in coordination with the affected agencies. Priority is granted to fully supported and registered installations, except in the case of medical, safety, or emergency devices, as appropriate.

1.4 Compliance with Other Network Standards

Agency WLANs must satisfy all existing and future standards pertaining to use and security of the state's network as required by law or established by the Nebraska Information Technology Commission or ITS.

1.5 General Recommendations for Agencies Implementing WLANs

1.5.1 Agencies must not undertake wireless deployment until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of operations. Agencies should perform a periodic risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products will be considered for purchase.

1.5.2 Agencies must be aware of the technical and security implications of wireless and handheld device technologies.

1.5.3 Agencies must carefully plan the deployment of 802.11, Bluetooth, or any other wireless technology.

1.5.4 Agencies must be aware that security management practices and controls are especially critical to maintaining and operating a secure wireless network.

1.5.5 Agencies must be aware that physical controls are especially important in a wireless environment.

1.5.6 Agencies must enable, use, and routinely test the inherent security features, such as authentication and encryption that exist in wireless technologies.

1.5.7 Where appropriate, agencies must employ protection mechanisms, such as firewalls and intrusion detection systems will be employed.

1.5.8 State agencies must assure all Federal, State, and agency compliance regulations are addressed prior to implementing wireless technology.

1.5.9 Agencies must educate wireless users in wireless security measures and controls to protect information resources they are accessing.

1.5.10 Agencies must utilize the DOC's Wireless Access Point Checklist (see Section 7.3).

2.0 Purpose and Objectives

The purpose of this standard is to ensure that only registered and secure WLANs are deployed by state government agencies.

3.0 Definitions

3.1 Access Point (AP)
A hub or interconnect device on a Local Area Network (LAN) that supports wireless (IEEE 802.11x) devices such as laptops, PDA's, etc. In some cases, the Access Point constitutes a stand-alone LAN where only a few wireless devices that are needed to communicate or share resources.

3.2 Campus Connection
Any building with high-speed access (at least 10Mb) to the 501 building.

3.3 Local Area Network (LAN)
A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. For State agencies, LANs are defined as restricted to rooms or buildings. An interconnection of LANs over a city-wide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas is commonly called a wide area network (WAN).

3.4 Metropolitan Area Network (MAN)

A data communications network that (a) covers an area larger than a local area network (LAN) and smaller than a wide area network (WAN), (b) interconnects two or more LANs, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs.

3.5 Strong Password

A strong password must be a minimum of 8 characters, and possess 2 of the 3 following attributes.

- Must contain at least one (1) numeric,
- Must contain both upper and lowercase letters,
- Must contain special characters (!@#$%^&*{}).

3.6 Wide Area Network (WAN)

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN.

4.0 Applicability

This standard applies to state agencies, excluding higher education institutions, which deploy a Wireless Local Area Network (WLAN).

Wireless services that fall within the definition of Campus Connection, Metropolitan Area Network (MAN), or Wide Area Network (WAN) must be purchased through DAS Information Technology Services (ITS) to comply with state statutes.

4.1 Exemption

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

4.1.1 Exemption Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion, federal government requirement, or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 521 S 14th Street, Suite 301, Lincoln, NE 68508). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the Technical Panel may be appealed to the NITC.

5.0 Responsibility

5.1 Agency and Institutional Heads

The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs, including disaster recovery plans for information technology. The Agency must notify the DOC before implementing a wireless system. Self-registration is available through the ITS website (see Section 7.1). Wireless services that fall within the definition of Campus Connection, MAN or WAN, must be purchased through the ITS to comply with State statutes. The agency authority may delegate this responsibility but delegation does not remove the accountability.

5.2 DAS Information Technology Services Divisions (ITS)
ITS shares responsibility for the security of the state's network. ITS reserves the right to disable network access for a device, server or LAN if adequate security for a wireless connection is not in place.

6.0 Related Documents

6.1 NITC Security Officer Handbook
http://www.nitc.state.ne.us/standards/security/so_guide.doc

6.2 NITC Network Security Policy
http://www.nitc.state.ne.us/standards/index.html

6.3 NITC Incident Response and Reporting Procedures for State Government
http://www.nitc.state.ne.us/standards/index.html

7.0 References

7.1 DOC's Wireless Registration Website
http://wlansupport.ims.state.ne.us/wlan_form.html

7.2 ITS Website
http://its.ne.gov/

7.3 DOC's Wireless Access Approval Process
(LINK TO BE ADDED ~ NITC file URL of appendix)

7.4 DOC's Wireless Access Point Checklist
(LINK TO BE ADDED ~ NITC file URL of appendix)

7.5 NIST Wireless Network Security Special Publication 800-48
http://csrc.nist.gov/publications/nistpubs/index.html

7.6 ITS "Network Security Standards", Draft - February 11, 2003
http://its.ne.gov/