COUNTY OF SACRAMENTO

Inter-Departmental Correspondence

December 6, 2007

TO: Information Technology Policy Board Members

FROM: Jeff Leveroni, Chair
Technology Review Group

SUBJECT: Update to County WAN/LAN Wireless Standards

1. FOR REVIEW AND FILE:

a. Updates to the County WAN/LAN Wireless Standards (attachment B of the Wireless Data Network Policy and Standards)
b. Updates to the County Public Internet Wireless Access Standards (attachment C of the Wireless Data Network Policy and Standards)

2. BACKGROUND:

The current wireless standards were developed around the technology that was available in 2004. During the last several years the technology has advanced to provide enhanced reliability and usability of mobile computing. The updates to our standards will address the following issues currently faced by the County:

- The Cisco Protected Extensible Authentication Protocol (PEAP) client software has been problematic with the Cisco communications server (ACS) causing login and disconnection issues for end-users
- RSA SecurID is not compatible with Microsoft Vista.
- Scripting is not supported with Microsoft's wireless client. Intel and other clients allow for scripts to be automatically initiated once a wireless connection is established.

The recommended updates will expand the type of authorized devices to include those that were not compatible with the initial wireless network, including the tablet PC and various PDA devices. The changes will also allow for additional

resources, such as public terminals and kiosks, to utilize the wireless infrastructure to connect to the County with increased security.

3. DISCUSSION:

The updates have been recommended by the WAN/LAN Steering Committee (WLSC) and approved at the October 2007 TRG meeting. The County Wireless Data Network Policy and Standards requires that all wireless data networking deployments must adhere to approved policy and standards as defined by the WLSC. The new standards are being distributed for your review and file. The attachments to this memo highlight the changes. The County Wireless Data Network Policy and Standards (http://inside.saccounty.net/sites/itpb/standards-policies/wireless-policy/docs/Wireless-Policy-v2.pdf) will be updated to reflect the same.

4. IMPACT OF IMPLEMENTING THIS RECOMMENDATION:

There is no impact expected from the adoption of the updated standards.

COUNTY OF SACRAMENTO

WAN/LAN STEERING COMMITTEE

ORIGINAL DATE: December 4, 2003
MODIFIED DATE: December 6, 2007

TO: Technology Review Group

FROM: WAN/LAN Steering Committee

SUBJECT: Wireless Data Networking Policy and Standards

1. RECOMMENDATION:

a. Approval of Wireless Data Networking Policy
b. Approval of Wireless Data Networking Standards

2. BACKGROUND:

As Sacramento County's Wide Area Network evolves, the County must consider Wireless Data Networking as an evolutionary step and make the appropriate considerations for its use and implementation. This Wireless policy and standards only apply to Sacramento County Data Network. It does not apply to the Sacramento Regional Radio Communications System.

While Wireless Data Networking provides the ease of connectivity and the freedom of mobility it also introduces greater vulnerabilities. The traditional physical securities of a wired network can no longer be relied upon with regard to Wireless Data Networking.

It is the intent of this recommendation to provide the necessary and required standards and policy for Wireless Data Networking. Together these establish the base requirements that both ensure that acceptable standards are adhered to and that necessary security measures are put in place.

3. DISCUSSION:

Wireless Data Networking introduces a new technology into the County of Sacramento Wide Area Network. This technology, as with all others, is not without its unique risks or benefits. With the ease of connectivity and the freedom of mobility come vulnerabilities. Corporate networks that have WLAN extensions create an entry for their users as well as anyone else within the connectivity area of the Access Point (AP). Hackers have developed software that enables them to "sniff" for wireless connectivity. Through a

practice known as war driving, hackers map out these Access Points and use them as onramps to corporate networks or the Internet. The traditional physical security that is enforced by fences, guards, doors, and locks are now bypassed by radio waves.

Deploying Wireless Data Networking introduces risks not previously assumed by the County of Sacramento. The following is a summary of known risks.

- Potential for unauthorized access to County of Sacramento resources.
- Potential eavesdropping of communications.
- No means of providing traditional physical security.
- Loss of the 2nd factor of security that is provided by physical building security.
- Rogue (unauthorized) wireless access points installed on the network.
- Reliability cannot be guaranteed, due to the unlicensed nature of Wireless Data Networking or interference from other foreign elements.
- Additional entry point for potential intrusion or denial of service.

While these risks are present deploying Wireless Data Networking provides benefits that can have a positive impact for the County of Sacramento.

- Avoidance for recurring cost of circuit connectivity.
- Mobility of access – provide roaming capability within the sphere of the wireless deployment.
    - Local Area Network
    - Wide Area Network
    - Nation-wide Coverage
- Rapid deployment of network services.
- Deployment of temporary network services.
- Public Internet access at County facilities.
- Connectivity in areas where access has previously not been possible.
- Provide cost-effective redundant, disparate connectivity path.

4. STRATEGY:

Minimized wireless exposure through the strategic use of authentication, encryption, multiple security layers and technologies to reduce the exposure to risk when deploying Wireless Data Networking technologies.

5. POLICY STATEMENTS:

As the capabilities of Wireless Data Networking range according to need, as listed below Wireless Data Networking has been divided into two service categories. Each of these categories is defined and is accompanied by requirements specific to that service. These requirements are in accordance with the County's strategy for Wireless Data Networking.

Core Policies

These policies apply to all wireless deployments regardless of technology:

a. All Wireless Data Networking deployments must adhere to approved policy and standards as defined by the WLSC.
b. Any Wireless Data Networking deployment will be reviewed and approved by Security Perimeter Team prior to implementation.
c. A perpetual audit will be conducted to locate weaknesses in Wireless Data Networking deployments as well as those not adhering to County of Sacramento policy and standards.
d. Any Wireless Data Networking deployment not adhering to County of Sacramento Wireless Data Networking policy and standards can and will be severed from the network.

Deployment Specific Policies

These policies apply to specific technology deployments as defined in each of the sections below:

1. County Wireless Services:

A. Point-to-Point:

Definition: The use of Wireless Data Networking technology to provide network connectivity between two County sites.

Requirements:
- Must not associate with more than one network device.
- Must use directional antennas.
- Must utilize encrypted traffic as defined by approved governance bodies.
- Must support SNMP for network management.

B. WAN/LAN Access:

Definition: The use of Wireless Data Networking technology to extend Local Area Networks.

Requirements:
- Must be compliant with Wi-Fi standards.
- Must employ at least two-factor authentication.
- A factor of authentication must be centrally managed.
- Must have centrally managed access points.
- Must utilize encrypted traffic as defined by approved governance bodies.
- Must not allow peer-to-peer access.
- The strategic use of various forms of authentication to ensure the identity of the individual and/or resource authenticating.

C. Public Internet Access:

Definition: The use of Wireless Data Networking technology to provide County of Sacramento constituents and guests access to Internet based resources while visiting County of Sacramento facilities on County of Sacramento business.

Requirements:
- Must be compliant with Wi-Fi standards.
- Must not allow peer-to-peer access.
- Must not allow unauthenticated access to the County of Sacramento Wide Area Network.
- Must not be connected to County of Sacramento Wide Area Network.[1]

2. Commercial Wireless Services:

A. Internet Access:

Definition: The use of commercially available wireless service for Internet access.

Requirements:
- Must not be connected to County of Sacramento Wide Area Network.
- Access to the County network is provided by using the County of Sacramento's security perimeter via a VPN connection.
- Must be an approved vendor having signed all appropriate Business Partner Service Levels agreements as established by the County of Sacramento.

B. Extranet Access:

Definition: The use of commercially available wireless service to connect to the County's Extranet.

Requirements:
- Must connect to the County of Sacramento's security perimeter via a dedicated connection.
- The commercial wireless service must not transport County data across the Public Internet.
- Must be an approved vendor having signed all appropriate Business Partner Service Levels agreements as established by the County of Sacramento.

---

[1] WLSC will re-evaluate using the County's WLAN infrastructure for public access after the pilot project for MPLS is successfully implemented.

6. CONCLUSION:

The use of Wireless Data Networking is dependent upon business need. The requirements, as they relate to core policies and each specific deployment, are mandatory requirements prior to implementation of a Wireless Data Networking solution.

Attachment A
County: Point-to-Point Wireless Standards

Description	Standard
Wireless Security	▪ Minimum of 128bit encryption via WI-FI Protected Access (WPA)[2] or IPSEC. ▪ No SSID broadcast. ▪ Maximum of one association allowed. ▪ Filter on MAC address of associated bridge.
Radio infrastructure	All Cisco models, All Proxim models.
Antenna	Directional only, no omni-directional allowed.
Transmit power output	Set to the minimum required for establishing a link.
Radio management	Must support SNMP for network management.

[2] WPA will serve until the 802.11i standard is ratified and support available for the wireless equipment.

Attachment B
County: WAN/LAN Wireless Standards

Description	Standard
Wireless Security	WI-FI Protected Access (WPA/WPA2).
Access Point	All 802.11a/b/g/n that support WPA/WPA2.
Client Wireless Network Adapters	Must be WPA/WPA2 compliant. Various types of adapters can be found on a list of compliant equipment at http://www.wi-fi.org
Client Wireless Network Software	Must be Windows 2000 or higher. Palm versions built on Windows 2000 kernel are acceptable.
Authentication Server	Cisco RADIUS (no pre-shared keys).
EAP Type	PEAP-GTC or equivalent security that requires two-factor authentication.
RSA and RADIUS Hardware	Must meet existing County standards for enterprise server.
Access Point Management	Cisco Wireless LAN Solution Engine (WLSE).
Access Point Configuration Management	OCIT managed.
Rogue Access Point Detection	Cisco Wireless LAN Solution Engine (WLSE).[3]

Note: WAN/LAN Wireless Standards modified by WLSC and approved by the TRG on October 16, 2007. Submitted for Review and File to the ITPB on December 6, 2007.

[3] WLSE version 2.5 will have rogue AP detection capabilities. Version 2.5 is due to be release Q4 2003.

Attachment C
County: Public Internet Wireless Access Standards

Description	Standard
Wireless security	None
Access point	Any vendor/model that supports Wi-Fi standard 802.11a/b/g/n.
Internet Connectivity	Departments can utilize the public wireless infrastructure provided by OCIT or departments can implement direct Internet connections to the Access Points. At no time can the public wireless devices nor the supporting infrastructure have a physical connect to the County.
Wireless network adapters	Any adapter that supports Wi-Fi standard.
Client software	Any software that supports Wi-Fi standard.
Access point configuration management	OCIT or department managed and configured as per standards.

Note: Public Internet Wireless Access Standards modified by WLSC and approved by the TRG on October 16, 2007. Submitted for Review and File to the ITPB on December 6, 2007.

Attachment D
Commercial: Internet Wireless Standards

Description	Standard
Service provider	Any County approved service provider.
Wireless security	County's security perimeter via VPN.
Internet service	Service provider's Internet connection.
Client adapter	Service provider approved.
Client software	Service provider provided.

Attachment E
Commercial: Extranet Wireless Standards

Description	Standard
Service provider	Any County approved service provider.[4]
Wireless security	County's security perimeter via Extranet connection.
Internet Service	County's security perimeter Internet connection.
Client adapter	Service provider approved.
Client software	Service provider provided.

[4] The County is currently evaluating multiple service providers. When a selection(s) is made the document will be updated with the available providers. (Note: AT&T, NEXTEL, Sprint, and Verizon are examples of commercial wireless service providers)