

A. Cover Sheet

2009 NASCIO Recognition Awards

Secure Wireless LAN

Michigan Department of Information Technology

Nomination Category: Information Security and Privacy

Nominee: Rhea Linn
Wireless LAN Project Manager
Design Services, Office of Telecommunications
Michigan Department of Information Technology
608 West Allegan
1st floor - MDIT Telecommunications
Lansing, MI 48933
Linnr@michigan.gov
517 335 7043

Nominator: Jack Harris
Director of Telecommunications
Michigan Department of Information Technology
608 West Allegan
1st floor - MDIT Telecommunications
Lansing, MI 48933
Harrisj8@michigan.gov
517 241 7565

B. Executive Summary

Resolving security issues is pivotal to implementing current and emerging high performance information and communications technology (ICT) solutions, and enabling modernization in our increasingly open, shared and mobile operational and service environment. Whether the public policy or CIO service priority is shared services, electronic records management or ensuring transparency – or the solution being considered involves legacy application modernization, voice and data communications, or identity and access management – security safeguards are an ever present priority.

Wireless communications are emblematic of this issue. Wireless has become a ubiquitous service expectation and a near universal public policy goal. It is also one of the ever-present ICT challenges; and effective, transferable, best practice solutions are exceptionally valuable contributions to the CIO solution portfolio. Security breaches can also involve privacy issues, and affect service quality and trust in the integrity of government services. Adverse security publicity can severely damage IT management and organizational standing.

Over the last two years the Michigan Department of Information Technology (MDIT) has developed an innovative and effective balance of management, operational, technical and enterprise service solutions for wireless communications in a best-practice security environment, providing transferable policy, operational and technical lessons for other jurisdictions.

Innovative: Michigan is the first state government to have a centrally managed enterprise wide wireless LAN solution, accelerating a convergence of policies for wired and wireless LAN's .

Transferable: The policy, procedural and technology lessons are transferable to other jurisdictions, either in whole or in part.

Best Practice Solution: Five barriers or challenges were addressed.

Security: Improve wireless security to match or exceed wireline standards

Enterprise Solution: Establish enterprise standards and service capability

WAN / Wireless Integration: Provide a Wireless LAN solution for Wide Area (CBDS) customers

Seamless Log-on Experience: Integrate wireline and wireless policies and practices, and provide a seamless log-on experience

Affordability: Provide an affordable, cost-effective service

Cost Effectiveness: A comparison of the legacy wireless approach used before 2007 and the current design shows a significant gain with the wireless version two (V2), cost savings per site of \$3,591 a month, or \$43,092 per year. The 16 statewide sites installed to date have an estimated annual savings of \$688,000. Long-term payback is estimated at \$7 million per year (See section E)

C. Description

Security Issue: Resolving security issues is pivotal to implementing current and emerging high performance ICT solutions, and enabling modernization in our increasingly open, shared and mobile operational and service environment. Whether the public policy or CIO service priority is shared services, electronic records management or ensuring transparency – or the solution being considered involves legacy application modernization, voice and data communications, or identity and access management – security safeguards are an ever present priority.

Wireless communications are emblematic of this issue. Wireless has become a ubiquitous service expectation and a public policy goal. It is also one of the ever-present ICT challenges and effective, transferable, best practice solutions are exceptionally valuable contributions to the CIO solution portfolio. Over the last two years the Michigan Department of Information Technology (MDIT) has developed such a solution.

Initial Solution: Michigan, along with many other states had responded to the driving trend, and has had wireless capability for several years. Drivers included:

- Technology maturity, increased manageability, and higher-speed standards
- Changing employee demographics, with a new generation of workers, having an expectation of instant connection anytime / anywhere
- Heavy reliance on e-mail, including wireless Internet
- Emphasis on shared services, with associated changes in working relationships with partners
- Priority emphasis on the MDIT IT Strategic Plan goal of a high performance worker and workplace
- MDIT priority on mobile services and telecommuting, including disaster preparedness

At the same time security issues and concerns were accelerating at an even faster rate. Cracking methods have become more sophisticated, innovative, and prevalent with wireless and are also used to crack into wired networks. Adverse security publicity can severely damage IT management and organizational standing.

Legacy Wireless Version 1 (v1) Solution and Challenges: The first MDIT wireless solution had numerous challenges. The initial implementation used heterogeneous solutions from multiple vendors, causing multiple issues with policies, standards, operation, maintenance, compatibility and management.

- No enterprise wide policy or standards on wireless LAN implementations had been developed

- No Wide Area Network solution was available; restricted to fiber connected offices only
- The re-occurring \$260 per Access Point monthly charge proved cost-prohibitive for most agencies. This resulted in limited installations
- Service providers consolidated or discontinued solutions
- State of Michigan (SoM) users were taking it upon themselves to install unsecure, unauthorized wireless solutions within the workplace.
- Local Area Network (LAN) services within conference rooms and community areas incurred additional costs, posed potential hazardous environments, and created security vulnerabilities
- Two-Factor authentication standards involved additional administration of accounts and monthly charges, and were viewed as too cumbersome by key government executives

Secured Enterprise Wireless Solution Framework (Version 2): In order to mitigate security and other issues with the original Wireless LAN version, MDIT developed and tested version 2 solution by March 2007. Five barriers or challenges were addressed.

Security: Improved wireless security to match or exceed wireline standards

Enterprise Solution: Establish enterprise standards and service capability

WAN / Wireless Integration: Provide a Wireless LAN solution for Wide Area (CBDS) customers

Seamless Log-on Experience: Integrate wireline and wireless policies and practices, and provide a seamless log-on experience

Affordability: Provide an affordable, cost-effective service

The V2 solution was implemented May 2007. Currently 16 locations throughout Michigan are installed with LAN services, 13 are LMAN connected in the Lansing area, where the largest number of state employees are located. Wide area implementation is in three counties, and Wireless LAN Access Points are installed and awaiting a security decision in five other counties.

Solution to the Challenges / Barriers

- Develop Wireless LAN policy and standards in collaboration with the MDIT Office of Enterprise Security.
- Implement a single vendor solution with proven performance, reliability, security and scalability (Cisco Unified Wireless Solution)
- Use existing Infrastructure authentication methods to secure Wireless LAN connectivity and eliminate the VPN/SecurID requirement. Meet two-factor authentication standards by using:
 - Radius and Active Directory (AD) for machine and user account/password authentication.
 - Ensure higher level of security by limiting SoM Intranet access to SoM workstations only. Implement AD machine authentication prior to allowing wireless access and AD UID/PW authentication.

- Implement best practice authentication and encryption protocols; Microsoft Server Certificates, MS-CHAPv2, PEAP, AES, WPA2, and 802.1X.
- Provide Guest Access to visitors in a secured fashion
 - Internet access only
 - Bandwidth limitations – 384K to prevent Wireless ‘Guest’ users from consuming too much bandwidth
 - Surf Control/BlueCoat/Proxy - limits and logs Internet access by guest clients.
 - Firewall all Guest traffic
 - Tunnel Guest traffic inside of AES tunnel
- Implement Wireless WAN using Hybrid REAP (H-REAP) to remote SoM office locations. H-REAP keeps data traffic local, while allowing the WLAN access points to communicate with the centralized WLAN controllers for manageability.
- An Enterprise Standard was developed to provide effective use of WAN bandwidth by allowing LAN access to local resources at WAN connected sites. All existing WLAN security practices are applicable. The experience to the Wireless LAN user is now the same across the enterprise.

In addition, All Web transactions through the Security Servers are logged, providing detailed accounting information. This gives the visibility necessary to determine web usage patterns, audit user history, track security issues, and develop comprehensive web protection and control policies.

Transferability of Solutions: The following policy, procedural and technology lessons are transferable to other jurisdictions.

Policy and Governance

- Executive level sponsorship with clear definition of service requirements
- Establish Enterprise level policies and standards first
- Develop sound procedural requirements up front, especially security

Processes

- Collaborate with all stakeholders; Security, desktop support, Customer Service Support
- Demonstrate and document value of lab tests

Technology

- Utilize existing infrastructure as much as possible: Active Directory, RADIUS, VPN concentrators, LAN infrastructure.
- Select all components based on integration and product compatibility
- Implement Hybrid REAP for WWAN to realize cost savings on local WLAN controllers.
- Design for implementing Wireless LAN solutions without proprietary methods

Communications and Support Plan: A description of the Wireless LAN service is in the MDIT Telecommunications Service catalog, defining scope of services,

agency responsibilities, and how to order the service. The MDIT Customer Service Center is trained to help clients triage and resolve any connectivity and authentication problems that may be reported with WLAN.

D. Significance: The solution is an innovative and effective balance of management, operational, technical and service solutions in a best practice security environment, providing transferable policy, operational and technical lessons to other jurisdictions.

Innovative: Michigan is the first state government to have a centrally managed enterprise wide wireless LAN solution, accelerating a convergence of policies for wired and wireless LAN's . Other innovative aspects include:

- use of MS-AD machine credentials as “two-factor” authentication for secured
- WiFi access for state employees
- bundling of WiFi as a “no-extra-cost” service with Managed LAN rated service
- consistent architecture for WiFi controls and security between metro-area and wide-area implementation

Policy, Strategic and Goal Alignment: Supports - Gubernatorial goals for better government and a ‘great workplace’; Michigan Statewide IT Plan goal for a high performance workforce and workers; MDIT IT plan mobile and wireless strategies; Office of Enterprise Security Strategic Plan; aligns with the ‘Enterprise Architecture - Strategic Approach’ ; and maximizes service options for the ARRA broadband proposal expansion of government services.

Service Sectors: Supports services for health, education, employment services, environment and natural resources, transportation and others

Legacy Modernization: Represents a successful, cost effective example of ICT modernization.

Wireline and Wireless Integration: Smooths the transition from legacy services to next generation services, with a seamless sign-on

Beneficiary, Stakeholder Groups: Supports directors and employees, shared service partners, vendors, visitors, trainees using state facilities and citizens using state offices and service areas

Addresses Leadership and Citizen Comfort-zone Needs: Meets Governor’s, CIO’s and management needs, increasing policy support and strategic utilization, accelerating implementation and educating decision-makers and the public on the benefits of ICT modernization.

E. Benefits

Impact and Outcomes

Direct Security Benefits:

- The security practices now in place for the State of Michigan (SoM) Wireless LAN Service are stricter than those imposed for Ethernet LAN implementations.
- DIT Telecommunications is now able to identify Rogue Access Point installations within SoM office buildings where Wireless LAN is installed. The Wireless Control System (WCS) offers the ability to automatically detect and contain these devices from a central management console.

Supports, Helps Reconcile ICT Community and CIO Priorities: The secure wireless LAN solution helps reconcile the conflicts among integrated clusters of some of the highest 2009 NASCIO / CIO priority strategies (shared services and security) and technologies and solutions (legacy applications and modernization, voice and data communications), in a cost-containment environment.

Enterprise, Statewide Benefits: Currently 13 state departments out of 19 have these services at sites in 6 counties

Employee, Partner and Visitor Needs: Guest needs are met on site by enabling a virtual home office environment. Productivity is maintained and off site decision-making enabled

Operational and Service Efficiencies:

- **Mobility:** Enhances freedom to move anywhere / anytime within a building or multi-building campus and remain connected to real-time information

- **Flexibility:** Public areas, meeting rooms and office space in general become more flexible; capacity and utilization patterns can be modified readily

- **Productivity:** All users can access the resources they need instantly. Downtime can be changed to productive time during breaks in meetings.

- **Process Efficiencies:** Reduces the costs of moves, adds and changes for rapidly growing organizations

- **Decisionmaking:** Faster-decision making through instant access to networked information

Financial Benefits: Cost comparison WLAN version 1 & WLAN version 2

Sample V1 Cost: \$3696.00 per month; Sample V2 Cost: \$105 per month:

Wireless v2 cost savings per month: \$3,591.00

Version 1	Hardware/Software investment:	\$116,580
	Staff support and overhead PER YEAR:	\$93,677
	Cost to customer PER USER:	\$31.00 per month
	VPN/SecurID PER USER:	\$13.00 per month
Version 2	Hardware/Software investment:	\$33,779
	Staff support and overhead:	\$14,989 per year
	Cost to customer PER USER:	\$1.25 per month

Long Term Payback: Assuming an average site of 80 workers, with annual V2 savings of \$43,000 per site, and with full V2 implementation for a conservatively estimated 25 percent of the states 55,000 employees, would save over \$7 million annually.