



Compliance Component

DEFINITION

<i>Name</i>	Wireless LAN
<i>Description</i>	A wireless LAN (WLAN) is a radio-based communication system connecting wireless-enabled devices such as laptop computers with wireless access points using the IEEE 802.11 set of standards. This in turn connects to an agency's wired network for connectivity to the agency's business applications.
<i>Rationale</i>	Wireless communications are desirable in areas where a wired network may not be possible or practical, or limits the implementation of new applications where mobility is a key enabler.
<i>Benefits</i>	<p>The use of wireless LAN's has shown to be beneficial in the following ways:</p> <ul style="list-style-type: none"> • Provide connectivity where no wired network is available • Provide mobile connectivity for a variety of business applications • Increased user productivity in many environments

ASSOCIATED ARCHITECTURE LEVELS

<i>Specify the Domain Name</i>	Infrastructure
<i>Specify the Discipline Name</i>	Network
<i>Specify the Technology Area Name</i>	Network Hardware
<i>Specify the Product Component Name</i>	

COMPLIANCE COMPONENT TYPE

<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	

COMPLIANCE DETAIL

<i>State the Guideline, Standard or Legislation</i>	<p>There are several issues to address before the deployment of a wireless network (WLAN):</p> <ul style="list-style-type: none"> • Procurement and deployment of WLAN equipment (adapters, access points, etc.) should be restricted to the agency's IT department • Procurement of devices with built-in WLAN capabilities should be coordinated with the agency's IT department to ensure radio and security compatibility • A site survey should be performed before deployment to indicate areas of potential interference (e.g., cordless phones, microwave ovens, building materials, other wireless implementations), and for recommendations related to access point / antenna location and configuration – the person performing the site survey should have sufficient tools and expertise to correctly perform the process • Check the manufacturer's equipment to verify compatibility with current WLAN deployments – it is recommended to keep the
---	---

number of different manufacturers in a WLAN structure to a minimum

- Physical security of the wireless access points should be ensured
- Provide user education on wireless network usage and risks

The following features should be required for WLAN access points:

- Upgradeable firmware
- Radio compatibility should be 802.11b/g
- Should be compatible with 11I Security standards
- Be configurable for wireless security standards as defined by the State's Architecture Security Domain (see below)
- Ability to adjust radio transmission power
- Automatic radio channel sensing for non-congested connections
- Ability to use in-line power to the access point
- Ability for WLAN users to roam among access points without losing network connectivity
- Ability to adjust bandwidth rate based on radio signal strength to maintain client connections as long as possible

The following features are desirable for WLAN access points:

- Ability to have an integrated or external antenna
- Ability to add 802.11a radio capabilities if necessary
- Intrusion detection or rogue access point detection
- QoS (quality of service) capabilities
- Ability to segregate wireless clients into separate VLAN's
- Hot standby (failover) or load-balancing deployment options
- Interference detection

Wireless adapter (purchased or integrated) requirements:

- Software utilities that assist in the connection and monitoring of the device's wireless connection
- Compliance with radio and security standards as defined at the access point level

Security considerations:

- The State's Architecture Security Domain as defined requirements for implementing wireless networks. Refer to the web site at:

<http://oit.mo.gov/architecture/tamain.htm>

Areas covered include:

- Default administrative access
- SSID security considerations
- Encryption levels to be used
- Authentication methods to be used
- Radio security measures (power adjustments)
- Various deployment scenarios, such as utilizing VPN over wireless, wireless VLAN's, etc.
- Accessing WLAN's not controlled by your agency, such as retail or airport "hotspots"
- Auditing wireless deployments for vulnerabilities and rogue

	<p>installations, coverage limits, etc.</p> <p>Management considerations:</p> <p>If WLAN equipment is deployed, it is recommended to have a management platform capable of monitoring and performing maintenance on the WLAN access points. Functions that should be performed would include:</p> <ul style="list-style-type: none"> • Monitor access point availability • Monitor access point radio health (interference, usage, etc.) • Process alerts issued by the access point due to system health or security issues (e.g., rogue access points) • Perform firmware and/or configurations upgrades to the access points • Logging access point configuration changes • Delegate management functionality to non-administrative staff as deemed appropriate
--	--

Compliance Sources

<i>Name</i>	Internet Engineering Task Force	<i>Website</i>	www.ietf.org
<i>Contact Information</i>	ietf-info@ietf.org		
<i>Name</i>	Cisco, Inc.	<i>Website</i>	www.cisco.com
<i>Contact Information</i>	-		
<i>Name</i>	MoreNet	<i>Website</i>	www.more.net
<i>Contact Information</i>	-		
<i>Name</i>	NASCIO	<i>Website</i>	www.nascio.com
<i>Contact Information</i>	-		

KEYWORDS

<i>List Keywords</i>	Wireless, Access point, SSID, site survey, 802.11
----------------------	---

COMPONENT CLASSIFICATION

<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i>	<input checked="" type="checkbox"/> <i>Current</i>	<input type="checkbox"/> <i>Twilight</i>	<input type="checkbox"/> <i>Sunset</i>
<i>Sunset Date</i>				

COMPONENT SUB-CLASSIFICATION

Sub-Classification	Date	Additional Sub-Classification Information
<input type="checkbox"/> <i>Technology Watch</i>		
<input type="checkbox"/> <i>Variance</i>		
<input type="checkbox"/> <i>Conditional Use</i>		

Rationale for Component Classification

Document the Rationale for Component Classification

Migration Strategy

Document the Migration Strategy

Impact Position Statement

Document the Position Statement on Impact

CURRENT STATUS

Provide the Current Status

In Development *Under Review* *Approved* *Rejected*

AUDIT TRAIL

Creation Date

9/21/2004

Date Approved / Rejected

7/12/05

Reason for Rejection

Last Date Reviewed

Last Date Updated

2/16/05

Reason for Update