Directives and Instructions Regarding Wireless LAN in Department of Defense (DoD) and other Federal Facilities

Wireless Infrastructure, Article 12-29-2011

The federal government, and the Department of Defense (DoD) in particular, recognizes that standards based wireless networking has become an essential part of conducting business in an efficient manner. Many commercially available products offer the capability of providing the electronic security comparable to wired networks. However, these products must be configured and secured properly to provide the degree of security desired. Unlike a wired network, wherein the active components of the data communications network can be physically secured in a telecom room with restricted access, the wireless network, by its very nature, requires that access points and antennas are distributed throughput the facility, requiring consideration of policies for protecting these assets. This article provides a brief guide to Directives, Instructions, and STIGs regarding the wireless LAN infrastructure in federal facilities, with an emphasis on physical security requirements for the access points.

DoD Directive 8500.01 – Information Assurance

http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

This overarching security policy, DoD Directive 8500.01, establishes policy and assigns responsibilities to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare. DoD directive 8500.01 applies to All DoD-owned or -controlled information systems that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity.

In addition to other equipment, this directive applies to *"2.1.2.7. Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed."*

DoD Instruction 8420.01- Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies

http://www.dtic.mil/whs/directives/corres/pdf/842001p.pdf

DoD Instruction 8420.01 establishes policy, assigns responsibilities, and provides procedures for the use of commercial WLAN devices, systems, and technologies to achieve and increase joint interoperability, appropriately protect DoD information, and enhance overall security to sufficiently protect DoD information by embracing open standards for WLAN devices, systems, and technologies.

8420.01 specifies that the Defense Information Security Agency (DISA) shall "*develop and provide architectures, specifications, systems engineering, and integration guidelines for command and control capable WLAN systems in coordination with National Security Agency/Central Security Service (NSA/CSS), per National Security Directive 4".*

8420.01 specifies that unclassified WLAN infrastructure devices shall have FIPS 140 validated encryption to protect data-in-transit on the WLAN infrastructure portion of the end-to-end WLAN communications link. WLAN infrastructure systems may be composed of either stand-alone (also referred to as an autonomous) APs, or thin APs that are centrally controlled by a WLAN controller (also referred to as a WLAN switch). All WLAN infrastructure devices shall implement AES-CCMP as defined in the IEEE 802.11-2007 standard. The AES-CCMP encryption shall be validated under the NIST CMVP as meeting FIPS 140.

This instruction requires validated Physical Security. APs used in unclassified WLANs should not be installed in unprotected environments due to an increased risk of tampering and/or theft. If installed in unprotected environments, APs that store plaintext cryptographic keying information shall be protected with added physical security to mitigate risks. DoD Components may choose products that meet FIPS 140-2 Overall Level 2, or higher, validation (to ensure that the AP provides validated tamper evidence, at a minimum). Alternatively, DoD Components may physically secure APs by placing them inside of securely mounted, pick-resistant, lockable enclosures.

WLAN APs used to transmit or process classified information shall be physically secured, and methods shall exist to facilitate the detection of tampering. WLAN APs are part of communication systems and shall have controlled physical security, in accordance with DoD 5200.08-R (Physical Security Program- http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf).

Additionally, either physical or electronic inventories may be conducted by polling the serial number or MAC address. APs not stored in a COMSEC-approved security container shall be physically inventoried.

8420.01 specifies Wireless Security Technical Implementation Guide (STIG) compliance. In addition to adhering to the procedures specified in this enclosure, incorporate the security best practices specified in the Wireless STIG (below) as it pertains to the implementation of WLANs.

Wireless Security Technical Implementation Guide (Wireless STIG) V6R5, can be found at the DISA Website: http://iase.disa.mil/stigs/net_perimeter/index.html

The *Wireless Security Technical Implementation Guide (STIG)* is published as a tool to improve the security of Department of Defense (DoD) commercial wireless information systems. This document is meant for use in conjunction with the *Enclave, Network Infrastructure, Secure Remote Computing,* and appropriate operating system (OS) STIGs.

This STIG supports the design, implementation, and management of wireless devices and networks that are used to provide information technology (IT) services to mobile workers in the DoD; in addition to providing implementation guidance for DoD Directive 8100.02 and other DoD policies related to wireless systems.

In this STIG, *"for wireless systems and devices, policies are classified as CAT I if failure to comply may lead to an exploitation which has a high probability of occurring, does not require specialized expertise or resources, and leads to unauthorized access to sensitive information (e.g., Classified). Exploitation of CAT I vulnerabilities allows an attacker physical or logical access to a protected asset, allows privileged access, bypasses the access control system, or allows access to high value assets (e.g., Classified)".* Thus, physical access to wireless APs is a CAT 1 vulnerability.

This STIG includes a 100 + element checklist for securing the wireless network. STIG ID WIR0025 specifies that wireless access points are physically secured.

DoD Directive 8100.02- Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf

This directive specifies, among other thinks, that Encryption of unclassified data for transmission to and from wireless devices is required. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, overall Level 1 or Level 2, as dictated by the sensitivity of the data.

FIPS-140-2 Security Requirements for Cryptographic Modules

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

This publication provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module.

No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. Security Level 1, however, is inadequate. DoD Instruction 8420.01 specifies Security Level 2 for wireless LAN.

Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or for pick-resistant locks on removable covers or doors of the module. Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorized physical access.

FIPS-140-2 paragraph 4.5 states “A cryptographic module shall employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module (including substitution of the entire module) when installed. All hardware, software, firmware, and data components within the cryptographic boundary shall be protected.”

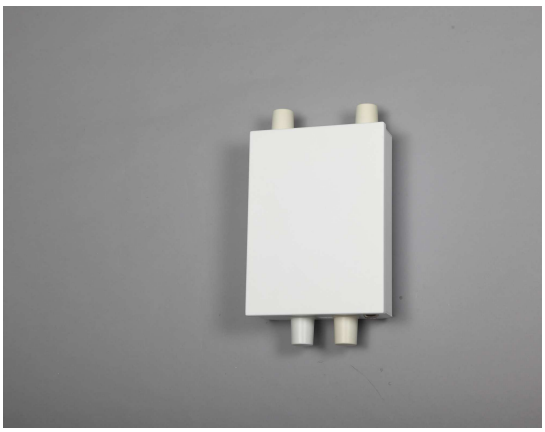
The NIST Cryptographic Module Validation Program (CMVP) maintains a list of items which have been validated for FIPS 140-2 capability. This list is located at:

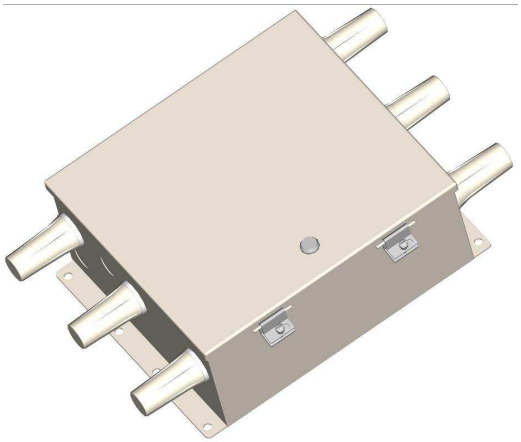
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

This list includes the *Security Policy*, as created by the vendor. This document constitutes the Cryptographic Module Security Policy for the controllers and access points with FIPS 140-2 Level 2 validation from the vendor. This security policy describes how the controller and AP meet the security requirements of FIPS 140-2 Level 2, and how to place, secure, and maintain the AP in a secure FIPS 140-2 mode. This policy was prepared by the vendor as part of the FIPS 140-2 Level 2 validation of the product.

Secure, Convenient, Aesthetic suspended ceiling enclosures and mounts for wireless access points with non-detachable antennas or body integrated antennas

Suspended ceiling enclosures for wireless access points with detachable antennas. Interchangeable doors on enclosure permit easy upgrades to new APs and antennas.





Indoor/outdoor NEMA wall mounted security enclosures with antennas

Additional information on wireless network infrastructure is available at http://www.oberonwireless.com/faq-resources.php