U.S. Customs and Border Protection

Attachment Q1

Sensitive Wireless Systems

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 21, 2010	Introduced new terminology Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53

CONTENTS

1.0 INTRODUCTION

This document provides techniques and procedures for implementing wide area, local area, and personal area wireless architectures within the Customs and Border Protection (CBP) Information Security Program. This document, published as an attachment to the CBP Information Systems Security Policies and Procedures Handbook, 1400-05D, serves as a foundation for CBP to use in developing and implementing their wireless Information Technology (IT) security programs. It incorporates guidance from the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the Department of Defense (DoD).

1.1 Purpose and Scope

This document is issued as implementation guidance under the authority of the CBP Chief Information Officer through the CBP Chief Information Security Officer (CISO). Existing implementation of prior directives shall remain in effect until new DHS and CBP policy or implementation guidance is issued. This document addresses the security specifics of sensitive wireless systems only and does not cover the use of classified wireless systems. In accordance with the Department of Homeland Security (DHS) Sensitive Systems Policy Directive 4300A, DHS Wireless Communications Policy stipulates that wireless communications technologies are prohibited from use within DHS unless the CBP Authorizing Official (AO) specifically approves the technology and application. Further, CBP AO must approve the implementation and use of wireless systems at a specified risk level during the certification and accreditation (C&A) process and ensure appropriate and effective security measures are included in the System Security Plan.

Given the ongoing rapid evolution in wireless technology, including current dissimilarities between wireless systems and across multiple vendors' product offerings, specific wireless systems may or may not have the ability to be made wholly compliant with the countermeasures this document outlines. The guidelines set forth in this document are not intended to prohibit the use of devices that cannot meet the countermeasures recommended herein. Rather, the intent is to provide a detailed explanation of the many countermeasures that can be applied to wireless systems. CBP AO should pay particular attention to the potential risks that must be considered in approving systems that have technological barriers that prevent the adoption of these countermeasures. CBP AO should understand the risks associated with a particular wireless system. This may include applying some but not all of the outlined countermeasures, as long as the risk is measured and mitigated to an acceptable level determined by the CBP AO.

The scope and contents of this document will change over time as new capabilities are added to CBP systems, as security standards are upgraded, and as a result of user experience and comment. As the CBP IT Wireless Security Program matures, additional attachments to the CBP Information Systems Security Policies And Procedures Handbook that address specific security areas of interest will be developed and published.

1.2 Background

Wireless communications is the technology that enables the transfer of information among separated locations by encoding emanations of energy that travel through space between locations. The distances between locations may be measured in millimeters or in thousands of

kilometers. Wireless technologies use a wide range of energy spectrum (e.g., radio frequency [RF] and infrared [IR]), both analog and digital wave forms, and various types of encoding (e.g., multiplexing and modulation schemes, layered protocols) for delivery. As technology continues to evolve, new forms of secure wireless communications continue to emerge.

The DHS Wireless Security Board (WSB) coordinates and evaluates DHS-wide approaches to wireless security on behalf of the Wireless Management Office (WMO). The WMO's role is to "coordinate the development of policy and strategy for the use of wireless technologies across the department to ensure interoperability, value delivery, and architectural compliance while moving to the desired state of our enterprise architecture" (MD 4100.1). As such, the WSB assists the WMO in formulating and coordinating department-wide policies and guidelines related to security of wireless services and technologies. The WSB is co-chaired by WMO and DHS CISO to ensure consistency in the development and application of risk management approaches and C&A processes for wireless services and technologies. The WSB also assists DHS in the development, deployment, and maintenance of wireless security strategies for major wireless IT programs and system development initiatives. In addition, the WSB serves as a forum for identifying and resolving emerging wireless security issues and concerns, and it provides DHS operational elements with a mechanism for ensuring that risks to their wireless systems are adequately addressed by the WMO and DHS. This collaboration ensures that the WMO is effectively managing the Department's wireless security risks.

2.0 4300A POLICY REQUIREMENTS

Wireless systems include wireless local area networks (WLAN), wireless wide area networks (WWAN), wireless personal area networks (WPAN), peer-to-peer wireless networks (i.e., ad hoc wireless networks), and IT systems that leverage commercial wireless services. Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols. DHS Sensitive Systems Policy Directive 4300A establishes DHS wireless systems policy. The wireless systems policies from the Policy Directive are provided below. The system owner should submit the documentation required by policy to the CBP AO.

CBP Policy
a. Annual security assessments shall be conducted on all approved wireless systems. Wireless security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.
b. Risk mitigation plans shall be developed to address wireless security vulnerabilities. These plans shall prioritize corrective actions and implementation milestones in accordance with defined risk levels.
c. Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless system being approved for use.
d. System Security Plans shall adopt a defense-in-depth strategy that integrates firewalls, screening routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure security solutions and secure connections to external interfaces are consistently enforced.

CBP Policy
e. Legacy wireless systems that are not compliant with CBP IT security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to CBP-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the CBP and DHS CISO, as appropriate.

Within Attachment Q1, the use of the word "shall" shall be considered mandatory only in as it applies to existing DHS policy elements.

3.0 SECURITY REQUIREMENT FOR ALL WIRELESS SYSTEMS

The WMO is in the process of finalizing *Sensitive Wireless Portable Electronic Devices*, a document that will detail mobile computing challenges and the proper security mitigations for client devices. (When finalized, this document will be included as an attachment to the DHS 4300A Sensitive Systems Handbook.) The Wireless Security Checklist in Appendix A provides configuration details.

3.1 Authentication

Authentication methods include 802.1X port-based network access control, Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) authentication, and the use of enterprise Remote Authentication Dial-In User Service (RADIUS) servers to provide authentication to user databases while providing for dynamic key management.

Administrative passwords will be strong passwords. Strong passwords contain a mixture of upper and lowercase letters, numbers, and special characters, and meet the organization's minimum password length requirements. Passwords should not be able to be easily guessed or be based on dictionary words.

3.1.a. Wireless systems SHALL employ strong authentication methods.

3.1.b. Systems SHOULD NOT operate using default factory passwords; these must be changed prior to the system being put into operational use.

3.1.c. Administrative passwords SHOULD be changed to a strong password that complies with overarching organization password conventions defined in DHS 4300A.

3.2 Confidentiality

Strong encryption, at a minimum, consists of Federal Information Processing Standards (FIPS) 140-2 certified crypto implementation using Advanced Encryption Standard (AES) 128-bit encryption and preferably using AES 256-bit encryption.

3.2.a. Wireless systems SHOULD use strong encryption to protect the confidentiality of data.

3.2.b. WLAN systems SHOULD meet the Wi-Fi Alliance Wireless Protected Access 2 (WPA2) interoperability standard that is based on the Institute for Electrical and Electronics Engineers (IEEE) 802.11i security standard.

3.2.c. The use of static keys SHOULD be avoided.

3.2.d. Dynamic key rotation SHOULD be used in conjunction with an enterprise RADIUS server.

3.3 Integrity

The integrity of wireless traffic is essential in ensuring that data have not been modified in transit, as well as protecting against man-in-the-middle attacks. The 802.11i security standard includes robust hash functions to ensure data integrity.

If an available mechanism exists that allows for cryptographic verification of the integrity of messages, then system nodes must discard all messages that cannot be verified. WiFi Alliance Wired Equivalent Privacy (WEP) is vulnerable to both replay attacks and integrity violations, and should not be used or relied upon. Message integrity can also be supplemented by use of virtual private network (VPN) communications, which provide message hashing through the use of encryption protocols.

3.3.a. Strong hash routines and security controls SHOULD be used to ensure data have not been modified in an unauthorized or accidental manner.

3.3.b. 802.11i security SHOULD be employed.

3.4 Management Control

Wireless systems must have the ability to manage devices, establish or change configurations to comply with security policy, and perform updates on software and firmware remotely if needed. Total system visibility and the ability to apply template policies are preferred. The ability to establish prioritization of network traffic based on application or data type, as well as to configure quality of service (QoS) parameters, is preferred. Security protections must not degrade or impede critical services or usability features protected by law or published policy (e.g., compliance with Section 508 of the U.S. Rehabilitation Act), as appropriate. Likewise, assistive devices and/or software must not degrade or circumvent established system security controls. Any system modifications require appropriate security review. In addition, configuration management should be addressed in the organization's System Security Plan for that system.

3.5 Physical Security

Physical access can allow attackers to reconfigure access points (AP), interrupt or deny service, and/or create additional points of access to the network. Conducting routine inspections and looking for suspicious behaviors will reduce the likelihood of equipment theft. Because wireless networks are susceptible to eavesdropping from a distance, guards and users alike should report any suspicious individuals in or around the facility to the appropriate security personnel.

3.5.a. Each wireless infrastructure device SHOULD be secured in a locked enclosure or space that is resistant to tampering, theft, and unauthorized access to console ports, power supplies, and reset buttons.

3.5.b. Guards who routinely patrol the facilities SHOULD visually inspect AP enclosures.

3.5.c. Guards SHOULD be made aware of the importance of these devices and the likelihood of potential theft or tampering, as well as be able to recognize signs of tampering or unauthorized individuals attempting to access the enclosures.

3.6 Default Configuration Settings

Usually, wireless systems are initially configured with default vendor settings that are commonly known. These settings can include network information such as default channel or modulation; security information such as network name, encryption methods, pass phrases, or keys; and systems management information such as administration usernames, passwords, management port numbers, and default running application services.

3.6.a. All sensitive settings for wireless systems SHOULD be changed to protect against unauthorized intrusion and modification of system settings.

3.7 Denial of Service

Wireless communications are susceptible to interference, eavesdropping, Layer 1 RF jamming, and Layer 2 denial of service (DoS) attacks. Monitoring is performed using sensors, systems management tools, or mobile handheld security and surveying tools to detect and locate RF threats.

Wireless links are more susceptible to jamming attacks than wired links. These types of attacks can be mitigated only through contingency planning. It is important to have an alternative method of communications available so that in the event of a jamming attack, service can be resumed—providing availability until the jamming attack can be stopped. Because these vulnerabilities inevitably exist, it may be necessary to ensure that wireless systems are not used for certain mission-critical applications if redundant or on-demand communication mechanisms cannot be put in place. Sample security controls are provided in Table 1. Note that wireless security is performed at the Physical and Data Link Layers while Layers 3 and higher of the Open Systems Interconnection (OSI) model may employ a variety of security protocols.

3.7.a. Sensitive wireless systems SHALL have the capability to detect, identify, and locate attacks, as well as capture transmissions for wireless forensics.

Table 1: Open Systems Interconnection (OSI) Layer Security Considerations

OSI Layer	Security Considerations
Application	Detect and prevent malicious code, viruses, and other malware applications. Mitigation tools include firewalls, anti-virus, and intrusion detection applications.
Presentation	Protect data files by cryptography (e.g., file password encryption).
Session	Protect system from port exploits and validate digital certificates. Secure Sockets Layer (SSL) operates between the Session and Transport layers.
Transport	Provide authentication and secure end-to-end communications. Encryption protocols include Secure Shell (SSH-2) and Simple Key Management for Internet Protocols (SKIP).
Network	Protect the routing and the forwarding protocols. The Internet Protocol Security (IPSec) standard provides multiple and simultaneous tunnels rather than the single connection limit of the lower layer encryption standards.

OSI Layer	Security Considerations
Data Link	Protect the Media Access Layer (MAC) from masquerade, DoS, impersonation, and Address Resolution Protocol (ARP) threats. Common encryption protocols include the Point-to-Point Tunneling Protocol (PPTP) and the Layer 2 Tunneling Protocol (L2TP).
Physical	Prevent jamming and DoS attacks in the air medium.

3.8 National Information Assurance Partnership Common Criteria Security Validations

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative begun to meet security testing needs of both IT consumers and producers. NIAP is a collaboration between the NIST and the NSA to add a level of trust in IT products and networks. The Common Criteria define a set of validated IT requirements that can be used in establishing security requirements for products and systems. The Common Criteria also define Protection Profiles (PP), or implementation-independent, standardized sets of security requirements based on particular needs. PPs are available for products within a wireless security architecture. Additionally, a Security Target (ST) can be developed to measure security threats, objectives requirements, and summary specifications of security functions. STs are developed for specific products with specifically identified targets of evaluation. The STs may or may not conform to PPs to form a basis for evaluation.

3.8.a. CBP administrators SHOULD carefully evaluate products to ensure that security validations have been performed and that the products conform to commonly used PPs.

3.8.b. The NIAP validation reports SHOULD be examined carefully to ensure that all required targets of evaluation are validated to an appropriate level of robustness.

3.9 Disabling Non-Secure or Non-Essential Ports and Protocols

Protocols that send clear text passwords or otherwise do not use a secure protocol (e.g., Telnet, HyperText Transport Protocol [HTTP], Simple Network Management Protocol [SNMP] v1/2, and Cisco discovery protocol [CDP]) should not be used as a means of in-band device management. A possible secure configuration is to encapsulate insecure protocols inside encrypted tunnels; examples include IPSec and Secure Socket Layer (SSL) based VPN. In accordance with CBP policy, only FIPS 140-2 or NSA type 1 and 2 validated products are permitted to encrypt sensitive data.

3.9.a. Ports, protocols, and services that are enabled by default and are not essential to mission requirements SHOULD be disabled.

3.9.b. APs SHOULD be tested at least quarterly for compliance with the organization's list of approved ports and protocols.

3.10 Audit Logs

As audit tools for wireless systems mature, DHS may consider centralized audit solutions.

The integrity of audit logs is essential for Emergency Response Teams (ERT) to understand attack methodologies and is essential for legal proceedings. Audit logs serve as evidence that an intrusion has taken place and may help identify what has occurred during system troubleshooting. The integrity of audit logs should be protected by synchronizing the time

clocks on all bridges, remotely recording all log information, securing the audit trail logs, providing strict access control for logs, and recording all log access to preserve the chain of custody. In addition, if mechanisms for digitally signing log files are available, they should be implemented. CBP auditing policies should be implemented and adhered to.

3.10.a. Systems SHOULD be configured to create audit logs and capture important events such as successful and unsuccessful administrator logins, client device access attempts, client device MAC addresses, access violations, associations, disassociations, ports and protocols used, and user activities.

3.10.b. Log entries SHOULD be captured by a remote system on the wired network that has robust security, making the organization's overall network less vulnerable to attack.

3.10.c. Audit log management SHOULD be addressed in the organization's System Security Plan for that system.

3.11 Login Timeouts

Timeouts can be implemented on the console so that after a period of time has elapsed, console port access is disabled. This functionality allows only those with the ability to power cycle the device to conduct console port configuration.

3.11.a. Administrative login timeouts SHOULD be implemented on a system's management interface so that after a period of inactivity, administrative sessions automatically logout.

3.12 Restricting Access During Off-Hours

If a wireless system is being operated in an environment where access to the network is needed only during normal business hours, users' access should be regulated via role-based access controls. These access policies would be mapped to usage policies specifying a group of users that could access the network only during normal business hours and restrict access during nights and weekends.

3.13 Software and Firmware Updates

The NIST National Vulnerability Database (NVD) "… NVD is a comprehensive cybersecurity vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources."[1] When possible, test the updated firmware in a nonproduction environment to validate functionality before a production rollout. System audit policy and guidance is provided in CBP Information Systems Security Policies And Procedures Handbook (HB 1400-05C).

3.13.a. Security updates and patches SHOULD be applied to all system devices to ensure that up-to-date firmware and software that protects these systems against known vulnerabilities is installed.

3.13.b. Vendor-related and security vulnerability alert sites SHOULD be monitored frequently.

[1] http://nvd nist.gov

3.14 Network Intrusion Detection System

The goal of an intrusion detection system (IDS) is to detect anomalies and monitor wireless system links. Anomalies may include, but are not limited to, increased utilization, abnormally low utilization, multiple login attempts, attack signatures, off-hour logins, and other detected variances from the system baseline. It is necessary to thoroughly test automated reactive IDS network protection mechanisms before their implementation; however, their use should be considered to provide rapid response to wireless intrusions.

3.14.a. A network IDS sensor SHOULD monitor the wireless system links to detect anomalies.

3.14.b. Additionally, host-based IDS sensors SHOULD be employed to monitor system and administrator level activities.

4.0 WLANS—SECURING THE AP

The following measures should be implemented to ensure secure use of WLAN APs. See Appendix A for specific requirements and Appendix B for an example enterprise implementation diagram.

4.1 WLAN Network Naming Conventions

WLANs contain a network name that identifies the network to client devices. In 802.11-based WLAN networks, this name is referred to as the Extended Service Set Identifier (ESSID). It is difficult to keep this network name a secret (i.e., known only by valid users) because it is transmitted unencrypted as a part of protocol management messages and can easily be intercepted by attackers.

4.1.a. The WLAN network name SHOULD be changed from the default name to a unique name that does not reveal its affiliation to DHS operations or organizations.

4.1.b. The ESSID name SHOULD NOT be associated with organizational function or identity to avoid advertising the network's identity or function to potential attackers.

4.2 Disable ESSID Broadcasting

In certain physical environments or operational areas, disabling the ESSID in broadcast beacons may be important, so that APs do not advertise the existence of a WLAN in the coverage area. War-driving is the act of driving, walking, or flying within a geographical area while employing wireless equipment to detect the presence of WLANs and attempting to map the locations in which these networks are discovered. Disabling the ESSID in the beacons prevents advertisement of the private WLAN to war-driving software tools and can help limit attackers' awareness. An attacker listening for probed request and response packets can still capture a WLAN's ESSID, but typically, this information is collected by determined hackers rather than those who pass by while conducting a war-drive.

4.3 WLAN Authentication

Authentication and authorization can be enforced on WLANs by using 802.1X—port-based access control, and EAP authentication methods. These technologies combine to ensure that access is provided only to clients who have supplied valid credentials. Many EAP

implementations exist for WLANs and are being incorporated into WPA and WPA2 interoperability certification processes.

4.4 Over-the-Air Encryption Recommendations

A properly configured WLAN should use the strongest over-the-air encryption mechanisms available to protect the confidentiality of traffic traveling across wireless links. WPA2 and the IEEE 802.11i security standard in Robust Security Network (RSN) mode address virtually all the security concerns identified within WEP, as well as remaining concerns identified in WPA, relying on the AES for confidentiality and integrity services. Even when dynamic 802.11i WPA2 Enterprise is implemented, additional layers of security may need to be implemented to protect systems so that they operate under a defense-in-depth approach. Defense-in-depth is the process by which a single vulnerability cannot negatively impact the entire system. The use of multiple layers of defense helps to protect the wireless system from a number of individual attacks thus raising the cost and complexity to the attacker. Table 1 details the OSI layers; again, wireless security is only performed at Layers 1 and 2. Layers 3 and higher may employ a variety of security protocols.

Non-standardized wireless products implementing proprietary techniques and protocols must implement FIPS 140-2 compliant AES strong encryption and robust authentication routines. Non-standard systems require CISO waiver and exemption approval. A comprehensive list of validated products can be found at http://csrc.nist.gov/cryptval/140-1/140val-all.htm. Standards, protocols, and products approved for use can be found within the DHS Technical Reference Model (TRM) at https://interactive.dhs.gov/suite/portal.do?$p=1485.

4.4.a. Static WEP encryption offered by 802.11-based networks SHOULD NOT be used.

4.4.b. WLAN systems SHOULD implement a NIST FIPS-approved mode with AES encryption.

4.4.c. FIPS 140-2 validated commercial off-the-shelf (COTS) products SHOULD be considered as preferable to those that have not been validated.

4.4.d. Systems that provide per-session dynamic RC4 keys, such as dynamic WEP, temporal key integrity protocol (TKIP), and WPA, SHOULD NOT be adopted.

4.5 OSI Layer 2 and Layer 3 Security Considerations

Layer 3 security methods leave MAC hardware addresses and some routing information exposed and may allow man-in-the-middle attacks and peer-to-peer attacks against other nodes on the wireless segment. However, these Layer 3 methods are often easy to implement and manage. In environments where other mitigations are in place, such as secured physical perimeters or strong mutual authentication, a Layer 3 approach may be sufficient. Layer 2 security methods protect addresses and most routing information, limiting exposure to man-in-the-middle attacks and peer-to-peer-attacks. However, Layer 2 methods are often proprietary, may limit routing capabilities, may limit system performance, and may have interoperability and scalability concerns. Use of Layer 2 security technology (e.g., IEEE 802.11i) does not preclude the use of defense-in-depth protection at other layers, including support for Layer 3 or higher security technologies, e.g., a VPN or IPSec solution. The OSI Layer at which security methods are implemented is not the only technical consideration in determining the robustness of a security method. Section 3.0 of this document provides greater OSI layer detail.

4.5.a. The wireless system risk profile and the mitigation options SHOULD be evaluated in their entirety so that the appropriate balance is achieved among all system requirements.

4.6 Identification and Authentication Recommendations

Identification and authentication recommendations are listed below:

4.6.a. Authentication (username/password, public key infrastructure [PKI] certificate, biometrics, or one-time-password, etc.) SHOULD be implemented as an access control mechanism for authorizing system access to WLANs.

4.6.b. WLAN systems SHOULD implement 802.1X access control and EAP-TLS mutual authentication.

4.6.c. If identification and authentication cannot be enforced at the AP, then a firewall, captive portal, or other appliance SHOULD be implemented that denies network access unless proper credentials are provided.

4.7 AP Configuration Management

Additionally, the configuration of every AP must be stored remotely and properly documented. These measures will assist in disaster recovery procedures, facilitate automated configuration management procedures, and help with troubleshooting procedures. Some architectures may implement thin APs, such as those conforming to Cisco's Lightweight Access Point Protocol (LWAPP), where no default configuration information is stored on the AP and even unauthorized APs are automatically configured to conform to policy. Such architectures are recommended as inherently more secure if they meet system requirements.

4.7.a. APs SHOULD be routinely checked to ensure they have the correct configuration and are in compliance with the security policy.

4.7.b. Enterprise-grade APs SHOULD be integrated into a secure network management framework.

4.7.c. Administration access SHOULD only be permitted from trusted wired interfaces on the AP or by direct console port access.

4.7.d. Access to administration settings SHOULD never be permitted from either open network interfaces or wireless connections.

4.7.e. Access SHOULD only be provided when physically connected to a management network.

4.8 AP Radio Coverage Recommendations

Below are AP radio coverage recommendations:

4.8.a. Each AP's RF power output SHOULD be adjusted to the minimal level necessary to provide optimal in-building coverage with minimal external propagation.

4.8.b. The following elements SHOULD be considered for determining coverage performance: signal strength, noise level, and signal-to-noise ratio.

4.8.c. Channel usage SHOULD be coordinated and designed with care to avoid overlap and interference.

5.0 WLANS—SECURING THE PERIMETER

Perimeter security devices include firewalls, VPN concentrators, and IDSs. These devices provide access control, encryption and decryption for message confidentiality, and the detection of security policy violations. The interconnection point between the wired and the wireless network should be segmented with perimeter security devices to ensure that all devices operating on the WLAN comply with the CBP IT Security Policy.

5.1 Wired/Wireless Perimeter Traffic Filtering

Below are wired/wireless perimeter traffic filtering procedures:

5.1.a. Traffic traveling from the wireless network to the wired segment SHOULD be restricted by a firewall or other filtering device to authorized users only.

5.1.b. Traffic traveling from the wireless network to the wired network SHOULD be restricted to specific machines, specific ports, and specific protocols to help prevent unauthorized access violations.

5.1.c. Traffic traveling from the wired segment to the wireless segment SHOULD be restricted to only administrative functions (such as AP management) and allowed on a host-by-host basis.

5.2 Using Network-Based IDS

The goal of an IDS is to detect anomalies. Anomalies may include, but are not limited to, increased utilization, multiple login attempts, accessing of the systems in unusual ways, attack signatures, off-hour logins, and other detected variances from the system baseline. System administrators should be aware that sophisticated hackers may attempt intrusions as decoys or as a means to learn of incident response methods.

5.2.a. IDS sensors SHOULD be placed at ingress and egress points or supported within the wired or wireless perimeter firewall device so that anomalies can be detected.

5.2.b. Additionally, host-based IDS sensors SHOULD monitor any administrator-level activities.

5.2.c. Automated network defense mechanisms require significant field adjustments and SHOULD be thoroughly tested before their implementation.

5.2.d. IDSs SHOULD incorporate location-aware capabilities to speed incident response and forensic capabilities to identify and track modified information.

5.3 VPN Tunnel Termination

It is important that wired-side traffic be unencrypted only on a secured intranet network so that IDS sensors, anti-virus gateways, and network management systems can interpret and interact with incoming traffic.

5.3.a. VPN concentrators SHOULD be placed at wired and wireless ingress and egress points so that they provide end-to-end encryption from the wired network to the client and so that information passes over the wired network in an unencrypted format.

5.3.b. To avoid increased risks of vulnerable points of entry, multiple tunnels or split tunnels SHOULD NOT be allowed at the same client device.

6.0 WLANS—IMPLEMENTING WIRELESS INTRUSION DETECTION SYSTEMS

Wireless intrusion detection systems (WIDS) incorporate remote sensors that listen to the airwaves and report findings to a WIDS management appliance. These systems scan the airwaves to detect malicious activities such as installation of unauthorized wireless hardware, AP outages, wireless client device hijacking, DoS attacks, unauthorized ad hoc or peer-to-peer networks, and other WLAN-specific vulnerabilities.

6.0.a. Mobile spectrum analyzers SHOULD be used to perform troubleshooting, traffic and interference analysis, and unauthorized device detection to identify non-WLAN devices that operate in the same frequency bands, e.g., Bluetooth devices, cordless telephones, and microwave sources of interference.

6.0.b. An Incident Response Plan SHOULD be developed and maintained as part of the System Security Plan for each wireless system, as appropriate, and executed when vulnerabilities, threats, and attacks are discovered.

6.1 Unauthorized APs and Other Unauthorized Wireless Devices

An adversary who gains physical access to a wired local area network (LAN) can connect an unauthorized AP device and continue exploiting the network from outside its secure perimeter. In addition, authorized users may also install unauthorized devices for convenience and unintentionally expose the physical LAN to new attack vectors. These user-installed devices are typically not compliant with the organization's security policy and are easily compromised by attackers. Reference the System Security Plan for incident response details.

6.1.a. Unauthorized devices severely weaken the organization's security posture and SHOULD be taken seriously if found.

6.1.b. Incident response teams SHOULD perform a thorough investigation whenever an unauthorized wireless device is detected.

6.2 Using WIDS Location Services

Rudimentary location information will simply inform administrators that the attack is within the range of a particular sensor. This could be a large area, or multiple floors of a building, and could make it difficult to locate the point of attack. More advanced WIDS sensors may provide triangulation information that assists administrators in identifying attacker locations based on a two-dimensional map of the physical network.

6.2.a WIDS sensors SHOULD be location aware and should offer location information so that administrators can respond appropriately to attacks.

6.3 Approaches to Intrusion Detection

Signature-based WIDS scan for known attack signatures. These systems are only as good as their latest signature update and therefore should be updated regularly. Although signature-based WIDS systems are not highly effective against new or zero-day attacks, they actively defend against known vulnerabilities generating very few false-positives (also know as false alarms). A complementary approach to WIDS scanning is to implement anomaly detection. These WIDSs require capture of a system baseline. They operate by comparing the current system against the system baseline. Anomaly-based WIDSs are more effective against new attacks than signature-based WIDSs but require a large amount of system resources on the WIDS management appliance. In addition, anomaly-based WIDSs produce more false positives.

6.4 Wired-Side Unauthorized AP Detection

Wired-side WIDS scans for unauthorized APs are also possible but these systems can be fooled easily. Wired-side WIDS probe the wired network for known wireless devices based on the manufacturer portion of the unauthorized devices' MAC addresses. While this can help organizations rapidly identify unauthorized hardware installed by internal users, it will not detect unauthorized hardware that has modified MAC addresses. Hackers and internal users that do not want to be detected by these types of WIDS can simply modify the unauthorized hardware's MAC address. A defense-in-depth security approach that includes methods such as banner grabbing, port scans, and stack analysis may be necessary to effectively implement a wired-side WIDS.

6.5 Disparate Wireless Communications Device Monitoring

The effectiveness of a WIDS is measured by the number of attacks it can detect, the number of technologies it supports, and the diversity of frequencies and/or protocols it supports. Wireless communications devices that operate under alternative methods of communication may be used unknowingly in DHS areas of responsibility. WIDS must be able to detect unauthorized or unapproved internally controlled devices.

> 6.5.a. Devices such as WLANs with altered frequencies, cellular modems, Bluetooth, Wireless Microwave Access (WiMAX), etc. SHOULD be passively monitored through the use of specially configured WIDS sensors whenever possible.

6.6 Wired/Wireless IDS Integration

Sophisticated attackers may use a combination of wired and wireless intrusions. Attack identification and asset modification identification may require passing anomaly or signature information between wired and wireless IDSs.

6.7 Wireless Intrusion Prevention Systems

Wireless Intrusion Prevention Systems (WIPS) with active forensic countermeasure capabilities are emerging within the WLAN industry. Such systems can actively deny service to suspected intruders, can quarantine suspected intruders to benign segments of the network, or can even perform active forensics on the suspected intruder to learn as much as possible about the intruder's identity, methods, and goals. However, because of privacy concerns, such countermeasures are not necessarily legal. Thus, only passive intrusion detection methods should be deployed. WIPS should include the capability to identify the network switch port to

which an unauthorized device is connected and to disable that network port via wired-side network management mechanisms.

7.0 WLANS—INFRASTRUCTURE CONSIDERATIONS

WLAN-specific network infrastructure devices consist of network equipment located on the wired network that support such WLAN operations as bandwidth management, Internet Protocol (IP) address assignment, and identity management systems. Bandwidth management addresses WLAN availability and reliability and is supported by traffic-shaping appliances or routing infrastructure that provides QoS or class-of-service (CoS) guarantees to WLAN users. Dynamic Host Control Protocol (DHCP) servers typically provide IP address assignment to wireless client devices. RADIUS has emerged as the dominant identity management service supporting WLAN identification and authentication.

Additional security information can be found in the DHS IT Security Architecture Guidance documents. This three-volume set provides DHS requirements and industry best practices regarding the security policies, procedures, and technical security capabilities needed for the DHS enterprise network infrastructure.

7.1 Managing IP Address Assignment

Through its DHCP servers and using DHCP clients, the network is open to network reconnaissance and DHCP attacks. If an attacker can establish a communications session (i.e., associate) with an AP, that attacker will be provided automatically with an IP address if DHCP is enabled. This makes the attacker's job easier and provides that attacker with network information such as IP address range, network topology, and IP subnet information. Any attacker with a valid IP address can launch OSI Layer 3 attacks against other nodes on the wireless segment. For standard DHCP, client devices blindly trust any machine that responds to a DHCP address request because no authentication is provided. Attackers can set up an unauthorized DHCP server on their client device and provide unauthorized DHCP services to other unsuspecting client devices to hijack sessions or conduct man-in-the-middle attacks. Static DHCP does not solve this problem completely because an attacker can spoof his/her MAC address and receive useful DHCP information. Implementing static rather than dynamic DHCP services does not prevent an attacker from using an unauthorized DHCP server to compromise clients.

The use of strong access controls can mitigate the risks associated with a standard DHCP configuration. Alternative mitigations are to implement either static IP addresses or a non-standard secure DHCP service that allows for mutual authentication. Attackers may still be able to scan network traffic to determine the IP address, subnet, and network topology, but this is mitigated by the use of encryption. DHCP with 802.1X authentication is an acceptable risk mitigation strategy.

7.2 Identity Access Management Systems

Identity access management systems are needed to effectively operate WLANs. RADIUS, which was designed initially to support remote dial-in users, has been adapted to support WLAN authentication. RADIUS often has built-in support for Microsoft Active Directory (AD), Novell Directory Service (NDS), Windows Domain Authentication, Lightweight Directory Access Protocol (LDAP), and other identification and authentication databases.

7.2.a. Wireless nodes such as APs and WLAN switches SHOULD be able to support strong authentication and authorization services that verify identity before granting access to the network.

8.0 FIXED ACCESS WIRELESS NETWORKS—BRIDGE COUNTERMEASURES

A fixed access wireless network is a network covering a wide geographical area, involving several point-to-point or point-to-multipoint nodes. Applications of this technology are employed when interconnecting two or more locations with RF line-of-sight (LOS) or near-LOS devices called bridges. Point-to-point connections typically involve the use of highly directional antennas that can be tuned to span great distances, as long as the area between the two points is free of obstructions. Point-to-multipoint configurations involve a master bridge located in a central position and multiple client bridges making up a hub-and-spoke topology. The master bridge typically employs an omni-directional antenna.

Bridges are typically employed in a fixed-access wireless network to provide OSI Layer 2 connectivity between sites. It is important to secure bridged networks because beam scattering may allow unauthorized users to monitor the communications. Bridge links must be secured by encryption and access controls. Bridge devices must provide strong access controls, authentication, and configuration management. To provide defense in depth, additional network layer devices should be installed at site ingress and egress points.

8.0.a. Bridge devices SHOULD be configured to accept connections only from other bridge devices and not from client devices.

8.1 Bridge Link Confidentiality

Bridges must provide a mechanism to ensure that information is not made available or disclosed to unauthorized individuals, entities, or processes. A list of FIPS 140-2 validated products can be found at http://csrc.nist.gov/cryptval/140-1/140val-all.htm. Standards, protocols, and products approved for use can be found within the DHS TRM at https://interactive.dhs.gov/suite/portal.do?$p=1485.

8.1.a. FIPS 140-2 validated products SHOULD be selected to secure link-level communications between bridges.

8.1.b. If the bridges selected do not support FIPS-approved algorithms, then an algorithm SHOULD be selected according to industry best practices.

8.2 Mutual Authentication of Authorized Bridges and Pairing Arrangements

Bridges provide a mechanism to mutually authenticate each other before communications are established. This is done to ensure man-in-the-middle attacks are mitigated.

8.2.a. Bridges SHOULD provide a mechanism to mutually authenticate each other before communications are established and periodically during the communications.

8.2.b. Bridges SHOULD identify themselves by supplying a unique identifier that cannot be easily spoofed or duplicated.

8.2.c. Lists of authorized bridge partnerships SHOULD be maintained on the devices and documented by IT personnel.

8.3 Bridge Radio Coverage Recommendations

The following elements should be considered for determining outdoor coverage performance: antenna gain, transmitter power, receiver performance, cable losses, and environmental structures. Reference the System Security Plan for greater detail.

8.3.a. Bridge RF power output SHOULD be adjusted to the minimum level necessary to provide LOS communications.

8.3.b. Site survey documentation SHOULD be kept in a secured location and made available to the ERT for incident response.

8.3.c. Site survey documentation SHOULD be kept in a secured location and made available to the ERT for incident response purposes.

8.4 Restricting Bridge Communications Based on MAC Addresses

MAC addresses are sent in the clear and therefore can be captured and eventually spoofed by attackers. Regardless, this security control prevents accidental connections and forces attackers to perform additional work to compromise the system.

8.4.a. MAC-address-based access control capabilities SHOULD be configured on all bridges so that any connection from any other bridge that is not specifically allowed will be denied by default.

9.0 WWANS—COMMERCIAL SERVICES COUNTERMEASURES

A WWAN is a network covering a wide geographical area, involving a vast array of clients. Commercial service WWANs, such as cellular telephone service, packet radio networks, Cellular Digital Packet Data (CDPD), or WLAN hotspots, should be treated as untrusted, public networks. Commercial data services are typically used in a highly mobile WWAN to provide OSI Layer 3 connectivity between an end-user device and an enterprise server. CBP does not have control over the commercial service infrastructure, its configuration, operation, maintenance, or personnel with access to the infrastructure or management systems.

Security methods implemented on WWANs that are free or fee-for-service commercial networks should not be relied on for enterprise security. The WMO is in the process of finalizing Sensitive Wireless Portable Electronic Devices, a document that will detail mobile computing challenges and the proper security mitigations for client devices. (When finalized, this document will be included as an attachment to the DHS 4300A Sensitive Systems Handbook .) Data communications via commercial services WWANs should always be secured using strong encryption, authentication, and access controls.

9.0.a. Additional defense-in-depth layers of protection SHOULD be implemented at DHS networks and end-user device ingress and egress points across untrusted commercial services WWANs.

9.1 Commercial Services WWAN Link Confidentiality

All data systems accessible via commercial services WWANs must provide a mechanism to ensure that information is kept confidential as it passes over the air interface and as it passes

through the commercial service or public wired network. A list of FIPS 140-2 validated products can be found at http://csrc.nist.gov/cryptval/140-1/140val-all.htm.

9.1.a. FIPS 140-2 approved algorithms SHOULD be used to secure link-level communications between servers and client devices.

9.1.b. FIPS 140-2 validated products SHOULD be selected in preference to nonvalidated products.

9.1.c. If the products selected do not support FIPS-approved algorithms, then an algorithm SHOULD be selected according to industry best practices.

9.1.d. Acquisition of a FIPS 140-2 validated product SHOULD be implemented at each endpoint to provide secure communications.

9.2 Mutual Authentication of Authorized Data Services

Authorized data servers and clients should provide a mechanism to mutually authenticate one another before communications are established and periodically during the communications. This is done to ensure man-in-the-middle attacks are mitigated. Digital certificates are commonly used to ensure mutual authentication between parties, mitigating the risk of man-in-the-middle attacks.

10.0 WIRELESS PERSONAL AREA NETWORKS

WPANs are the least secure of the wireless systems addressed in this handbook. WPANs are typically established in an ad hoc, peer-to-peer manner, have no static infrastructure, and are often undetected. Users often leave WPAN systems in their default configuration, which allows insecure operation. The encryption provided by standard Bluetooth products is not sufficient for protecting sensitive information. Operation of these noncompliant systems requires an approved waiver or exception from the CISO, as appropriate.

10.1 WPAN Ad Hoc Networks

WPAN client devices should not be allowed to create ad hoc networks. If the DHS CISO approves the use of an ad hoc network, the system owner shall provide documentation detailing system security in accordance with DHS and CBP Policy and IT architecture guidance. The DHS IT Security Architecture Guidance documents (volumes I–III) provide DHS requirements and industry best practices in regard to the security policies, procedures, and technical security capabilities needed for the DHS enterprise network infrastructure.

10.1.a. Strict configuration of ad hoc networks on client devices SHOULD be enforced.

10.1.b. These networks SHOULD be tested at least monthly for compliance and SHOULD be disabled immediately when they are no longer necessary.

10.2 Identification of WPAN Capabilities for Risk Assessment

It is important that IT security managers identify the WPAN capabilities in all personally owned devices present within the organization to educate users on the risks of these devices and to mitigate vulnerabilities through effective countermeasures. Users must ensure that device Bluetooth, IR, and RF ports are disabled and rendered inoperable before their entry into sensitive environments to prevent the sharing of information with untrusted and/or unauthorized users.

10.2.a. Appropriate awareness training SHALL be provided.

10.2.b. Any appropriate wireless security awareness training SHOULD be included in the annual training provided by CBP.

10.2.c. Any WPAN capabilities that are not required by the user SHOULD be deleted or disabled.

10.2.d. Security personnel SHOULD be properly trained to recognize PAN-capable devices and be familiar with disabling PAN functions in those devices.

10.2.e. Security personnel SHOULD provide assistance to users by helping them disable any unwanted PAN functionality.

10.3 Device Power Requirements

Device power requirements will vary depending on the application being used. The power output level should be chosen that provides the minimum needed to support the particular wireless application in use. This limits the distance from which eavesdroppers can listen in and/or stage attacks. Bluetooth WPANs provide three power output classes. Class 1 devices provide 100 milliwatts (mW) of power output, Class 2 devices provide 1–2.5 mW of power output, and Class 3 devices provide the lowest power output at 1 mW.

10.3.a. The RF power output of devices SHOULD be limited to only that which is needed for communication with authorized user devices.

10.4 Bluetooth Device Communication Risks and Recommendations

During Bluetooth communications, critical information is passed between devices during and after pairing, which, if captured, could allow an attacker to gain full remote access to the WPAN device. For more information on Bluetooth security reference NIST SP 800-48 Wireless Network Security 802.11, Bluetooth and Handheld Devices (Nov 2002).

10.4.a. IT security managers SHOULD ensure that Bluetooth communications are conducted in an environment where information exchanged cannot be captured by eavesdroppers.

10.4.b. Communication SHOULD be restricted to private areas where there is limited RF signal propagation.

10.4.c. To prevent devices from advertising themselves to would-be attackers, devices SHOULD be configured for the non-discoverable mode unless the user is in the process of pairing Bluetooth devices.

10.4.d. To avoid increased risks of vulnerable points of entry, multiple or split communications paths SHOULD not be allowed for the same client device.

10.5 Personal Identification Number Protection

WPAN device communications typically relies on the devices' hardware address for identification and a personal identification number (PIN) for authentication. If possible, PINs should be generated randomly, avoid identifiable patterns, and be sufficiently long to ensure that the PIN is not easily ascertained by unauthorized users. For example, Bluetooth security is only

as strong as the PIN the user selects and will typically range between 4 and 16 bytes. Avoid non-configurable devices.

Devices that are not configurable typically have a hard-coded manufacturer PIN that creates a vulnerability that an attacker can exploit. For example, attackers can determine a hard-coded PIN by reading the device's user manual or by inspecting the device while left unattended. These devices also do not allow the user to disable discovery mode. While eavesdropping on a Bluetooth mouse would only provide an attacker with X and Y coordinates, eavesdropping with an ear-bud microphone would allow the attacker to intercept a complete telephone conversation.

10.5.a. The Bluetooth PIN is exposed during the pairing function and therefore SHOULD be unique while at the same time not exposing important organizational information.

10.5.b. IT security managers SHOULD avoid deploying or permitting the use of wireless devices that do not provide the necessary user interface to allow PINs to be changed or reconfigured (e.g., Bluetooth mice, ear-bud microphones, keyboards).

10.6 Disabling Unwanted Profiles

One example of a profile for Bluetooth WPANs that could potentially expose sensitive information is the Object Exchange Protocol (OBEX). This profile, if exploited, could provide an attacker with unrestricted file access and file push capabilities. Theft of information from a wireless device through a Bluetooth connection is commonly known as bluesnarfing.

10.6.a. IT security managers SHOULD disable unwanted WPAN profiles to reduce the points of access an attacker might exploit.

10.6.b. Organizations SHOULD operate under the principle of least privilege and only enable functionality that users absolutely require for day-to-day operations.

10.6.c. Profiles that can expose sensitive information SHOULD be used extremely conservatively.

10.7 Device Security Modes

The strongest security mode should be chosen to protect WPAN-enabled devices. In Bluetooth, "Mode 3" provides the best security by offering link-level encryption between all paired devices. If WPANs are used to provide Transport Control Protocol (TCP)/IP services, then VPN encryption should be used as an extra layer of security. The Bluetooth 1.2 specification offers stronger authentication by supporting the Diffie-Hellman key exchange and is protected against offline brute-force PIN attacks.

10.7.a. Devices that support Bluetooth 1.2 SHOULD be selected in preference to those that support only Bluetooth 1.1.

10.8 Avoid Social Engineering

It is possible for unauthorized users to send unsolicited messages to Bluetooth-enabled devices using a technique called bluejacking. These unsolicited messages could be carefully crafted to coerce users into providing information such as the Bluetooth PIN that could compromise system

confidentiality. Malicious code and unsolicited messages may be received through other means as well, such as via cellular telephone Multimedia Messaging System (MMS) messages.

Social engineering is the art of prying information out of users via alternative and often nontechnical methods that exploit a natural human tendency to trust. This trust is exploited to gain access to a target system without actually breaking into the system. To defend against these types of attacks, users need to be made aware of the types of attacks that occur and how often these methods are used. Many attacks commonly require a user to "accept" an unknown message.

10.8.a. Users SHOULD be instructed on how to detect social engineering attacks and to verify the identity of persons and/or information they receive, rather than applying blanket levels of trust.

10.8.b. Users SHOULD report any unusual activities (e.g., harassment, solicitation, or social engineering attacks) to the appropriate security personnel or other incident response entity.

11.0 INTEROPERABILITY

Organizations requiring highly mobile staff operating across many physical locations, mission groups, agencies, and commercial networks may require a wireless infrastructure that allows for interoperable mobile computing. Several commercial associations and Federal Government interoperability groups alike investigate vendor products and rate compliancy based on published standards. A list of FIPS 140-2 validated products can be found at http://csrc.nist.gov/cryptval/140-1/140val-all.htm. Standards, protocols, and products approved for use can be found within the DHS TRM at https://interactive.dhs.gov/suite/portal.do?$p=1485.

11.1 Interoperability Concerns

In light of interoperable certifications, certified wireless equipment and respective security implementations for specific networks may have different configurations than other networks of interest and may require additional means for interoperability among multiple networks. For example, VPN clients and servers from different vendors typically have problematic communications interoperability. Aside from architectural concerns, usage policy may generate transitory trust issues among external users. Consequently, CBP should coordinate with the WMO in specifying, designing, and establishing wireless networks for purposes of interoperability. The WMO is the central coordinator with regard to cross organizational interoperability issues and may need to perform research and coordination with respect to other wireless-enabled components or agencies during the system design process to ensure that interoperability concerns are met appropriately.

11.2 Roaming Implications

As wireless networks increase in density, enterprise applications employing wireless connections are also expected to gain popularity. Many of these emerging technologies take advantage of multiple APs, such as Wireless Voice over IP (W-VoIP), location-based services, Real-time Location Sensing (RTLS), and Mobile IP. These technologies maintain connections to one or

more internally or externally owned APs, otherwise known as roaming. To be properly used, roaming services often require a specifically defined architecture.

11.3 Interoperability and Roaming Standards

Wireless architectures ideal for interoperable communications among coordinating organizations incorporate products designed with wireless communications standards such as IEEE 802.11 a/b/g, security standards such as IEEE 802.11i, and interoperability certifications such as Wi-Fi Alliance WPA2.

IEEE 802.21, the Media Independent Handoff Working Group, is an emerging interoperability standard for communication among IEEE 802 and non-802 standard equipment. The Unlicensed Mobile Access (UMA) technology alliance is developing leading interoperability specifications for communications roaming across cellular, WLAN, and Bluetooth systems. The use of standards and industry certifications increases the probability of multiple organizations' systems working together with minimal user intervention when changing networks.

To alleviate trust concerns or incompatible networks, it is technically possible for an organization to create a guest network in a "Demilitarized Zone" for outside users to obtain access to external systems. However, guest access via DHS wireless systems is prohibited. CBP may need to develop memoranda of understanding with external systems if a more formal link is established between systems. Currently, there is no single accepted interoperability solution. Management may require adherence to interoperability standards in the future.

Appendix A
Wireless Security Checklist

APPENDIX A: WIRELESS SECURITY CHECKLIST

Mobile Feature/Configuration	Required	Recommended
Security Requirements for All Wireless Systems		
3.1 Authentication		
3.1.a. Wireless systems SHALL employ strong authentication methods.	X	
3.1.b. Systems SHOULD NOT operate using default factory passwords; these must be changed prior to the system being put into operational use		X
3.1.c. Administrative passwords SHOULD be changed to a strong password that complies with overarching organization password conventions defined in CBP1400-05D		X
3.2 Confidentiality		
3.2.a. Wireless systems SHOULD use strong encryption to protect the confidentiality of data.		X
3.2.b. WLAN systems SHOULD meet the Wi-Fi Alliance Wireless Protected Access 2 (WPA2) interoperability standard that is based on the Institute for Electrical and Electronics Engineers (IEEE) 802.11i security standard.		X
3.2.c. The use of static keys SHOULD be avoided.		
3.2.d. Dynamic key rotation SHOULD be used in conjunction with an enterprise RADIUS server.		X
3.3 Integrity		
3.3.a. Strong hash routines and security controls SHOULD be used to ensure data have not been modified in an unauthorized or accidental manner.		X
3.3.b. 802.11i security SHOULD be employed.		X
3.5 Physical Security		
3.5.a. Each wireless infrastructure device SHOULD be secured in a locked enclosure or space that is resistant to tampering, theft, and unauthorized access to console ports, power supplies, and reset buttons.		X
3.5.b. Guards who routinely patrol the facilities SHOULD visually inspect AP enclosures.		X
3.5.c. Guards SHOULD be made aware of the importance of these devices and the likelihood of potential theft or tampering, as well as be able to recognize signs of tampering or unauthorized individuals attempting to access the enclosures.		X
3.6 Default Configuration Settings		
3.6.a. All sensitive settings for wireless systems SHOULD be changed to protect against unauthorized intrusion and modification of system settings.		X
3.7 Denial of Service		
3.7.a. Sensitive wireless systems SHALL have the capability to detect, identify, and locate attacks, as well as capture transmissions for wireless forensics.	X	
3.8 National Information Assurance Partnership Common Criteria Security Validations		
3.8.a. CBP administrators SHOULD carefully evaluate products to ensure that security validations have been performed and that the products conform to commonly used PPs.		X

3.8.b. The NIAP validation reports SHOULD be examined carefully to ensure that all required targets of evaluation are validated to an appropriate level of robustness.		X
3.9 Disabling Non-Secure or Non-Essential Ports and Protocols		
3.9.a. Ports, protocols, and services that are enabled by default and are not essential to mission requirements SHOULD be disabled.		X
3.9.b. APs SHOULD be tested at least quarterly for compliance with the organization's list of approved ports and protocols.		X
3.10 Audit Logs		
3.10.a. Systems SHOULD be configured to create audit logs and capture important events such as successful and unsuccessful administrator logins, client device access attempts, client device MAC addresses, access violations, associations, disassociations, ports and protocols used, and user activities.		X
3.10.b. Log entries SHOULD be captured by a remote system on the wired network that has robust security, making the organization's overall network less vulnerable to attack.		X
3.10.c. Audit log management SHOULD be addressed in the organization's System Security Plan for that system.		X
3.11 Login Timeouts		
3.11.a. Administrative login timeouts SHOULD be implemented on a system's management interface so that after a period of inactivity, administrative sessions automatically logout.		X
3.13 Software and Firmware Updates		
3.13.a. Security updates and patches SHOULD be applied to all system devices to ensure that up-to-date firmware and software that protects these systems against known vulnerabilities is installed.		X
3.13.b. Vendor-related and security vulnerability alert sites SHOULD be monitored frequently.		X
3.14 Network Intrusion Detection System		
3.14.a. A network IDS sensor SHOULD monitor the wireless system links to detect anomalies.		X
3.14.b. Additionally, host-based IDS sensors SHOULD be employed to monitor system and administrator level activities.		X
4.0 WLANS—Securing the AP		
4.1 WLAN Network Naming Conventions		
4.1.a. The WLAN network name SHOULD be changed from the default name to a unique name that does not reveal its affiliation to DHS operations or organizations.		X
4.1.b. The ESSID name SHOULD NOT be associated with organizational function or identity to avoid advertising the network's identity or function to potential attackers.		X
4.4 Over-the-Air Encryption Recommendations		
4.4.a. Static WEP encryption offered by 802.11-based networks SHOULD NOT be used.		X
4.4.b. WLAN systems SHOULD implement a NIST FIPS-approved mode with AES encryption.		X
4.4.c. FIPS 140-2 validated commercial off-the-shelf (COTS) products SHOULD be considered as preferable to those that have not been validated.		X

4.4.d. Systems that provide per-session dynamic RC4 keys, such as dynamic WEP, temporal key integrity protocol (TKIP), and WPA, SHOULD NOT be adopted.		X
4.5 OSI Layer 2 and Layer 3 Security Considerations		
4.5.a. The wireless system risk profile and the mitigation options SHOULD be evaluated in their entirety so that the appropriate balance is achieved among all system requirements.		X
4.6 Identification and Authentication Recommendations		
4.6.a. Authentication (username/password, public key infrastructure [PKI] certificate, biometrics, or one-time-password, etc.) SHOULD be implemented as an access control mechanism for authorizing system access to WLANs.		X
4.6.b. WLAN systems SHOULD implement 802.1X access control and EAP-TLS mutual authentication.		X
4.6.c. If identification and authentication cannot be enforced at the AP, then a firewall, captive portal, or other appliance SHOULD be implemented that denies network access unless proper credentials are provided.		X
4.7 AP Configuration Management		
4.7.a. APs SHOULD be routinely checked to ensure they have the correct configuration and are in compliance with the security policy.		X
4.7.b. Enterprise-grade APs SHOULD be integrated into a secure network management framework.		X
4.7.c. Administration access SHOULD only be permitted from trusted wired interfaces on the AP or by direct console port access.		X
4.7.d. Access to administration settings SHOULD never be permitted from either open network interfaces or wireless connections.		X
4.7.e. Access SHOULD only be provided when physically connected to a management network.		X
4.8 AP Radio Coverage Recommendations		
4.8.a. Each AP's RF power output SHOULD be adjusted to the minimal level necessary to provide optimal in-building coverage with minimal external propagation.		X
4.8.b. The following elements SHOULD be considered for determining coverage performance: signal strength, noise level, and signal-to-noise ratio.		X
4.8.c. Channel usage SHOULD be coordinated and designed with care to avoid overlap and interference.		X
5.0 WLANS—Securing the Perimeter		
5.1 Wired/Wireless Perimeter Traffic Filtering		
5.1.a. Traffic traveling from the wireless network to the wired segment SHOULD be restricted by a firewall or other filtering device to authorized users only.		X
5.1.b. Traffic traveling from the wireless network to the wired network SHOULD be restricted to specific machines, specific ports, and specific protocols to help prevent unauthorized access violations.		X
5.1.c. Traffic traveling from the wired segment to the wireless segment SHOULD be restricted to only administrative functions (such as AP management) and allowed on a host-by-host basis.		X
5.2 Using Network-Based IDS		

5.2.a. IDS sensors SHOULD be placed at ingress and egress points or supported within the wired or wireless perimeter firewall device so that anomalies can be detected.		X
5.2.b. Additionally, host-based IDS sensors SHOULD monitor any administrator-level activities.		X
5.2.c. Automated network defense mechanisms require significant field adjustments and SHOULD be thoroughly tested before their implementation.		X
5.2.d. IDSs SHOULD incorporate location-aware capabilities to speed incident response and forensic capabilities to identify and track modified information.		X
5.3 VPN Tunnel Termination		
5.3.a. VPN concentrators SHOULD be placed at wired and wireless ingress and egress points so that they provide end-to-end encryption from the wired network to the client and so that information passes over the wired network in an unencrypted format.		X
5.3.b. To avoid increased risks of vulnerable points of entry, multiple tunnels or split tunnels SHOULD NOT be allowed at the same client device.		X
6.0 WLANS—Implementing Wireless Intrusion Detection Systems		
6.0.a. Mobile spectrum analyzers SHOULD be used to perform troubleshooting, traffic and interference analysis, and unauthorized device detection to identify non-WLAN devices that operate in the same frequency bands, e.g., Bluetooth devices, cordless telephones, and microwave sources of interference.		X
6.0.b. An Incident Response Plan SHOULD be developed and maintained as part of the System Security Plan for each wireless system, as appropriate, and executed when vulnerabilities, threats, and attacks are discovered.		X
6.1 Rouge APs and Other Unauthorized Wireless Devices		
6.1.a. Unauthorized devices severely weaken the organization's security posture and SHOULD be taken seriously if found.		X
6.1.b. Incident response teams SHOULD perform a thorough investigation whenever an unauthorized wireless device is detected.		X
6.2 Using WIDS Location Services		
6.2.a WIDS sensors SHOULD be location aware and should offer location information so that administrators can respond appropriately to attacks.		X
6.5 Disparate Wireless Communications Device Monitoring		
6.5.a. Devices such as WLANs with altered frequencies, cellular modems, Bluetooth, Wireless Microwave Access (WiMAX), etc. SHOULD be passively monitored through the use of specially configured WIDS sensors whenever possible.		X
7.0 WLANS—Infrastructure Considerations		
7.2 Identity Access Management Systems		
7.2.a. Wireless nodes such as APs and WLAN switches SHOULD be able to support strong authentication and authorization services that verify identity before granting access to the network.		X
8.0 Fixed Access Wireless Networks—Bridge Countermeasures		
8.0.a. Bridge devices SHOULD be configured to accept connections only from other bridge devices and not from client devices.		X
8.1 Bridge Link Confidentiality		

8.1.a. FIPS 140-2 validated products SHOULD be selected to secure link-level communications between bridges.		X
8.1.b. If the bridges selected do not support FIPS-approved algorithms, then an algorithm SHOULD be selected according to industry best practices.		X
8.2 Mutual Authentication of Authorized Bridges and Pairing Arrangements		
8.2.a. Bridges SHOULD provide a mechanism to mutually authenticate each other before communications are established and periodically during the communications.		X
8.2.b. Bridges SHOULD identify themselves by supplying a unique identifier that cannot be easily spoofed or duplicated.		X
8.2.c. Lists of authorized bridge partnerships SHOULD be maintained on the devices and documented by IT personnel.		X
8.3 Bridge Ratio Coverage Recommendations		
8.3.a. Bridge RF power output SHOULD be adjusted to the minimum level necessary to provide LOS communications.		X
8.3.b. Site survey documentation SHOULD be kept in a secured location and made available to the ERT for incident response.		X
8.3.c. Site survey documentation SHOULD be kept in a secured location and made available to the ERT for incident response purposes.		X
8.4 Restricting Bridge Communications Based on MAC Addresses		
8.4.a. MAC-address-based access control capabilities SHOULD be configured on all bridges so that any connection from any other bridge that is not specifically allowed will be denied by default.		X
9.0 WWANS—Commercial Services Countermeasures		
9.0.a. Additional defense-in-depth layers of protection SHOULD be implemented at DHS networks and end-user device ingress and egress points across untrusted commercial services WWANs.		X
9.1 Commercial Services WWAN Link Confidentiality		
9.1.a. FIPS 140-2 approved algorithms SHOULD be used to secure link-level communications between servers and client devices.		X
9.1.b. FIPS 140-2 validated products SHOULD be selected in preference to nonvalidated products.		X
9.1.c. If the products selected do not support FIPS-approved algorithms, then an algorithm SHOULD be selected according to industry best practices.		X
9.1.d. Acquisition of a FIPS 140-2 validated product SHOULD be implemented at each endpoint to provide secure communications.		X
10.0 Wireless Personal Area Networks		
10.1 WPAN Ad Hoc Networks		
10.1.a. Strict configuration of ad hoc networks on client devices SHOULD be enforced.		X
10.1.b. These networks SHALL be tested at least monthly for compliance and SHOULD be disabled immediately when they are no longer necessary.	X	
10.2 Identification of WPAN Capabilities for Risk Assessment		

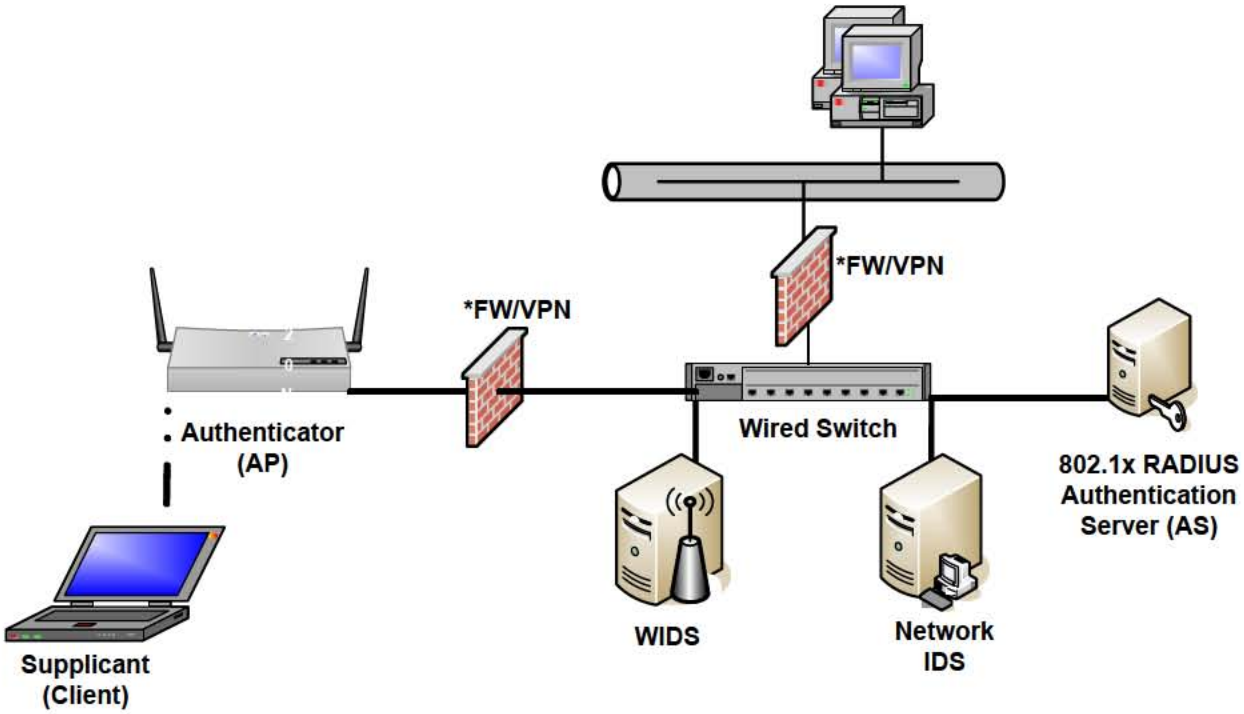
10.2.a. 4300A requires that appropriate awareness training be provided. Any appropriate wireless security awareness training should be included in the annual training provided at the component level.	X	
10.2.b Any appropriate wireless security awareness training SHOULD be included in the annual training provided at the component level.		X
10.2.c. Any WPAN capabilities that are not required by the user SHOULD be deleted or disabled.		X
10.2.d. Security personnel SHOULD be properly trained to recognize PAN-capable devices and be familiar with disabling PAN functions in those devices.		X
10.2.e. Security personnel SHOULD provide assistance to users by helping them disable any unwanted PAN functionality.		X
10.3 Device Power Requirements		
10.3.a. The RF power output of devices SHOULD be limited to only that which is needed for communication with authorized user devices.		X
10.4 Bluetooth Device Communication Risks and Recommendations		
10.4.a. IT security managers SHOULD ensure that Bluetooth communications are conducted in an environment where information exchanged cannot be captured by eavesdroppers.		X
10.4.b. Communication SHOULD be restricted to private areas where there is limited RF signal propagation.		X
10.4.c. To prevent devices from advertising themselves to would-be attackers, devices SHOULD be configured for the non-discoverable mode unless the user is in the process of pairing Bluetooth devices.		X
10.4.d. To avoid increased risks of vulnerable points of entry, multiple or split communications paths SHOULD not be allowed for the same client device.		X
10.5 Personal Identification Number Protection		
10.5.a. The Bluetooth PIN is exposed during the pairing function and therefore SHOULD be unique while at the same time not exposing important organizational information.		X
10.5.b. IT security managers SHOULD avoid deploying or permitting the use of wireless devices that do not provide the necessary user interface to allow PINs to be changed or reconfigured (e.g., Bluetooth mice, ear-bud microphones, keyboards).		X
10.6 Disabling Unwanted Profiles		
10.6.a. IT security managers SHOULD disable unwanted WPAN profiles to reduce the points of access an attacker might exploit.		X
10.6.b. Organizations SHOULD operate under the principle of least privilege and only enable functionality that users absolutely require for day-to-day operations.		X
10.6.c. Profiles that can expose sensitive information SHOULD be used extremely conservatively.		X
10.7 Device Security Modes		
10.7.a. Devices that support Bluetooth 1.2 SHOULD be selected in preference to those that support only Bluetooth 1.1.		X
10.8 Avoid Social Engineering		
10.8.a. Users SHOULD be instructed on how to detect social engineering attacks and to verify the identity of persons and/or information they receive, rather than applying blanket levels of trust.		X

10.8.b. Users SHOULD report any unusual activities (e.g., harassment, solicitation, or social engineering attacks) to the appropriate security personnel or other incident response entity.		X

Appendix B

Implementation Architecture Diagrams

APPENDIX B: IMPLEMENTATION ARCHITECTURE DIAGRAMS



** Firewall / VPN Concentrator placement will vary by implementation*

Diagram B-1: Generic WLAN Architecture

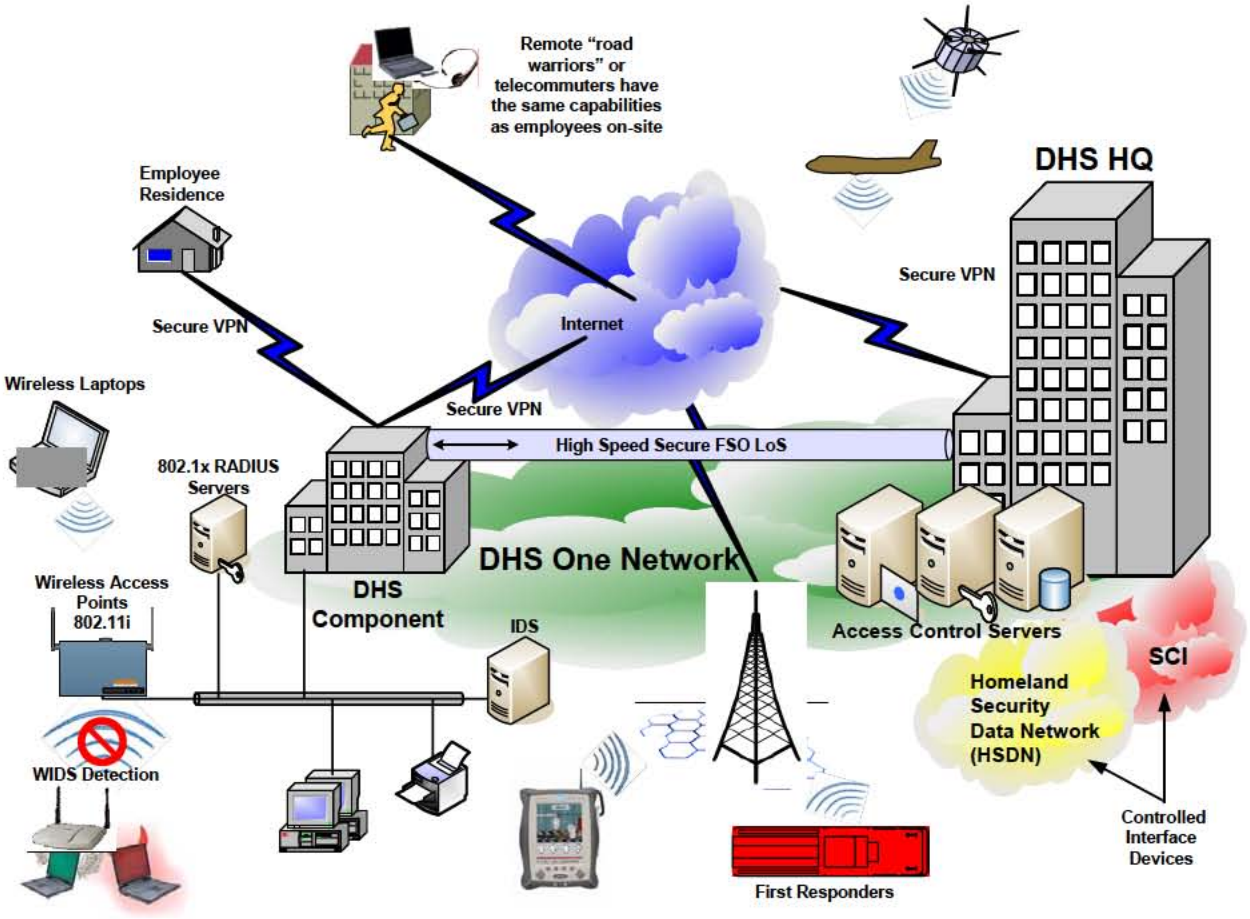


Diagram B-2: Notional DHS Enterprise Architecture

Appendix C

Management Responsibilities Associated with Wireless Systems

APPENDIX C: MANAGEMENT RESPONSIBILITIES ASSOCIATED WITH WIRELESS SYSTEMS

Wireless System Responsibilities are detailed in Section 4.0 of the 4300A Sensitive Systems Handbook, https://dhsonline.dhs.gov/portal/jhtml/dc/sf.jhtml?doid=17606

Appendix D
Technical References

APPENDIX D: TECHNICAL REFERENCES

- Department of Homeland Security. *DHS Sensitive Systems Policy Directive 4300A*.
- Department of Homeland Security. *DHS 4300A Sensitive Systems Handbook*.
- Department of Homeland Security. *IT Security Architecture Guidance, Volume I: Network and System Infrastructure*.
- Department of Homeland Security. *IT Security Architecture Guidance, Volume II: Security Operations and Support*.
- Department of Homeland Security. *IT Security Architecture Guidance, Volume III: Application Infrastructure Design*.
- Department of Defense. Defense Information Systems Agency. 2005. *Wireless Security Technical Implementation Guide.* ver. 4, rel. 1.
- Department of Defense. Defense Information Systems Agency. 2005. *Secure Wireless Local Area Network Addendum to the Wireless Security Technical Implementation Guide.* ver. 1, rel. 1.
- Department of Defense. Defense Information Systems Agency. 2005. *Wireless LAN Security Framework Addendum to the Wireless Security Technical Implementation Guide.* ver. 2, rel. 1.
- National Security Agency. 2006. *National Security Agency/Central Security Service Website*. National Security Agency. http://www.nsa.gov (accessed January 17, 2006).
- Committee on National Security Systems. August, 2005. *National Information Assurance (IA) Policy on Wireless Capabilities*. http://www.cnss.gov/policies.html (accessed January 18, 2006).
- National Institute of Standards and Technology. 2006. *National Vulnerability Database*. National Institute of Standards and Technology. http://nvd.nist.gov (accessed January 17, 2006).
- National Institute of Standards and Technology. November, 2002. *NIST SP 800-48: Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*. National Institute of Standards and Technology. http://www.nist.gov (accessed January 17, 2006).
- National Institute of Standards and Technology. October, 2003. *NIST SP 800-42: Guideline on Network Security Testing*. National Institute of Standards and Technology. http://www.nist.gov (accessed January 17, 2006).
- National Institute of Standards and Technology. February, 2005. *NIST SP 800-53: Recommended Security Controls for Federal Information Systems*. National Institute of Standards and Technology. http://www.nist.gov (accessed January 17, 2006).

Appendix E
Acronyms

APPENDIX E: ACRONYMS

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
AMPS	Advanced Mobile Phone System
AO	Authorizing Official
AP	Access Point
ARP	Address Resolution Protocol
C&A	Certification and Authentication
CBP	Customs and Border Protection
CDP	Cisco Discovery Protocol
CISO	Chief Information Security Officer
CoS	Class of Service
COTS	Commercial Off-the-Shelf
DHCP	Dynamic Host Control Protocol
DHS	Department of Homeland Security
DoD	Department of Defense
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ERT	Emergency Response Team
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
HTTP	HyperText Transport Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	IP Security
IR	Infrared
IT	Information Technology
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol

Acronym	Definition
LOS	Line of Sight
LWAPP	Lightweight Access Point Protocol
MAC	Media Access Control
MMS	Multimedia Messaging System
mW	milliwatt
NDS	Novell Directory Service
NIAP	National Information Assurance Partnership
NIST	National Institute of Science and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OBEX	Object Exchange Protocol
OSI	Open Systems Interconnection
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RSN	Robust Security Network
RTLS	Real-time Location Sensing
SKIP	Simple Key Management for Internet Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TRM	Technical Reference Model
UMA	Unlicensed Mobile Access
UWB	Ultra Wideband
VPN	Virtual Private Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System

Acronym	Definition
WiMAX	Wireless Microwave Access
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WMO	Wireless Management Office
WPA	Wireless Protected Access
WPAN	Wireless Personal Area Network
WSB	Wireless Security Board
W-VoIP	Wireless Voice over Internet Protocol
WWAN	Wireless Wide Area Network