Homeland Security

DHS 4300A
Sensitive Systems Handbook

Attachment Q1

Sensitive Wireless Systems

Version 11.0

August 5, 2014

Protecting the Information that Secures the Homeland

Document Change History

Version	Date	Description
1.0	2005	Initial release
2.3	November 29, 2005	Incorporates comments received from: ISSB, CISO, USCG
3.0	February 1, 2006	Incremented from version 2.4 to version 3.0 due to the number of comments received. Version 3.0 incorporates comments from: CBP, ICE, CISO, OCIO, S&T, and USCIS.
3.1	February 27, 2006	Incorporates comments received from WWG: CBP, FAMS, US-VISIT.
3.2	May 22, 2006	Presented to WSB for final approval before CIO Council
4.2	October 1, 2006	Document upgraded to version 4.2 to match 4300A policy version scheme. Approved Q1 without revised should/shall formatting. Pending Wireless Security Board final approval before sending to CISO for publishing.
4.3	December 12, 2006	Document upgraded to version 4.3 to reflect revised should/shall formatting. Also reflects comments received from WSB.
5.0	March 1, 2007	No change.
6.0	May 14, 2008	No change.
6.1	September 23, 2008	No change.
7.0	August 7, 2009	Introduced new terminology Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53
11.0	August 5, 2014	Rewritten as new document to reflect new wireless technologies and security guidelines.

Contents

This page intentionally blank

1.0 INTRODUCTION

Wireless communications technology enables exchange of information within a geographical area by encoding data into electromagnetic waves that propagate through space. The distances between communicating locations may be millimeters or thousands of kilometers. Wireless technologies utilize various portions of the electromagnetic spectrum, including radio frequency (RF) and infrared (IR), both analog and digital wave forms, and different types of encoding, including multiplexing, channel coding, modulation, and layered communication protocols. As technology evolves, new forms of wireless communications constantly emerge to meet the demands from governments, business communities, and consumers.

This document provides, from an information security perspective, techniques and procedures for implementing wide area, local area, and personal area wireless architectures for the Department of Homeland Security (DHS) information technology (IT) programs. Published as an attachment to the DHS 4300A Sensitive Systems Handbook, this document is the foundation for DHS Components to use in developing and implementing their wireless IT security programs. It is based on and considers statutes; Department directives and policies; guidance from the Government Accountability Office (GAO), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), the Department of Defense (DoD), and national and international standardization organizations; and general wireless security best practices commonly recommended and followed by private industry and academic communities.

1.1 PURPOSE

This document is issued as implementation guidance for IT program managers and security personnel under the authority of the DHS Chief Information Officer (CIO) through the DHS Office of the Chief Information Security Officer (OCISO). This document addresses the security specifics of sensitive wireless systems only and does not cover the use of classified wireless systems. In accordance with *DHS Sensitive Systems Policy Directive (PD) 4300A*, the use of wireless communications technologies is prohibited within DHS unless the technology and the application are specifically approved by the appropriate Authorizing Official (AO). (In accordance with NIST Special Publication (SP) 800-37, the term *Authorizing Official* replaces the term *Designated Accrediting Authority* (DAA). AOs must also approve the implementation and use of wireless systems at a specified risk level during the certification and accreditation (C&A) process and ensure that appropriate and effective security measures are included in the security plan.

Given the ongoing rapid evolution in wireless technology, including different technology standards and 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 systems that cannot meet the countermeasures recommended herein; the intent, rather, is to provide a detailed explanation of potential wireless vulnerabilities and practical countermeasures in order for the Components to perform risk analysis and make an informed decision. AOs should pay particular attention to the potential risks that must be considered in approving wireless systems with technological barriers that prevent the adoption of these countermeasures. AOs should ensure that they 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 AO.

1.2 SCOPE

Wireless networks covered under this document 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), as well as wireless infrastructure that leverages commercial wireless services. Wireless systems include the transmission medium, stationary integrated devices, device

firmware, supporting services, and communication protocols. Security policies and guidelines for wireless devices such as smart phones will be addressed in a separated document due to the complexity and rapid technology development in this area. *DHS Sensitive Systems Policy Directive 4300A* establishes the Department's wireless systems policies and general guidelines pertaining to all wireless communications technologies.

It should be noted that, with very few exceptions, almost all wireless systems are eventually connected to data packet-based wired networks that are managed by either DHS or outside third parties. While the security policies of wired networks are out of the scope of this document, the guidelines set forth in this document will address end-to-end as well as interface security requirements when both wireless and wired networks are involved.

The scope and contents of this document will change over time as new capabilities are added to DHS systems, as security standards are upgraded or created, and as a result of user experiences and comments. As the DHS IT wireless security programs mature, additional attachments to the DHS 4300A Sensitive Systems Handbook that address specific areas of security interest will be developed and published.

1.3 REFERENCES

The following documents were reviewed and referenced for this document:

- DHS, DHS Sensitive Systems Policy Directive 4300A, Version 9.1, July, 2012.
- DHS, Wireless Local Area Network Security Reference Architecture, Version 1.0, September 19, 2011.
- GAO, Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk, November 2010.
- NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.
- NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007.
- NSA, Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS), Version 1.1, November 2005.
- DoD 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, November 3, 2009.
- IEEE, IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE-SA, June 12, 2007.
- IEEE, IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements, July 23, 2004.
- NIST SP 800-121, Guide to Bluetooth Security, June 2012.
- Wi-Fi Alliance, the State of Wi-Fi Security, January 2012.

2.0 SECURITY REQUIREMENTS FOR ALL WIRELESS SYSTEMS

The wireless security requirements listed in this section consist of a common set of core security capabilities and features that are applied to all wireless technologies. Requirements unique to specific types of wireless systems (e.g., 802.11 WLAN) will be addressed in the subsequent sections. As mentioned earlier, these requirements are derived from DHS directives and policies, guidance from other government sources, and practices recommended and followed by private industry, academic communities, and standardization organizations.

2.1 RISK-BASED APPROACH

A risk-based approach to wireless system security is a system-engineering approach to identify, assess, and prioritize risks associated with wireless systems and determine the likelihood and potential impact of these risks. Mitigation strategies and resources are then applied in defending against the most significant threats and preventing the incurrence of undue risks. For instance, unauthorized access points or devices on the DHS internal network occur sometimes and they pose great threat to the DHS information security as the internal network is regarded as trusted and within the defense perimeter. One mitigation strategy against this threat is to deploy effective detection and prevention tools to identify these threats and block their access when detected.

- A risk-based approach shall be used to mitigate risks associated with wireless systems.

At the highest level, two security classifications can be used to help identify and assess risks associated with a given wireless system:

- Trusted: Any combination of people, information resources, data systems, and networks that are subject to a shared security policy (a set of rules governing access to data and services). A trusted wireless system is within the accreditation boundary established by DHS and over which DHS has direct control for the application of required security controls or the assessment of security control effectiveness.
- Untrusted: Any combination that is outside the "trusted." An untrusted wireless system is outside the accreditation boundary established by DHS and over which DHS has no direct control for the application of required security controls or the assessment of security control effectiveness.

Commercial or official visitor wireless networks, for example, should be considered untrusted because they are outside DHS control. DHS internal wireless networks are considered trusted because DHS can apply rigorous security policies and controls on these networks. Risks can be identified from the technology, process, and people perspectives by taking into account of the unique open nature of wireless systems and the rapid evolution of wireless technologies. The following section describes various wireless system threats and corresponding countermeasures in detail.

2.2 WIRELESS SYSTEM THREATS AND COUNTERMEASURES

Wireless systems have their inherent weakness and vulnerabilities due to the open nature of wireless technologies, and security threats are widespread through a wide variety of attack methods. Wireless communications are susceptible to interference, eavesdropping, RF jamming, as well as threats typical to wired networks.

Threat Category	Description
Denial of Service	Attacker prevents or prohibits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.

Threat Category	Description
Man-in-the-Middle	Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party. In the context of wireless systems, a man-in-the-middle attack can be achieved through a bogus or rogue Access Point (AP), which looks like an authorized AP to legitimate parties.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants, and extracts sensitive information.

Table 1. Wireless System Threats

Wireless system security addresses data confidentiality and integrity, authentication and access control, intrusion detection and prevention, logging and monitoring, as well as system availability and performance. The goal of wireless system security can be better achieved and the threats mitigated by adhering to federally-mandated standards and industry's information security best practices.

OSI Layer	Security Considerations
Application	Detect and prevent malicious code, viruses, phishing, and other malware applications. Mitigation tools include firewalls, anti-virus/malware detection software, Web security, and intrusion detection applications.
Presentation	Protect data files by cryptography (e.g., file password encryption).
Session	Protect system from port exploits or session hijacking. Use Secure Socket Layer (SSL) for Session and Transport layers.
Transport	Provide authentication and secure end-to-end communications such as the Secure Shell (SSH-2) protocol.
Network	Protect the routing and the forwarding protocols by robust authentication and encryption of routing data. The Internet Protocol Security (IPSec) standard provides meshed and simultaneous tunnels for secure communication.
Data Link	Protect the Media Access Control (MAC) sublayer from masquerade, DoS, impersonation, and Address Resolution Protocol (ARP) threats. Wireless protocols have built-in security features such as Layer 2 tunnels and message integration check.
Physical	Detect and prevent jamming and denial of service (DoS) attacks in the air medium via wireless intrusion detection system and intrusion prevention system (WIDS/IPS), which can detect abnormal signals and physically geolocate the suspicious devices via direction findings triangulation and timing algorithms. Employ anti-jamming techniques such as spread spectrum techniques.

Table 2. OSI Security Considerations

2.3 AUTHENTICATION

Authentication methods include IEEE 802.1X port-based network access control, Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) authentication, and enterprise Remote (RADIUS) servers to provide mutual authentication to user devices and systems while providing for dynamic key management.

It should be noted that EAP-TLS requires existing Public-key Infrastructure (PKI). If a full-fledged PKI is not available, other authentication protocols, such as EAP-Protected Extensible Authentication Protocol (EAP-PEAP), can be used. These protocols only require a server side x.509 digital certificate that can be purchased

from a third-party Certificate Authority, or a digital certificate can be issued from an organization's internal Certificate Authority. No user device authentication is provided in this case. Additional network control accesses, such as two-factor authentication, may be required to authenticate users and devices to ensure that they do not introduce security vulnerabilities and risks.

2.4 CONFIDENTIALITY

DHS PD 4300A requires that "Components shall use only cryptographic modules that are Federal Information Processing Standard (FIPS) 197 (Advanced Encryption Standard [AES]-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use."

2.5 INTEGRITY

Wireless traffic integrity is essential to ensure that data has not been modified in transit or at rest, and it also protects against other threats such as man-in-the-middle attacks. If a mechanism is available that allows for cryptographic verification of message integrity, system nodes must discard all messages that cannot be verified.

2.6 MANAGEMENT CONTROL

Wireless systems must be capable of supporting remote device management, establishment or change to configurations to comply with security policy, and updates of software and firmware. Wireless systems must have the ability to manage wireless infrastructure via management interfaces and tools which are part of the overall enterprise management infrastructure.

The network segment for management control should be integrated into the enterprise wired network, and it should be isolated from data networks to ensure robust management control. Security protections must not degrade or impede critical services or usability features protected by law or published policy (for example, compliance with Section 508 of the U.S. Rehabilitation Act).

A centralized wireless management structure provides a more effective means to manage the wireless infrastructure and the information security program as a whole. A centralized structure can also facilitate the development and implementation of standardized guidance, which allows organizations to consistently apply information security policies.

Wireless devices and/or software must not degrade or circumvent established system security controls. Any system modifications require appropriate security review and follow change management policies and procedures. In addition, configuration management and secure baseline configurations should be addressed in the organization's system security plan for that system.

2.7 PHYSICAL SECURITY

Routine inspections and surveillance for suspicious behavior will reduce the likelihood of unauthorized equipment operation and theft. Because wireless systems are susceptible to eavesdropping from a distance, guards and users alike should report to appropriate security personnel any suspicious individuals or activities in or around the facility.

2.8 NATIONAL INFORMATION ASSURANCE PARTNERSHIP COMMON CRITERIA SECURITY VALIDATIONS

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative to address IT system and product security testing demands of both IT consumers and producers. NIAP is a collaboration of NIST and 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 the 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.

When avoiding the use of processes 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]), for in-band device management, a possible secure configuration is to encapsulate insecure protocols inside encrypted tunnels; examples include IPSec and SSL-based virtual private network (VPN).

2.9 LOGS

Logs serve as part of the wireless network monitoring and management capabilities to ensure that wireless networks are constantly monitored. They provide a traceable mechanism to record network activities and discover network intrusions. The integrity of logs should be protected by synchronizing the time clocks on all devices, remotely recording wireless activities and events, and enforcing strict access control for logs.

2.10 CONFIGURATION CONTROLS

Establishing configuration requirements and secure baseline configurations for wireless networks and devices can help ensure they are deployed in a secure manner in accordance with DHS security policies.

Wireless systems are usually initially configured with default vendor settings that are common knowledge. These settings can include network information such as default channel or modulation specification; 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 application services running.

2.11 SOFTWARE AND FIRMWARE UPDATES

The NIST National Vulnerability Database (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, the updated firmware should be tested in a nonproduction environment to validate functionality before a production rollout. System audit policy and guidance is provided in *DHS Sensitive Systems Policy Directive 4300A* and the DHS 4300A Sensitive Systems Handbook.

2.12 WIRELESS MONITORING

Wireless monitoring capabilities include tools and methods for (a) conducting site surveys and the appropriate position of antennas to minimize signal leakage, (b) detecting misconfigured clients and using policy driven software or hardware solutions to ensure client devices and users comply with defined DHS wireless security policies, and (c) detecting and blocking suspicious or unauthorized activity or sources of radio interference.

Wireless intrusion detection systems (WIDS)/intrusion prevention systems (IPS) can detect network anomalies and monitor wireless infrastructure. Anomalies may include, but are not limited to, interference sources, abnormally high or low utilization, multiple login attempts, attack signatures, off-hour logins, and other suspicious variances from the system baseline.

2.13 CONTENT FILTERING

Content filtering is the process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users. A dedicated server can be used to perform the content filtering task. For wireless systems that are internal to the organization wired networks, there are no specific requirements associated with content filtering that is already applied to the wired networks. Content filtering for external wireless systems such as visitor WLAN may be

[1] http://nvd.nist.gov

different than those applied on the organization's internal networks. Traffic from this network is not inspected by the National Cyber Protection System (NCPS), also known as Einstein. Therefore, organizations should define separated security controls for this network, such as allowing normal client connections via HTTP, Secure HTTP (HTTPS), and Domain Name Service (DNS) to only access limited Internet sites. In addition, the existing Trusted Internet Connections (TIC) capability can be leveraged to protect and monitor these external wireless systems.

All content filtering products must be kept up-to-date to ensure that their detection is as accurate as possible. Another key feature of content filtering packages is the scanning of inbound and outbound data for suspicious activities and taking preventive actions accordingly.

2.14 TRAFFIC SEPARATION

Traffic from different network segments may come from different security trust boundaries. For instance, official visitor wireless networks cannot be totally controlled by DHS (e.g., official visitor personal devices), so they introduce potentially serious security risks. As such, official visitor wireless traffic should be separated from the enterprise traffic via logical and/or physical means (e.g., IPSec tunnels or separated network circuits). Therefore, official visitors are only allowed to connect to the Internet and never access DHS enterprise resources.

2.15 SECURITY ASSESSMENT

Regular security assessments should be performed to evaluate the security posture of wireless networks and determine corrective actions needed to ensure that the wireless networks remain secure. Regular assessments help to determine whether wireless systems are transmitting correctly and are on the correct channels. Assessments can help Components determine whether controls are appropriately designed and operating effectively to achieve the organization's control objectives. The DHS 4300A Sensitive Systems Handbook describes the assessment areas and procedures in great detail.

2.16 SECURITY INCIDENT RESPONSE

Most security controls are designed to protect an organization against security threats; regardless of how effective those controls are, some security incidents are inevitable, and organizations need to have an effective response capability in place before they occur.

2.17 SECURITY AWARENESS TRAINING

Security awareness training is a fundamental part of information security to ensure that wireless networks are configured, operated, and used in a secure and appropriate manner. For security policies to be effective, those who are expected to comply with them must be aware of the policies. Additionally, the Federal Information Security Management Act (FISMA) mandates that agencies provide security awareness training for their personnel, including contractors and other users of information systems, that support the operations and assets of the agency. NIST recommends that security awareness training include the risks of wireless security and how to protect against those risks. The goal of security awareness training is to protect the confidentiality, integrity, and availability of DHS IT assets and data.

3.0 WLAN SECURITY GUIDELINE

The security guideline outlined in this section is developed to ensure robust design and implementation of WLAN systems. Appendix B describes the key components of WLAN infrastructure and their functionalities and provides a high-level WLAN system architecture.

3.1 SECURITY APPROACH

WLAN security specification is addressed by the IEEE 802.11i standard that provides security mechanisms against various WLAN security threats. The Wi-Fi Alliance, an international WLAN interoperability-advocate association, introduced Wireless Protected Access 2 (WPA2)—the interoperability certification for 802.11i implementation.

It should be noted that the 802.11i security standard only addresses WLAN security at OSI Layer 2. Layer 2 security methods address wireless authentication, frame encryption, message integrity check, and other security features. Use of Layer 2 security technology (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, such as a VPN solution or application firewall. The strategy of multiple-layer defense helps to protect the wireless system from a number of individual attacks, thus raising the cost and complexity to potential attackers.

It is extremely important to understand one security deficiency associated with 802.11i security features: the management frames in 802.11 WLAN, such as authentication, association, beacon, and probe, are not protected. Therefore, WLAN is vulnerable to attacks associated with this deficiency, such as the DoS attack of bogus association requests. Security measures at higher layers, as well as the deployment of WIDS/IPS can mitigate this risk to a great degree. New security standard 802.11w addresses the protection of management frames, and this new security enhancement was added into the WPA2 implementation in 2012. However, support of the 802.11w standard among wireless devices is very limited.

3.2 NETWORK NAMING CONVENTIONS

WLAN contains 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. The ESSID name can be masked so that it does not reveal its affiliation to DHS operations or organizations or it is not associated with organizational function or identity to avoid advertising the network's identity or function to potential attackers. On the other hand, attackers may advertise false "Authorized DHS Wireless Service" and lure users to reveal their logon credentials through the fake wireless service, which is equally as dangerous as revealing the identity of the WLAN service through the explicit ESSID.

3.3 ESSID BROADCASTING

In some physical environments or operational areas, disabling the ESSID in broadcast beacons is important, so the existence of a WLAN is not advertised in the coverage area to mitigate the war-driving threat. 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 ESSID, but typically, this information is collected by determined hackers rather than those who pass by while conducting a war-drive. Therefore, it is essential to understand that disabling ESSID broadcasting only provides very limited deterrence to potential attackers but could cause inconvenience to end users and result in connection issues with some devices. It is important for organizations to understand the ESSID broadcasting mechanism and possible operation consequences and make an informed and balanced decision from both operation and security perspectives.

3.4 ACCESS CONTROL

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 WPA2 interoperability certification processes.

Other network access control or network admission control (NAC) solutions should be evaluated and deployed to ensure that only authorized devices are permitted network access, and risk based decisions should be implemented on hosts based upon their DHS or Component risk profiles. For example, DHS enterprise resource access is granted for DHS-issued devices only if they comply with antivirus and patch mandates; authorized visitor devices are only allowed to access the Internet.

Identity access management systems are needed to effectively operate WLANs. RADIUS, which was originally designed 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.

3.5 ENCRYPTIONS

A properly configured WLAN should use the strongest end-to-end encryption mechanisms available to protect the confidentiality of traffic traveling across wireless links. The IEEE 802.11i security standard and its implementation WPA2 rely on the AES encryption algorithm for confidentiality and integrity services.

DHS Sensitive Systems Policy Directive 4300A requires that "Components shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use." Non-standard systems require a CISO waiver and exemption approval.

3.6 WIDS

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

Signature-based WIDS scan for known attack signatures and are only as good as their latest signature update; therefore, they 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 and generate very few false-positives (also known as false alarms). Another complementary approach is anomaly detection. Anomaly detection operates by comparing the current system against the system baseline. Anomaly-based WIDS is more effective against new attacks than signature-based WIDS but places a large demand for system resources on the WIDS management appliance. In addition, anomaly-based WIDS produce more false positives than signature-based WIDS.

WIDS can 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. NSA published a detailed document to address the WIDS capability requirements and deployment best practices.[2] A key WIDS capability is the ability to provide, using triangulation or timing algorithms, physical location information on attackers, rogue devices, and other threats.

3.7 WIRELESS INTRUSION PREVENTION SYSTEMS

[2] NSA, "Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS)," November 2005.

Wireless intrusion prevention systems (WIPS) with active countermeasure capabilities are emerging within the WLAN industry. Such systems can actively deny service to suspected intruders, quarantine suspected intruders to benign segments of the network, and even perform active forensics on a suspected intruder to learn about the intruder's identity, methods, and goals.

3.8 OFFICIAL VISITOR NETWORK

Official visitors (interns, short-term contractors, and people on official business) need to access the Internet, and they often use VPN technology to connect securely back to their own enterprise networks. Their laptops and devices are normally outside DHS control.

Separate wireless network infrastructure is to be used for official visitors—either logically or physically separated from the DHS internal wireless or wired networks. The only purpose of the official visitor wireless network is to enable visitors to wirelessly access the Internet using visitor-owned devices.

A shared key encryption scheme, WPA2-Pre-Shared Key (PSK), offers a cost-effective way to limit WLAN traffic to authorized visitors. The PSK is shared by all visitors and may not protect traffic among visitors. The encryption key should be changed periodically, for example, weekly.

3.9 PERIMETER SECURITY

Perimeter security devices include firewalls, VPN concentrators, IDS/IPS, and so on. These devices provide access control, encryption and decryption for message confidentiality, and the detection of security policy violations.

3.10 RADIO COVERAGE AND POWER LEVEL

The RF signal strength and noise level need to be measured carefully at the coverage area to provide acceptable WLAN services. The leakage of wireless RF signals beyond the defined coverage areas should be minimized, which can be accomplished by fine-tuning the AP RF power and by positioning of the AP and its antenna.

The following elements should be considered for determining wireless coverage and service performance: signal strength, noise level, and SNR. Channel usage should be coordinated and designed with care to avoid overlap and interference.

4.0 FIXED ACCESS WIRELESS NETWORKS: SECURITY GUIDELINES

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 form a hub-and-spoke topology with a master bridge located in a central position and multiple client bridges. The master bridge typically employs an omni-directional antenna. One such technology is the point-to-point microwave connection that has been used widely for voice and data communications

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 network 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.

- Bridge devices should be configured to accept connections only from other authorized and approved bridge devices and not from client devices.

4.1 BRIDGE LINK CONFIDENTIALITY

Bridges are a means of providing a mechanism to ensure that information is not made available or disclosed to unauthorized individuals, entities, or processes; to comply with DHS policy, select FIPS 140-2 validated products that use AES-256 encryption to secure link-level communications between bridges.

4.2 BRIDGE LINK AUTHENTICATION

One common practice is to deploy a MAC-address-based access control which only allows network connections for those devices if their MAC addresses are on a pre-defined MAC address list. MAC addresses within data frames are sent in the clear and, therefore, can be captured and eventually spoofed by attackers, but this security control prevents accidental connections and forces attackers to perform additional work to compromise the system.

4.3 BRIDGE RADIO COVERAGE RECOMMENDATIONS

The following elements should be considered for determining outdoor coverage and performance: antenna gain, antenna azimuth, antenna height, transmitter power, receiver sensitivity, cable losses, interference, and environmental structures.

5.0 WWAN: SECURITY GUIDELINES

A wireless wide area network (WWAN) is a network covering a wide geographical area, involving a vast array of clients. Wireless technology standards include Long Term Evolution (LTE), WiMAX, 802.11, and others. Commercial WWAN services such as cellular telephone service, packet radio networks, satellite communications, and WLAN hotspots provide a flexible and robust means for remote access and telework or extending DHS network coverage. However, these networks should be treated as untrusted public networks. DHS does not have control over the commercial service infrastructure, its configuration, operation, or maintenance, nor over the personnel with access to the infrastructure or management systems.

5.1 WWAN BUILT-IN SECURITY FEATURES

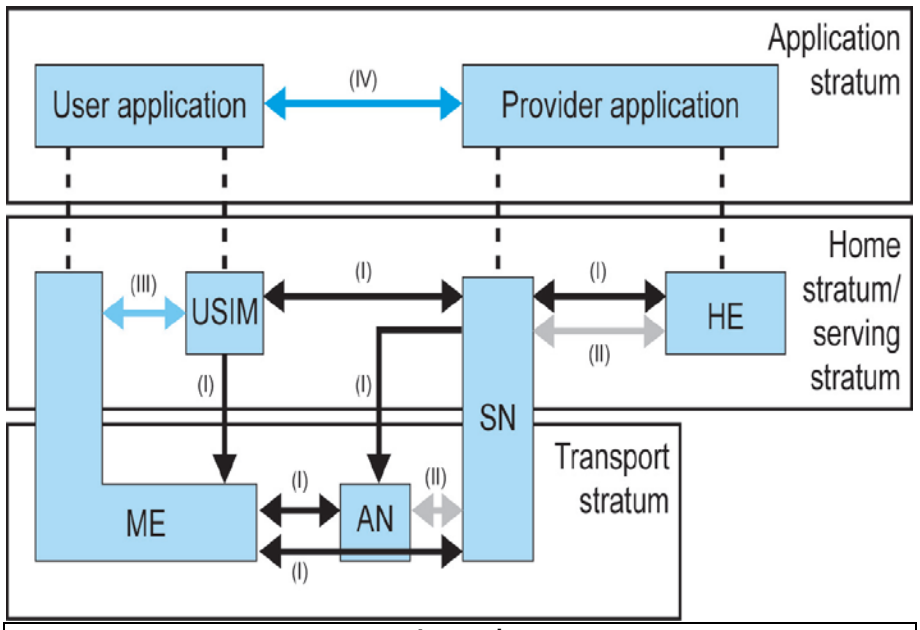
Different WWAN technologies implement various built-in security features based on the technology standards, and they are developed through the layered architecture approach. Security enhancement is implemented at all OSI layers, from lower physical medium all the way up to applications, as illustrated by the following common WWAN standards.

- The **IEEE 802.11i** standard implements the AES-Counter with Cipher Block Chaining (Counter with CBC)-Message Authentication Code (MAC) Protocol (AES-CCMP) to negotiate MAC-Layer specification security communications and establish the Layer 2 security connection that includes frame authentication, encryption, and integrity check. In addition, 802.1X port-based access control and EAP authentication, as well as the security measures at upper layers discussed in Section 3, are part of the overall security architecture.
- The **IEEE 802.16** standards define the air interface and medium access control (MAC) for a wireless metropolitan area network (WMAN). This is the first industry-wide standard suite that can be used for fixed, nomadic, and mobile wireless access with substantially higher bandwidth than the cellular networks. The 802.16d (Fixed WiMAX) standard provides an alternative to cabled access networks, such as fiber optic, cable modem, and digital subscriber line (DSL). The 802.16e (Mobile WiMAX) standard provides mobile voice, video and Internet services similar to 3G cellular, but with a higher data rate. The IEEE 802.16 devices need to be certified by the WiMAX forum to ensure interoperability. The IEEE 802.16 standards provide user authentication and data privacy as security measures. Privacy key management (PKM) is used for user authentication. PKM establishes a security association between the base station and subscriber device. The security association is a set of security information that a base station and one or more subscribers share to support secure communications. PKM distributes an authorization token to an authorized subscriber by verifying the subscriber's digital certificate. AES with at least 128 bits is used to ensure data privacy.
- **Satellite** network security measures include, among other means, encryption, high-power uplinks, spread spectrum, and digital interface certifications.

  Satellite networks generally employ proxy-based techniques to overcome the shortcomings associated with satellite communications: low bandwidth, long delay, and high error rate. Transmission Control Protocol (TCP) Performance Enhancing Proxy (PEP) is implemented to intercept TCP packets, break the connections, and act as a proxy server for both ends, all in an effort to improve TCP performance. Similar techniques are also used to improve the speed of responses to Web-browser requests and responses via HTTP proxy servers.

  The proxy approach requires that part of communication messages, TCP header or Web page request and response, be in clear text and be available to proxy servers, which may be controlled by third parties. The proxy mechanism can be disabled, which leads to performance degradation. It is extremely important for organizations to understand the satellite proxy mechanism, evaluate the performance requirements, and make an informed and balanced decision from both operational and security perspectives.

- **LTE** has been chosen as a 3G/4G cellular technology by major cellular service providers around the globe. Specifically, the International Telecommunication Union (ITU) has approved LTE-Advanced as a candidate for 4G technologies. LTE and LTE-Advanced are standardized by the Third Generation Partnership Project (3GPP). LTE defines the security features at the application, device, and transport levels.[3] This security architecture is also applicable to 3G cellular networks.



Legend			
AN	Access Network	HE	Home Environment
ME	Mobile Equipment	SN	Serving Network
USIM	Universal Subscriber Identity Module		

Figure 1. LTE Security Architecture

Five security feature groups are defined, as shown in the figure above. Each of these feature groups meets certain threats and accomplishes certain security objectives:

- **Network access security (I) –** the set of security features that provides users with secure access to services, and which protects against attacks on the (radio) access link.
- **Network domain security (II) –** the set of security features that enables nodes to securely exchange signaling data and user data and protect against attacks on the wireline network.
- **User domain security (III) –** the set of security features that secures access to mobile stations.
- **Application domain security (IV) –** the set of security features that enables applications in the user and provider domains to securely exchange messages.
- **Visibility and configurability of security (V) –** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

Based on these specifications, some commercial LTE service providers implement the security features through Universal Integrated Circuit Card (UICC), Subscriber Identity Module (SIM), and

[3] 3rd Generation Partnership Project, "3GPP System Architecture Evolution (SAE): Security architecture (Release 8)."

key authentication using128-bit private keys. LTE also provides strong mutual authentication, user identity confidentiality, and integrity protection of signaling messages between end user devices and service provider networks.

Although the WWAN built-in security features sometimes do not offer the desired strong cryptographic capabilities (e.g., the AES key length is only 128-bit), they nevertheless provide one layer of defense against wireless security threats.

5.2 PRIVATE WWAN

Similar to the wired network private WAN concept, a new WWAN operation model has emerged through which commercial wireless service providers allow a certain group of customers to access their wireless networks anywhere but isolate the data traffic of this group from the rest as well as the Internet, effectively providing a dedicated and isolated private WWAN service.

A private WWAN enhances wireless communication security as the network is within the accreditation boundary established by DHS and over which DHS has direct control for the application of required security controls or the assessment of security control effectiveness. It provides visibility of all traffic thereby enabling the identification of and protection against malicious activities.

5.3 REMOTE ACCESS THROUGH VPN SERVICE

When DHS users access DHS internal resources via commercial WWAN, they should follow standard remote access guidelines and procedures. Secure remote access can be achieved through DHS VPN services that offer strong encryption, authentication, and access control mechanisms to ensure information security for sensitive data transferred across multiple, public networks.

6.0 WIRELESS PERSONAL AREA NETWORKS: SECURITY GUIDELINES

A wireless personal area network (WPAN) is a network for interconnecting peripheral devices in a short range (up to the order of tens of meters). Two common technologies under the WPAN category are IEEE 802.15.1 (also known as Bluetooth) and IEEE 802.15.4 (also known as ZigBee). WPANs are typically established in an ad hoc or peer-to-peer fashion without any static infrastructure. The security capability associated with WPAN is not sufficient for protecting sensitive information. Operation of such noncompliant systems requires an approved waiver or exception, as appropriate, from the CISO.

6.1 AD HOC OR PEER-TO-PEER NETWORKS

WPAN client devices should not be allowed to create ad hoc or peer-to-peer networks. If the CISO approves the use of such networks, the system owner shall provide documentation detailing security policies, procedures, and technical security capabilities and limitations.

6.2 DEVICES

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

6.3 COVERAGE AND POWER REQUIREMENTS

Device power requirements vary depending on the application being used. The RF power output level should be 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.

6.4 BLUETOOTH DEVICE COMMUNICATION RISKS AND RECOMMENDATIONS

For 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. Several Bluetooth versions are currently available such as high-speed 3.0 and Low Energy (LE) 4.0, and they support different levels of security modes. For example, for Bluetooth 3.0, Security Mode 3 is the strongest mode because it requires establishment of authentication and encryption before the Bluetooth physical link is completely established. More information on Bluetooth security can be found in NIST SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices* (November 2002), and NIST SP 800-121, *Guide to Bluetooth Security* (June 2012).

6.5 PERSONAL IDENTIFICATION NUMBER PROTECTION

WPAN device communications typically rely on the device's hardware address for identification and a 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.

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.

6.6 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.

6.7 DEVICE SECURITY CAPABILITIES

WPAN-enabled devices provide various security capabilities in the areas of encryption, authentication, and data integrity. The strongest security modes should be chosen to provide an extra layer of security, even though they often do not meet the DHS security standards (e.g., the encryption key is shorter).

7.0 INTEROPERABILITY

Organizations operating across many physical locations, mission groups, agencies, and commercial networks may require a wireless infrastructure that allows for interoperable mobile computing with diversified platforms and wireless standards. Standards, protocols, and products approved for use within DHS can be found in the DHS Technical Reference Manual (TRM) documents. However, devices that are listed in the TRM and follow IEEE or NIST standards may still be subject to interoperability challenges. This section will address wireless system interoperability concerns and recommendations.

7.1 INTEROPERABILITY GOVERNING BODY

Even following the same IEEE or NIST standards, wireless equipment and respective security implementations for a given wireless network may have different configurations from those of other networks of interest and may require additional means for interoperability. For example, within WLAN networks based on the same IEEE 802.11 standard, AP from different vendors typically cannot communicate among themselves, as some of them are thin AP (basically a pass-through device) while others are thick AP (performing, among other functionalities, authentication and encryption). Consequently, a dedicated DHS organization, such as the TRM governing body, should coordinate the activities of specifying, designing, and establishing wireless systems for purposes of interoperability. The TRM governing body can be the central coordinator for resolution of cross-organizational interoperability issues and may need to perform research and coordinate with other wireless-enabled Components or agencies during the system design process.

7.2 WIRELESS SYSTEM INTEROPERABILITY

As wireless networks increase in density, enterprise applications that use wireless connections can be expected to gain in popularity. Many emerging technologies take advantage of multiple APs or even multiple distinct wireless networks; examples are Wireless Voice over IP (W-VoIP) and location-based services that leverage beacons from wireless networks to provide location services. These technologies maintain connections to one or more internally or externally wireless networks in a mobile fashion, otherwise known as roaming. The challenge is to provide seamless wireless services across different technologies or organization domains.

Although APs communicate with user devices via standard wireless protocols such as IEEE 802.11 a/b/g/n, the communication mechanisms between APs and wireless backend systems such as wireless controllers are almost all proprietary. Therefore, it is almost impossible for an AP from Vendor A to communicate with another AP or controller from Vendor B.

One way to address these issues is the adoption of Mobile IP mechanism (or IP mobility), which is an Internet Engineering Task Force (IETF) standard communications protocol that supports mobile device users to move from one wireless network to another by assigning two IP addresses to a mobile device. One address is the static permanent home address. The second address, the "care-of" address, is the dynamic address assigned by the current wireless network. All application packets are sent to the home IP address and the home wireless network forwards the packets to the current IP address (and therefore the mobile device).

7.3 WIRELESS STANDARDS

Wireless architectures ideal for interoperable communications among coordinating organizations should incorporate products designed with wireless communications standards. Wireless products built upon proprietary standards should be avoided.

As discussed in Section 3.1, new security standard 802.11w, which was added to WPA2 in 2012, addresses the protection of management frames. However, support of the 802.11w standard among wireless devices is very limited.

Other standards have also been developed to address interoperability of different wireless standards in order to provide seamless wireless services. IEEE 802.21is one interoperability standard for communication

among IEEE 802 and non-802 networks, such as 802.3, 802.11, 802.15, 802.16, and cellular networks. The Unlicensed Mobile Access (UMA) technology alliance is developing interoperability specifications for communications roaming across cellular, WLAN, and Bluetooth systems. The enforcement of standards and industry certifications increases the probability of multiple organizations' systems working together with minimal user intervention.

APPENDIX A – ACRONYMS

Acronym	Definition
3GPP	Third Generation Partnership Project
AD	(Microsoft) Active Delivery
AES	Advanced Encryption Standard
AO	Authorizing Official
AP	Access Point
ARP	Address Resolution Protocol
C&A	Certification and Accreditation
CBC	Cipher Block Chaining
CCMP	Cipher Block Chaining (Counter with CBC)-Message Authentication Code (MAC) Protocol
CDP	Cisco Discovery Packet
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DAA	Designated Accrediting Authority
dB	Decibel
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DoD	Department of Defense
DoS	Denial of Service
DSL	Digital Subscriber Line
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
ESSID	Extended Service Set Identifier
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IDS	Intrusion Detection System

Acronym	Definition
IEEE	Institute for Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IR	Infrared
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOS	Line of Sight
LTE	Long Term Evolution
MAC	Media Access Control
Mbps	Megabits per second
NAC	Network Access Control
NCPS	National Cyber Protection System
NDS	Novell Directory Service
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OBEX	Object Exchange Protocol
OCISO	Office of the Chief Information Security Officer
OSI	Open Systems Interconnection
PD	Policy Directive
PEAP	Protected Extensible Authentication Protocol
PEP	Performance Enhancement Proxy
PIN	Personal Identification Number
PKI	Public Key Infrastructure

Acronym	Definition
PKM	Privacy Key Management
PP	Protection Profiles
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
ROB	Rules of Behavior
SAP	Security Authorization Package
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise
SOP	Standard Operating Procedure
SSH-2	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
TIC	Trusted Internet Connections
TKIP	Temporal Key Integrity Protocol
TRM	Technical Reference Manual
UICC	Universal Integrated Circuit Card
UMA	Unlicensed Mobile Access
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA2	Wireless Protected Access 2
WPAN	Wireless Personal Area Networks

Acronym	Definition
WPS	Wireless Protected Setup
WWAN	Wireless Wide Area Networks
W-VoIP	Wireless Voice over Internet Protocol

APPENDIX B – WLAN SYSTEM ARCHITECTURE

This appendix describes the key components of WLAN infrastructure and their functionalities and provides high-level WLAN system architecture diagrams. The diagrams provide a depiction of generic WLAN systems in order to highlight the basic components of a WLAN and how it relates to the enterprise-wide network infrastructure.

Table B-1. Key Components of WLAN Infrastructure

Component	Provides:
User-Device	• WPA2-Enterprise encryption • Device authentication using EAP • Device certificate • User authentication
Access Point	• Wireless connection
RADIUS Authentication Server	• Authentication services
WIDS/IPS	• Rogue AP detection • Unauthorized client detection • Unauthorized access attempts • Continuous monitoring of 802.11 channels • Monitoring for user devices connected to both wireless and wired networks
Wireless Controller	• Centralized management of wireless APs and user Devices • Monitoring, control, and configuration of APs; enforcement of security policy
Management System	• Centralized management and configuration software

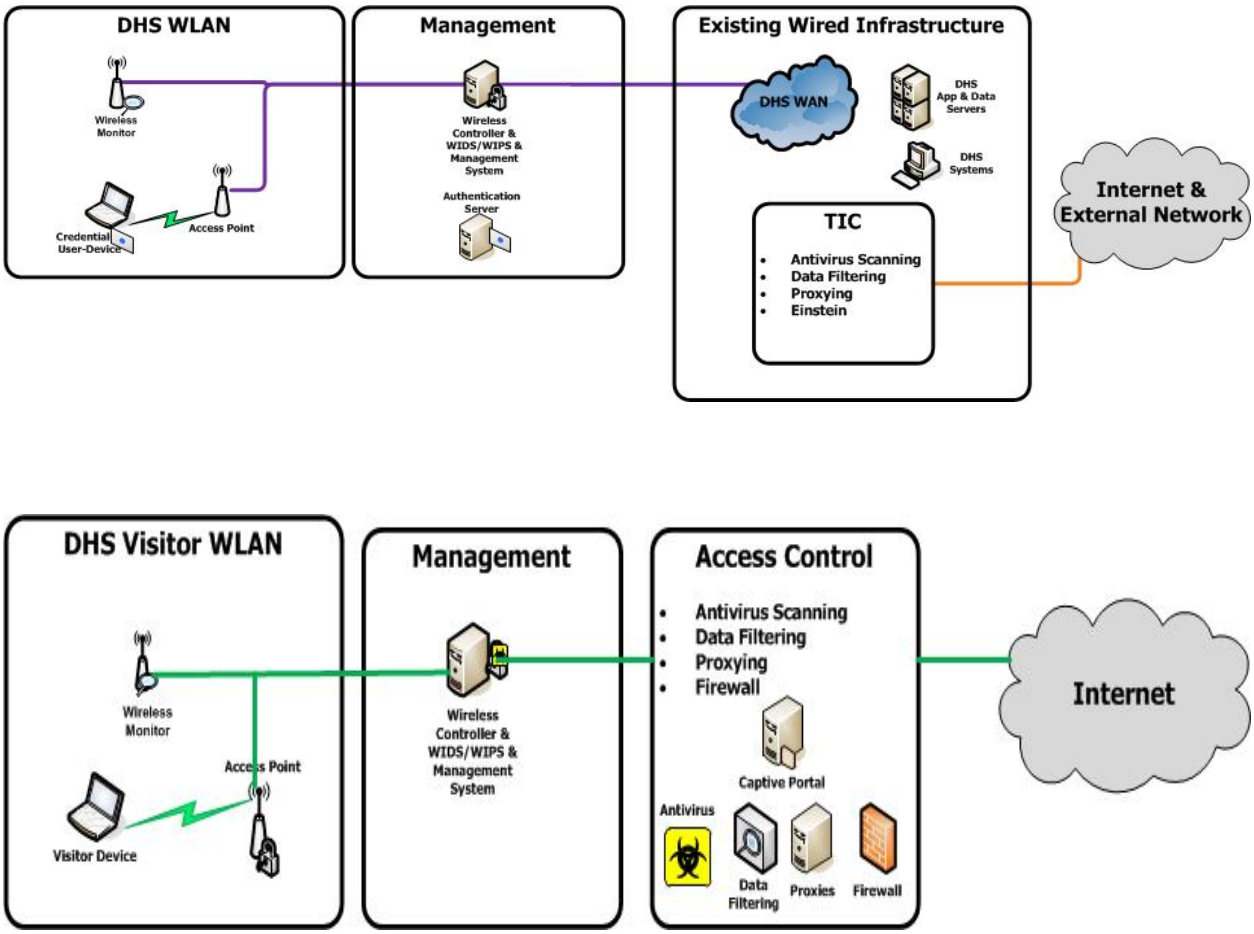


Diagram B-1. Notional WLAN Architecture Diagrams: Internal WLAN (top) and Visitor WLAN (bottom)

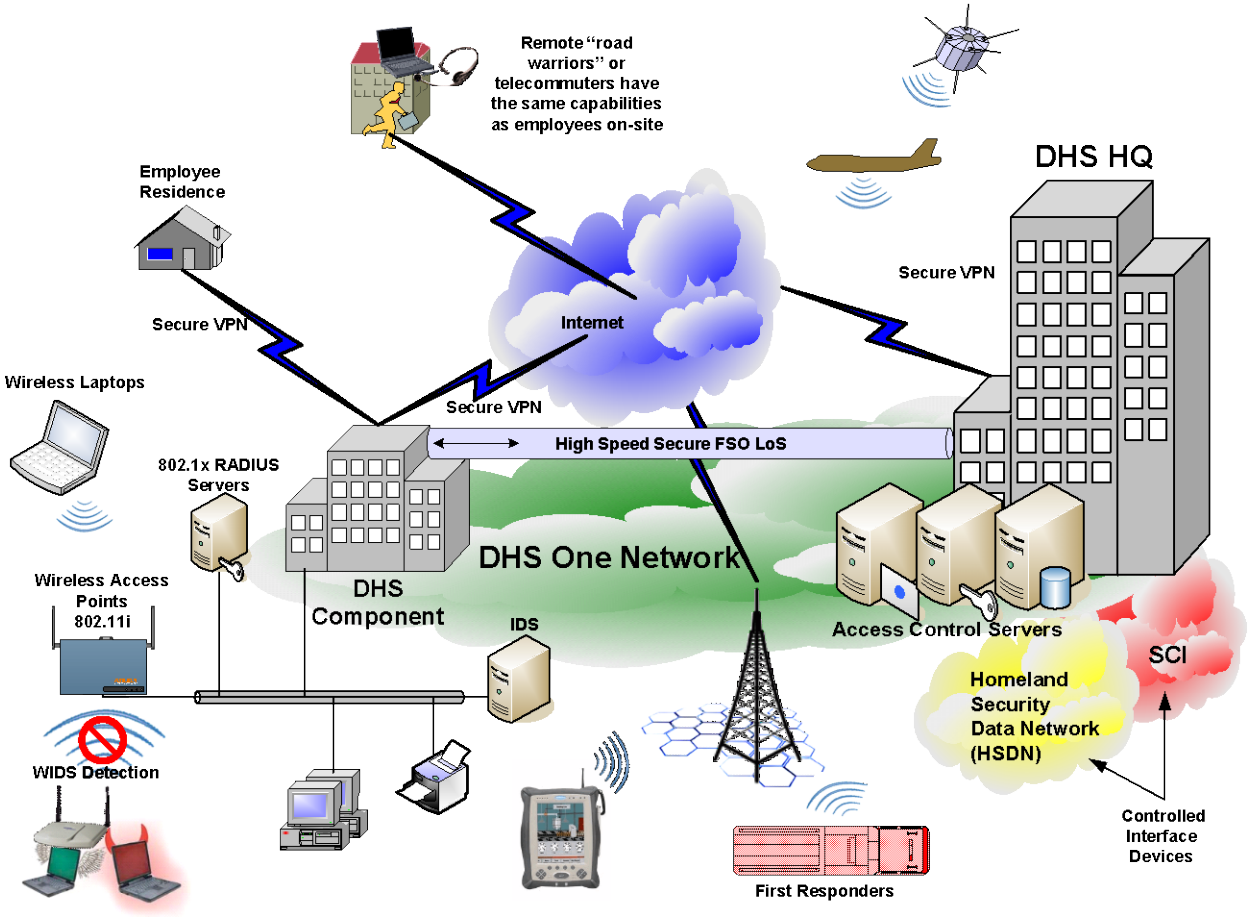


Diagram B-2. Notional DHS Enterprise Architecture

APPENDIX C – SECURITY REQUIREMENTS CHECKLIST FOR MOBILE SYSTEMS

Mobile Feature and Configuration Guidance			
SECTION 2.0 REQUIREMENTS FOR ALL WIRELESS SYSTEMS			
✓	**Section 2.1: Risk-Based Approach**	**Required**	**Recommended**
	A risk-based approach shall be used to mitigate risks associated with wireless systems.	X	
✓	**Section 2.2: Wireless System Threats and Countermeasures**	**Required**	**Recommended**
	Sensitive wireless systems shall have the capability to detect, locate, and identify attacks, as well as to capture transmissions for forensic analysis.	X	
	Security guidelines for layers of the Open Systems Interconne ction (OSI) model are followed when designing and implementing wireless sysstems.		X
✓	**Section 2.3: Authentication**	**Required**	**Recommended**
	Wireless systems shall employ IEEE 802.1X port-based authentication methods.	X	
	Every system administrative password shall be changed to a strong password that complies with overarching organization password conventions defined in DHS 4300A.	X	
	Systems should not operate using default factory passwords; these must be changed prior to the system being put into operational use.		X
✓	**Section 2.4: Confidentiality**	**Required**	**Recommended**
	Wireless systems shall use the FIPS 140-2 validated AES-256 encryption to protect the confidentiality of data.	X	
	The use of static keys should be avoided.		X
	Dynamic key rotation should be used in conjunction with an enterprise RADIUS server.		X
	End-to-end encryption shall be implemented across wireless and wired networks to protect the confidentiality of data.		X
✓	**Section 2.5: Integrity**	**Required**	**Recommended**
	FIPS 140-2 validated hash routines and security controls should be used to ensure data have not been modified in an unauthorized or accidental manner.		X
	Protocol built-in integrity capabilities should be enabled to ensure data integrity.		X
✓	**Section 2.6: Management Control**	**Required**	**Recommended**
	A centralized wireless management control structure shall be used that is integrated with the existing wired network.	X	
✓	**Section 2.7: Physical Security**	**Required**	**Recommended**
	Each wireless infrastructure device should be installed in a secured enclosure or space that is resistant to tampering, theft, and unauthorized access to console ports, power supplies, and reset buttons.		X

Mobile Feature and Configuration Guidance			
	Guards who routinely patrol the facilities should visually inspect AP enclosures.		X
	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
☐	**Section 2.8: National Information Assurance Partnership Common Criteria Security Validations**	**Required**	**Recom-mended**
	DHS administrators should carefully evaluate products to ensure that security validations have been performed and that the products conform to commonly used PPs.		X
	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
	Protocols that send clear text passwords, or otherwise do not use a secure protocolsuch as Telnet, HyperText Transport Protocol (HTTP), Simple Network Management Prot0ocol (SNMP) v1/2, and Cisco Discovery Protocol (CDP), are not used as a means of in-band device management. that are enabled by default and are not essential to mission requirements should be disabled.		X
	Ports, protocols, and services that are enabled by default and are not essential to mission requirements should be disabled.		
	Processes 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, or Cisco Discovery Protocol [CDP]), should not be used as a means of in-band device management.		X
	Wireless systems should be tested and inventoried regularly (e.g., quarterly) for compliance with the organization's list of approved ports and protocols.		
✓	**Section 2.9: Logs**	**Required**	**Recom-mended**
	Systems should be configured to create 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
	Log entries should be captured by a remote system on the wired network to make the organization's overall network less vulnerable to attack.		X
	Log management should be addressed in the organization's Security Plan for that system.		X
✓	**Section 2.10: Configuration Control**	**Required**	**Recom-mended**
	Configuration requirements shall be established for wireless networks and devices in accordance with the developed security policies and requirements.	X	
	All sensitive settings for wireless systems should be changed from vendor defaults to protect against unauthorized intrusion and modification of system settings.	X	
✓	**Section 2.11: Software and Firmware Updates**	**Required**	**Recom-mended**
	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 are installed.		X
✓	**Section 2.12: Wireless Monitoring**	**Required**	**Recom-mended**
	The RF signal should be constantly monitored to ensure minimal signal leakage.		X
	WIDP/IPS shall monitor the wireless infrastructure to detect suspicious activities.	X	

Mobile Feature and Configuration Guidance			
✓	**Section 2.14: Traffic Separation**	**Required**	**Recom-mended**
	Traffic from different security trust boundaries shall be logically and/or physically separated.	X	
✓	**Section 2.15: Security Assessment**	**Required**	**Recom-mended**
	Regular (at least annual) security assessment shall be performed to assess the wireless system security capabilities and discover any potential vulnerability.	X	
✓	**Section 2.16: Security Incident Response**	**Required**	**Recom-mended**
	The security incident response standard operating procedures (SOP) shall specify methods for wireless system users and other personnel to report security incidents in accordance with DHS 4300A.	X	
	Secton 2.17: Security Awareness Training	**Required**	**Recom-mended**
	In accordance with DHS Sensitive Systems Policy Directive 4300A, Components provide annual wireless security awareness training. The security awareness training may be combined with similar training for other systems and may be provided during an employee's orientation program.		
	Technical training of personnel shall include hands-on instruction on how to operate the wireless systems or devices assigned to them within the context of their roles and responsibilities.		
	All employees who use or administer the wireless system shall complete security awareness training prior to use of the system.		
	evidence of completion submitted to the Information System Security Manager (ISSM) of the program or the appropriate security authority.		
	Components should create Rules of Behavior (ROB) agreements that specifically cover policies and procedures for wireless systems.		
	users are required to receive a Rules of Behavior document whenever rights to access wireless systems are first granted and again during annual inventory re-certifications.		
	Component policies and procedures for wireless systems should ensure that Policies and procedures should ensure that all users sign and return a Rules of Behavior document when their wireless system access is first issued.	X	
Section 3.0: WLAN Security Guideline			
✓	**Section 3.1: Security Approach**	**Required**	**Recom-mended**
	WLAN systems shall 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	
	WLAN systems shall use the IEEE 802.11w security standard if such standard is supported by the systems	X	
✓	**Section 3.2: WLAN Network Naming Conventions**	**Required**	**Recom-mended**
	The WLAN network name should be changed from the default name to a unique name that does not reveal DHS sensitive information.		X
✓	**Section 3.3: ESSID Broadcasting**	**Required**	**Recom-mended**
	The wireless automatic connection capability should be disabled.		X
	DHS wireless users should not connect to any unknown wireless networks.		X

Mobile Feature and Configuration Guidance			
✓	**Section 3.4: Access Control**	**Required**	**Recommended**
	Two-factor 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
	WLAN systems should implement 802.1X or equivalent network access control solutions as well as or in conjunction with EAP-TLS mutual authentication.		X
	The NAC system should have the ability to identify users and their devices and apply access control accordingly.		X
✓	**Section 3.5: Encryption**	**Required**	**Recommended**
	Static WEP encryption offered by 802.11-based networks should NOT be used.		X
	WLAN systems shall implement a NIST FIPS-approved mode with AES-256 encryption.	X	
	Systems that provide per-session dynamic RC4 keys, such as dynamic WEP, temporal key integrity protocol (TKIP), and WPA, are not FIPS 140-2 approved and thus shall NOT be adopted.		X
✓	**Section 3.6: WIDS**	**Required**	**Recommended**
	WIDS has these capabilities: • Performs direction finding/triangulation to locate unauthorized AP or other wireless devices • Tracks the connection status of all clients • Detects bridging connections from wireless to the wired network directly in a wireless end-user device • Detects any RF interference sources with physical location information	X	
✓	**Section 3.7: WIPS**	**Required**	**Recommended**
	WIPS blocks or removes wireless end-user devices that have been determined to be a threat on the WLAN.	X	
✓	**Section 3.8: Official Visitor Network**	**Required**	**Recommended**
	A separate wireless network infrastructure is used for official visitors—either logically or physically separated from the DHS internal wireless or wired networks.	X	
	Official visitors accepts pre-defined DHS wireless use terms and conditions prior to accessing the visitor network. Content filtering, monitoring, logging, and other security measures should be deployed for the visitor network.	X	
	Records are maintained to demonstrate that all official accept pre-defined DHS wireless use terms and conditions prior to accessing the visitor network.	X	
	Content filtering, monitoring, logging, and other security measures are deployed for the visitor network.		X
✓	**Section 3.9: Perimeter Security**	**Required**	**Recommended**
	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 DHS IT Security Policy.		X

Mobile Feature and Configuration Guidance			
✓	**Section 3.10: Radio Coverage and Power Control**	**Required**	**Recommended**
	RF footprint and power output are adjusted to minimize RF leakage; for instance, a signal-to-noise ratio (SNR) of 25 decibels (dB) for data service (allowing a data rate of about 10 megabits per second [Mbps]) and 35 dB or more for Voice over Internet Protocol (VoIP) are two common parameters for acceptable wireless services.		X
SECTION 4: FIXED ACCESS WIRELESS NETWORKS			
✓	**Section 4.0: Bridge Configuration**	**Required**	**Recommended**
	Bridge devices should be configured to accept connections only from other bridge devices and not from client devices.		X
✓	**Section 4.1: Bridge Link Confidentiality**	**Required**	**Recommended**
	FIPS 140-2 validated products using AES-256 are used to secure link-level communications between bridges.	X	
✓	**Section 4.2: Bridge Link Authentication**	**Required**	**Recommended**
	Bridges provide a mechanism to mutually authenticate each other before communications are established and periodically during the communications.		X
	Bridges provide a mechanism to ensure data integrity.		X
	MAC-address-based access control capabilities are configured on all bridges so that any connection from any other bridge that is not specifically allowed will be denied by default.		X
✓	**Section 4.3: Bridge Ratio Coverage Recommendations**		**Recommended**
	Bridge RF footprint and power output are adjusted to minimize RF leakage		X
SECTION 5.0: WWAN			
✓	**Section 5.1: WWAN Built-in Security Features**	**Required**	**Recommended**
	WWAN built-in security features are enabled.		X
✓	**Section 5.2: Private WWAN**	**Required**	**Recommended**
	DHS encryption, authentication, and security control standards are applied to the private WWAN.	X	
✓	**Section 5.3: Remote Access Through VPN Service**	**Required**	**Recommended**
	DHS remote access security guidelines and procedures are followed when users access DHS internal resources via commercial WWAN.	X	
SECTION 6.0: WIRELESS PERSONAL AREA NETWORKS: SECURITY			
✓	**Section 6.1: Ad Hoc and Peer-to-Peer Networks**	**Required**	**Recommended**
	Strict configuration restriction of ad hoc and peer-to-peer networks on client devices are enforced.		X
	Ad Hoc and peer-to-peer networks are disabled immediately when they are no longer necessary.		X

Mobile Feature and Configuration Guidance			
	A regular (e.g., weekly) scan and audit are performed to ensure that unauthorized Ad Hoc and peer-to-peer networks are identified and disabled.		X
	Section 6.2: Devices	**Required**	**Recom-mended**
	Any WPAN capabilities that are not required by users are deleted or disabled.		X
	Security personnel are properly trained to recognize PAN-capable devices and be familiar with disabling PAN functions in those devices.		X
	Weekly scan and audit for these devices are being performed to ensure the proper enforcement of DHS policies and procedures.		X
✓	**Section 6.3: Coverage and Power Requirements**	**Required**	**Recom-mended**
	The RF footprint and power output of devices are adjusted to minimize RF leakage.		X
✓	**Section 6.4: Bluetooth Device Communication Risks and Recommendations**	**Required**	**Recom-mended**
	IT security managers ensure that Bluetooth communications are conducted in an environment where information exchanged cannot be captured by eavesdroppers.		X
	Communication are restricted to private areas where there is limited RF signal propagation.		X
	To prevent devices from advertising themselves to would-be attackers, devices are configured for the non-discoverable mode unless the user is in the process of pairing Bluetooth devices.		X
	To avoid increased risks of vulnerable points of entry, multiple or split communications paths are not allowed for the same client device.		X
	The strongest security mode is used for Bluetooth communications. Details can be found in the NIST SP 800-121 for various Bluetooth versions.	X	
✓	**Section 6.5: Personal Identification Number Protection**	**Required**	**Recom-mended**
	IT security managers 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
✓	**Section 6.6: Disabling Unwanted Profiles**	**Required**	**Recom-mended**
	Unnecessary WPAN profiles are disabled to reduce the points of access an attacker might exploit.		X
	Organizations operate under the principle of least privilege and only enable functionality that users absolutely require for day-to-day operations.		X
	SECTION 7.0: INTEROPERABILITY		
✓	**Section 7.3: Wireless Standards**	**Required**	**Recom-mended**
	Only IEEE 802.11 a/b/g/n standards are used for wireless device data communication.	X	
	Only Wi-Fi Alliance WPA2 Enterprise certified devices are deployed, which is based on IEEE 802.11i standard.	X	
	Only IEEE 802.1X standards-based WLAN identification and authentication methods are used.	X	
	WLAN systems use the IEEE 802.11w security standard if such standard is supported by the systems.	X	

APPENDIX D – WIRELESS SYSTEM RULES OF BEHAVIOR USER AGREEMENT

The following rules describe when and how to use your access to wireless systems.

- Use **Government**-owned wireless systems only for authorized and official Government functions and such private functions as are specifically authorized by regulation.
- Use only **Government**-owned wireless systems to access **sensitive** information or connect to **DHS** systems.
- Comply with all copyright and licensing requirements associated with the use of wireless systems.
- Use personal firewalls, anti-virus software, and other protective mechanisms as required by DHS security policy and procedures. Update the virus protection software and its virus signature files at least weekly.
- Ensure that unauthorized persons cannot view the screen if it contains sensitive information.
- Remove all personal and sensitive information when returning a wireless device to government custody.
- Do not share or loan account passwords or permission to access **Government**-issued wireless devices.
- Do not load or run unauthorized software on wireless systems or wireless devices.
- Do not make any changes to the wireless system configuration unless directed to do so by an authorized System Administrator.
- Do not program wireless systems with sign-on sequences, passwords, or access telephone numbers.
- Do not leave a wireless device unattended, especially while it is unlocked/logged in. Follow published locking and log-off procedures.
- Do not use wireless systems in areas where classified information is processed or discussed.
- Do not use wireless systems containing audio, video, or photographic recording and/or transmission capabilities in areas where classified information is processed or discussed.

Wireless Device Protection

- Assume responsibility for taking all necessary precautions to protect wireless systems and data against loss, theft, damage, abuse, or unauthorized use by employing lockable cases and keyboards, locking cables, and removable media drives.
- Keep the wireless device under physical control at all times, or secure it in a suitable locked container under your control.

Identification and Authentication (I & A)

The following rules address passwords on wireless systems:

- Follow DHS policy on password management.
- Protect passwords from disclosure.
- Ensure that no one can observe the entry of passwords.
- Promptly change a password whenever compromise of that password is known or suspected.

- Do not attempt to bypass I&A measures implemented at the device and network levels.
- Do not store passwords, access numbers, or smart cards with the wireless system.
- Do not record passwords on paper or in electronic form or store them with or on the wireless system.

Data Protection

- Protect sensitive information from disclosure to unauthorized persons or groups.
- Use only Government Furnished Equipment to access sensitive DHS information, unless the AO has previously provided written authorization.
- Do not access, process, or store classified information on wireless systems without proper authorization.

Encryption and Public Key Infrastructure (PKI)

- Comply with DHS encryption and PKI requirements.
- Transmit data using wireless systems that rely on wireless encryption protocol (WEP) and/or use commercial wireless network providers only if the data is encrypted end-to-end using AES-256 VPN encryption.
- Do not shut down, disable, or reconfigure the encryption software or alter file permissions or policy settings in any way that might affect the encryption software or its proper operation.

Network Connectivity

- Use only Government-issued wireless devices to access sensitive DHS information or connect to DHS systems.
- Follow DHS policy on connecting computers and wireless systems to networks, including the Internet.
- Use only DHS-authorized Internet connections that conform to DHS security and communications standards.

Incident Reporting

- Immediately report confirmed or suspected security issues (e.g., operational anomalies, security violations, a missing or stolen wireless device, compromise of the encryption software) via established procedures for reporting security issues.

Traveling with a wireless device

- Back up all files before traveling.
- Keep the wireless device under your physical control at all times when traveling.
- Never place the wireless device in checked luggage.
- Never store the wireless device in an airport, train station, bus station, or any public locker.
- If leaving the wireless device in a car, lock it in the trunk out of sight.
- Avoid leaving the wireless device in a hotel room. If necessary, lock it inside another piece of luggage.
- Be prepared for airport security checks. Have the wireless device’s batteries charged or a power cord handy so you can demonstrate that it is functional.

- Heighten vigilance at any security or luggage-scanning checkpoint. Place your wireless device on the conveyer belt only after the belongings of person ahead of you have cleared the scanner. If you are delayed, keep your eye on the wireless device.
- Exercise diligence when traveling in foreign countries because criminals or local intelligence may target your wireless device for the information it contains.
- Do not display any sensitive information on the wireless device screen when in any public place, such as an airport terminal, train or bus station, airplane, train, bus, or taxi.

Working From Home or an Alternate Workplace

- Implement security standards for hardware, software, and information to be used at the alternate workplace that are equivalent to those at the primary workplace.
- Provide physical security to protect the wireless system when not in use.

Consent Statement

I, _____, have read and understand the Rules of Behavior that apply to laptop computers and portable electronic devices. I agree to abide by these rules. I understand that failure to abide by these rules may result in disciplinary action.

I understand that DHS reviews telecommunications logs, computer logs, and telephone records and that it conducts spot-checks to determine compliance with controls placed on DHS IT resources.

I understand that I may acquire and use Sensitive information only in accordance with established policies and procedures. This includes properly destroying Sensitive information contained in hardcopy or softcopy and ensuring that Sensitive information is accurate, timely, complete, and relevant for the purpose for which it is collected, provided, and used.

I understand that any questions I may have regarding the security of wireless systems and data will be directed to my supporting Information Systems Security Officer (ISSO).

I acknowledge receipt of and understand my responsibilities for the use of DHS resources and will comply with the Rules of Behavior.

_____

Printed Name Organization

_____

Signature Date

Return this signed statement to _____ and retain a copy for your personal records.