U.S. Customs and
Border Protection

Attachment Q2

Sensitive Portable Electronic Devices

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 the use of wireless portable electronic devices (PED) within the Customs and Border Protection (CBP) Information Security Program. This document is structured as part of the CBP Information Systems Security Policies and Procedures Handbook, 1400-05D document compilation. Additional wireless security requirements involving other wireless communications subsets can be found within this compilation. This handbook serves as a foundation for wireless infrastructure components to use in developing and implementing their Information Technology (IT) security programs. It incorporates many of the procedures in use by security personnel from the Departmetn of Homeland Security (DHS), as well as other federal entities that have previously established wireless security foundations such as the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the Department of Defense (DoD).

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. 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 Chief Information Security Officer (CISO) to ensure consistency in the development and application of risk management approaches and certification and accreditation (C&A) processes for wireless services and technologies. The WSB also assists the 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 the DHS. This collaboration ensures that the WMO is effectively managing the Department's wireless security risks.

1.1 Purpose and Scope

Because of the rapid evolution in wireless technology, dissimilarities between wireless PEDs, and multiple vendors' product offerings, specific wireless PEDs may or may not have the ability to be made wholly compliant with the countermeasures outlined in this handbook. The guidelines set forth in this document are intended to further outline policy requirements and to provide a detailed explanation of the many countermeasures that can be applied to wireless PEDs. The Authorizing Official (AO) should pay particular attention to the potential risks that must be considered in approving PEDs that have technological barriers that prevent the adoption of these countermeasures. The AO should understand the risks associated with a particular wireless PED. This may include applying some, but not all of the outlined countermeasures, while ensuring that the risk is measured and brought down to an acceptable level as outlined within policy. In addition, the System Security Plan should address all applicable and effective security controls required for authority to operate.

Although this handbook addresses safeguards applicable to all PED platforms, PEDs commonly include—

- Cellular telephones
- Wireless-enabled laptop computers
- Two-way pagers
- Multifunction wireless devices.

A security checklist is provided in Appendix A.

1.2 Authority

This handbook is issued as user guidance under the authority of the CBP Chief Information Officer through the CBP CISO. This handbook addresses the use of PEDs only. Prior directives shall remain in effect until the new DHS and CBP policy and implementing guidance are issued.

1.3 Terminology

Within Attachment Q2, the use of the word “shall,” “will,” or “must” shall be considered mandatory only in as it applies to existing DHS policy elements. “MAY” or “SHOULD” indicates a non-mandatory action or condition.

1.4 1400-05D Policy Requirements

Wireless PEDs include wireless-capable laptop computers, personal digital assistants (PDA), smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services (PCS) devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices, and any other wireless clients capable of storing, processing, or transmitting sensitive information.

1.4.a. CBP policy states that personally owned equipment and software SHALL NOT be used to process, access, or store sensitive information without the written prior approval of the AO.

1.4.b. Only government furnished equipment (GFE) that has been properly configured by CBP-managed services SHALL be authorized for use on CBP wireless systems.

1.4.c. All contractor-owned or personally owned PEDs SHALL be prohibited for use on CBP wireless systems and must not be allowed to communicate directly with CBP systems.

1.4.1 Security Incident Response

Most security controls are designed to protect an organization against security threats; however, regardless of how effective those controls are, some security incidents are inevitable. Organizations need to have an effective response capability in place before the occurrence of such events.

1.4.1.a. The security incident response standard operating procedures (SOP) SHALL specify methods for PED users and other personnel to report security incidents, including a lost or stolen PED, in accordance with CBP 1400-05D, Attachment F.

1.4.1.b. One of the methods SHALL be via a telephone call to a security operations center or on-call security operations personnel.

1.4.1.c. The security incident response capability SHALL be available on a continuous basis (i.e., 24 hours a day, 365 days a year).

1.4.2 Security Awareness Training

The goal of security awareness and training is to protect the confidentiality, integrity, and availability of CBP IT assets and data.

1.4.2.a. Components are reminded that 4300A requires that appropriate awareness training SHALL be provided.

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

1.4.2.c. Each person's technical training SHALL include hands-on instruction on how to operate the PED assigned to him/her within the context of his/her roles and responsibilities.

1.4.2.d. All employees who use or administer the PED SHALL complete the security awareness training prior to use of the system. The security awareness training may be combined with similar training for other systems and may be provided during an employee's orientation program.

1.4.2.e. Such security awareness SHOULD be repeated on an annual basis and evidence of completion SHOULD be submitted to the Information System Security Manager (ISSM) of the program or the appropriate responsible security authority.

1.4.3 Wireless Portable Electronic Devices

The following tables are found in Section 4.0 of the CBP Information Systems Policies and Procedures Handbook.

Section 4.6.2.0
a. The use of wireless PEDs and accessory devices in areas where sensitive or classified information is discussed is prohibited unless specifically authorized by the AO in writing.

Section 4.6.2.0
b. Wireless PEDs shall not be connected physically or wirelessly to the CBP-wired core network without written consent from the AO.
c. Wireless PEDs shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats.
d. Wireless PEDs such as BlackBerry devices and smartphones shall implement strong identification, authentication, data encryption, and transmission encryption technologies. Portable electronic devices such as BlackBerry devices and smartphones shall be password-protected, with a security timeout period established. For BlackBerry devices, the security timeout shall be set to 10 minutes.
e. System Security Plans shall promulgate the provisions, procedures, and restrictions for using wireless PEDs to download mobile code in an approved manner.
f. Wireless PEDs shall be operated only when current CBP Technical Reference Model (TRM)-approved versions of antivirus software and software patches are installed.
g. Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless PED being approved for use.
h. A current inventory of all approved wireless PEDs in operation shall be maintained.
i. Wireless PEDs shall be cleared of all information before being reused by another individual, office, or Component within DHS or before they are surplused; wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using approved procedures.
j. Legacy wireless PEDs that are not compliant with CBP IT security policy shall implement a migration plan that outlines the provisions, procedures, and restrictions for transitioning these wireless PEDs to CBP-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS and CBP CISO, as appropriate.
k. Personally owned PEDs shall not be used to process, store, or transmit sensitive CBP information.
l. The AO shall approve the use of government-owned PEDs to process, store, or transmit sensitive information.
m. The use of add-on devices such as cameras and recorders is not authorized unless approved by the AO. Functions that can record or transmit sensitive information via video, IR, or RF shall be disabled in areas where sensitive information is discussed.

Table 1: Wireless Portable Electronic Devices Policy

Section 4.6.2.1
a. Guidance for discussing sensitive information on cellular phones shall be developed. Guidance shall be approved by a senior CBP official and is subject to review by the DHS CISO and the DHS Wireless Management Office. Under no circumstances shall classified national security information be discussed on cellular phones.

Comment [AU1]: Verify

Table 2: Cellular Phones Policy

Section 4.6.2.2
a. Pagers shall not be used to transmit sensitive information.

Comment [AU2]: Verify

Table 3: Pager Policy

Section 4.6.2.3
a. Functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information.
b. Functions that transmit or receive video, infrared (IR), or radio frequency (RF) signals shall be disabled in areas where sensitive information is discussed.
c. Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used and shall be disabled when possible.

Comment [AU3]: Verify

Table 4: Multifunctional Wireless Device Policy

2.0 THREAT OF OVERVIEW

PEDs are increasingly commonplace in many infrastructures because they offer benefits in communication and collaboration while remaining location independent. However, PEDs require strict security controls and governance to combat the rising threat these devices pose to infrastructure resources.

2.1 Wireless Threats and Vulnerabilities

Wireless communications employs an inherently insecure medium because it cannot be physically secured from interception or protected against jamming. In addition, many components restrict PED use to senior management; therefore, the unauthorized disclosure of PED data-at-rest or data-in-transit could reasonably be expected to cause damage to national security.

2.1.1 Taxonomy of Wireless Attack Devices

Wireless systems are vulnerable to specifically engineered wireless attacks and to traditional wireline attacks. Attacks are categorized according to the following basic threat consequences: unauthorized disclosure, disruption, deception, and corruption. Generally, attacks fall into one of two categories: active or passive attacks. Active attacks require actions on the part of the attacker to penetrate or disrupt the network, whereas passive attacks are used primarily for information gathering and surveillance. Figure 1 illustrates this taxonomy.

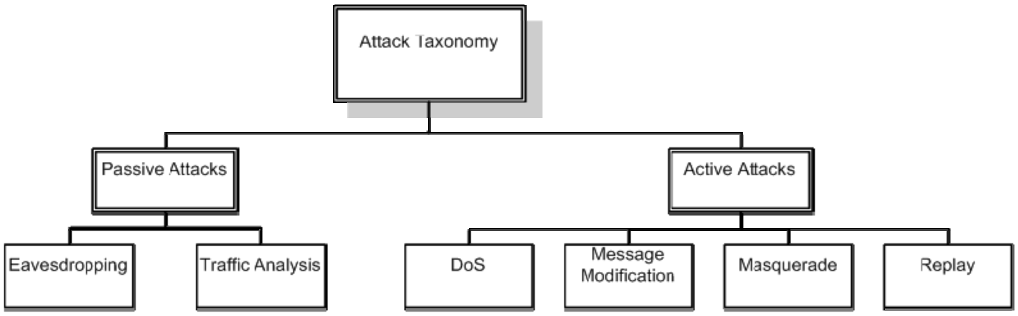

Figure 1: Taxonomy of Wireless Device Attacks

3.0 SECURING THE PHYSICAL DEVICE

Although the wireless PED is considered to be a critical component within the wireless local area network (WLAN), it is often overlooked as a network component. The device should be looked upon as an extension of the CBP network. One of the critical risks associated with the device lies in authentication of the user to the device. Approved PED software may be found at the CBP Technical Reference Model (TRM)

3.1 Authentication

Identification and authentication will be implemented at the device, network, and application layers.

3.1.a. Wireless PEDs SHALL implement password protection for device access.

3.1.b. PED authentication mechanisms should not be configured for automatic access, and PEDs SHALL require device re-authentication after the 10-minute timeout.

3.1.c. PED passwords SHALL use a minimum of eight characters, consisting of both alphanumeric and special characters, and SHOULD be able to resist dictionary-based attacks.

3.2 Virus Protection

The AO will approve anti-virus software for wireless PEDs but software support may vary based on the platform. In the event that suitable anti-virus software cannot be obtained for a particular PED, features must be disabled to make the PED more secure or the PED should be prohibited from use. For example, disabling e-mail attachments, Java 2 Platform Micro Edition (J2ME) support, and the Web browser can substantially lessen the likelihood that malicious mobile code will be downloaded to the device.

3.2.a. Anti-virus software SHOULD be centrally managed and continuously updated on PEDs to prevent the transfer of malicious mobile code (e.g., viruses, Trojan horses, key loggers).

3.2.b. Companion devices that provide personal information management (PIM) synchronization SHOULD have anti-virus software installed so that mobile code is not transferred between the PED and the companion device.

3.2.c. If no suitable anti-virus software exists for a particular PED, then the AO SHOULD take this into consideration when approving or disapproving the adoption of the PED.

3.3 Disabling of PED Capabilities and Unwanted Applications

Capabilities, if left in default configuration, can serve as unprotected attack vectors to the PED or trusted network. Wireless capabilities that may not be required include Infrared, Bluetooth, WiMAX, Wi-Fi, games, instant messaging, and synchronization tools. Appendix A provides recommended security settings.

3.3.a. Unapproved or unnecessary PED capabilities and applications SHOULD be disabled or removed whenever possible.

3.3.b. Additional integrated capabilities, such as cameras and recording mechanisms, pose significant levels of risk and SHOULD be disabled, unless specifically required, in order to mitigate the risk of exposing sensitive information.

3.3.c. Short Message Service (SMS) and MMS pose significant levels of risk and SHOULD be disabled, unless specifically required, in order to mitigate the risk of exposing sensitive information. For example, PocketPC or Windows Mobile telephones are able to send their MMS messages over their cellular or 802.11 wireless interfaces. This enables an attacker to bypass any sanitizing that a cellular carrier may perform on MMS messages.

3.3.d. As wireless convergence continues to increase, capabilities or functions SHOULD be restricted to specific wireless interfaces whenever possible. Securing the wireless link is discussed in Section 4.0.

3.3.e. CBP-issued PEDs SHALL be distributed and restricted to an approved baseline configuration.

3.3.f. Personal PEDs SHALL NOT be used to connect to CBP resources, i.e., e-mail, file shares, etc.

3.4 PED Configuration Management

IT security managers will limit PED deployment to NSA- and CBP-sanctioned devices, technologies, and applications. Depending on the PED platform, many updates can be centrally pushed to mobile users' PEDs. These automated updates should be sensitive to low-bandwidth considerations and provide mechanisms to roll back updated files and configurations if update-related failures occur. Configuration management systems that include remote disable and remote zeroise (i.e., a kill command) features should be implemented.

3.4.a. Changes to physical PED components SHALL adhere to CBP policies and security protocols.

3.4.b. The use of static IP addresses SHOULD be used for IP-based wireless PEDs (clients and access points [AP]).

3.4.c. Configuration management of the mobile devices SHALL be maintained, taking into account authorized network interface cards (NIC) and media access cards (MAC), and the sporadic nature of mobile device connectivity.

3.4.d. Wireless PED configuration management SHOULD include secure updates to security policies and user profiles where possible.

3.5 Data Protection

The AO ensures that all information stored on PEDs is encrypted using NIST-validated encryption schemes consistent with the sensitivity of the information stored on the device. Implementing countermeasures such as file and data encryption helps to ensure the confidentiality of information residing on the device.

3.5.a. Applications such as file sharing SHOULD be disabled on applicable PEDs, and all file sharing ports should be blocked in both directions, especially when processing sensitive information.

3.5.b. Where possible, data protection SHOULD be extended to include PIM databases, telephone contact lists, text messages, and temporary browser files.

3.5.c. Wireless PEDs SHALL encrypt all data-at-rest by securing either the individual files or the file system (operating system or storage partition), including removable media.

3.6 Monitoring of System Files

IT security managers implement mechanisms that periodically scan for unauthorized changes to system files or other critical files on all PEDs.

3.6.a. These mechanisms SHOULD perform system file integrity checks automatically, such as routinely comparing a cryptographic hash of the current system files on the PED to a “known good” previously recorded hash.

3.7 Device Synchronization and Backup

Wireless PEDs must use products or modules using NIST Federal Information Processing Standard (FIPS) 140-2 evaluated encryption when synchronizing wirelessly.

3.7.a. PEDs SHOULD periodically synchronize and back up all stored information. Recommended intervals are daily for incremental data backups and weekly for full data backups.

3.7.b. A replacement device SHOULD support full restoration functionality of the archived file(s) to limit the downtime and loss of productivity possible after an attack or loss has taken place.

3.7.c. Wireless capabilities SHOULD be disabled during hot-synchronization operations with companion devices.

3.7.d. Only a single network connection (wired or wireless) SHOULD be active at any one time in order to prevent unauthorized connections among multiple networks.

3.8 Recommended Maintenance Activities

PEDs will be data sanitized or zerosied when retired. It is important to note that a soft or hard reset will not permanently erase the device's data. Deleting files via a file management utility will also not permanently remove files.

3.8.a. Data SHALL be properly sanitized by degaussing, overwriting, or destroying the hardware.

3.9 Recommended Safeguards for Travel

Recommended Safeguards for Travel are detailed in Section 9 of APPENDIX D: RULES OF BEHAVIORS for PEDs.

4.0 SECURING THE WIRELESS LINK

The wireless interface is a critical component in the WLAN. This point—the link between a wireless PED and a network endpoint or between two wireless PEDs—is vulnerable to hackers.

4.0.a. Wireless communication cannot be protected from intercept; however, controls SHALL be implemented to prevent the unauthorized disclosure of information. Not all receivers of the signal will be authorized users; therefore, security mechanisms SHALL be put into place to protect wireless resources and data.

4.0.b. Users SHALL adhere to CBP policy and refrain from peer-to-peer associations unless approved by the appropriate AO.

4.0.c. AOs SHOULD ensure proper authentication and encryption mechanisms are implemented to ensure data integrity, confidentiality, and availability.

4.0.d. PEDs SHOULD indicate when the device is operating in encrypted versus unencrypted modes, i.e., by use of an icon, symbol, or even a blinking light. Approved PED software may be found at the CBP Technical Reference Model (TRM).

4.1 Authentication

All PEDs require mutual network identification and two-factor authentication.

4.1.a. Authentication SHALL be required at power-up and PED network and resource access SHOULD be challenged (through re-authentication) as often as possible, dependent on the capability of the operating environment.

4.1.b. CBP SHOULD configure systems to lock a user's account for 20 minutes after three consecutive failed logon attempts.

4.1.c. The authentication mechanisms SHALL include strong password protection and SHOULD be combined with the use of a smart card or biometrics authentication.

4.1.d. Administrators SHOULD be aware that the access control mechanisms supported by many wireless systems identify client stations and not users. Unauthorized users may gain access through lost or stolen devices or by a combination of the attacks documented earlier in Section 2.0.

4.1.e. Authentication mechanisms SHALL be put into place to require smart cards, certificates, or security tokens to verify a user's identity.

4.1.f. Identity management systems SHOULD authenticate wireless users and take full advantage of any existing public key infrastructure when accessing CBP resources. Identity Access Management is further detailed in the *DHS IT Security Program Handbook for Sensitive Wireless Systems* and *DHS IT Security Architecture Guidance Application Infrastructure Design, Volume III.*

4.2 End-to-End Secure Communications

End-to-end security means that the entire message is encrypted from sending device to receiving device. Both devices must explicitly meet FIPS 140-2. Secure Sockets Layer (SSL), Internet Protocol Security (IPSec) virtual private network (VPN), and Secure Shell (SSH) are common methods of providing end-to-end encryption. Although hackers may be able to determine that there is traffic on the network, the information transmitted is encrypted and unreadable. SSL and SSH are also used for additional applications such as e-mail and telnet. The use of certificates is also essential in the implementation of strong end-to-end encryption. Users need to be conscious of security warnings indicating a certificate error.

4.2.a. Users SHOULD be trained not to ignore warning messages and to report suspicious activity. For more information regarding incident response, see Section 1.0.

4.2.b. Encryption keys stored on client stations SHALL be protected from unauthorized disclosure. The use of dynamic keys is highly recommended and SHOULD include Extensible Authentication Protocol (EAP). Using dynamic keys helps to mitigate the risks associated with shared static keys.

4.2.c. The symmetric-encryption keys (128-bit) SHOULD be used to protect all information transmitted across the medium. Technologies such as IPSec VPN incorporate the use of public key cryptography and inherently use dynamic key exchange to set up the encrypted VPN tunnel.

4.2.d. Key distribution SHALL occur over a secure channel to minimize the risk of compromise. Also, Wireless Protected Access (WPA) should be active for all WLAN connections and will only be changed by the Information Security group or other similarly authorized personnel.

4.3 Personal Firewalls

Personal firewalls are software-based solutions that reside on a client machine and are either client managed or centrally managed. A firewall helps secure the PED from unauthorized access by blocking specific types of inbound and outbound network traffic. Client-managed versions are not recommended because users can easily circumvent security settings. Managed IT solutions standardize department-wide PED protection because IT departments can centrally configure and remotely manage client devices. Although personal firewalls offer some measure of protection, they do not protect against all advanced forms of attack. Users who access public wireless networks in airports or conference centers, for example, should also use a VPN.

4.3.a. Personal firewalls SHOULD block access to high-risk ports.

4.3.b. Personal firewalls SHOULD enable audit logging.

4.4 Virtual Private Network

Networks that are maintained by third parties increase typical security concerns given they are not maintained by the CBP. For example, cellular infrastructure facilities are often not owned by the cellular operator and are accessible to several different operations and maintenance subcontractors.

4.4.a. Wireless PED communications that move between third-party networks and the CBP network SHOULD be considered inherently untrustworthy, given the lack of network control and the public nature of these networks.

4.4.b. VPNs SHOULD be implemented with NIST FIPS 140-2 validated encryption and appropriate key management mechanisms. A list of FIPS 140-2 validated products may be found at http://csrc.nist.gov/cryptval/140-1/140val-all htm and at the CBP Technical Reference Model (TRM).

4.4.c. Remote access of personally identifiable information SHALL comply with all CBP requirements for sensitive systems, including strong authentication.

4.4.d. Strong authentication SHALL be accomplished via VPN or equivalent encryption (e.g., Hyper Text Transfer Protocol Secure sockets [https]) and two-factor authentication.

4.5 Intrusion Systems

Intrusion systems are host- and network-based technologies used to protect information assets from exploitation. An intrusion prevention system (IPS) is a proactive technology that makes access control decisions based on application content. An intrusion detection system (IDS) is a more reactive technology that is used to detect attacks as or after they occur. Systems Security Plans shall adopt appropriate network protection mechanisms such as an IDS. Refer to Intrusion Detection section of CBP Information Systems Security Policies and Procedures Handbook for additional information.

4.5.a. CBP system administrators SHOULD routinely scan wireline and wireless networks to determine whether unauthorized PEDs are connected to DHS OneNet.

4.6 Securing the Network Interface

When referring to the network interface or endpoint, two basic components are usually considered, the APs or base stations and the client stations on the network.

> 4.6.a. Other components SHOULD be included in the architecture to provide additional security services, such as authentication servers, firewalls, and VPN concentrators. Refer to the *DHS IT Security Program Handbook for Sensitive Wireless Systems* and *DHS IT Security Architecture Guidance Volumes (I–III)* for more detailed guidance.

Typical PED wireless interfaces are illustrated below in Figure 2. Section 4.0 describes protections for Bluetooth, Wireless LAN, cellular, and companion workstation protection. UWB and IrDA are not discussed in this handbook.

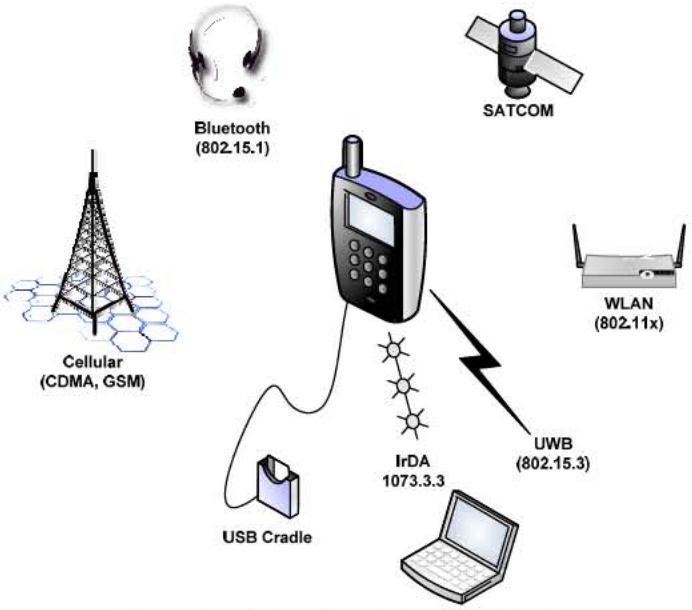

Figure 2: Typical PED Wireless Interfaces

4.6.1 Bluetooth

Bluetooth is an ad hoc personal area network (PAN) technology. Today, it is commonly used for close-proximity voice communications, i.e. wireless headphones. Its most distinguishing feature is its master-slave relationship between networked devices. To facilitate these temporary network connections or partnerships, security is commonly diluted or not implemented. For example, most headsets use "0000" as their password code. Bluetooth-enabled automobiles are also susceptible to wireless attacks because vehicle manufacturers also use a common link-establishment password for their product lines. Bluetooth does offer a link-level security mode (security mode 3), but its security protocol is not FIPS-validated and has known weaknesses. Appendix A of this handbook and *NIST SP 800-48: Wireless Network Security: 802.11, Bluetooth and Handheld*

Devices provide security checklists and greater details regarding Bluetooth operations and its security limitations.

4.6.1.a. Bluetooth SHALL NOT be used for any classified data or voice communications and is discouraged for unclassified use because of its inherently insecure modes of operation.

4.6.2 WLANs

WLAN APs communicate with PEDs equipped with Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless network adaptors. APs characteristically have a radius coverage area. Under highly idealized conditions, an adversary can greatly extend this range via special directional equipment; therefore PEDs network adaptors should be disabled when possible.

4.6.2.a. PED devices SHALL use authentication and encryption mechanisms as required in the *DHS Sensitive Program Handbook for Sensitive Wireless Systems*.

4.6.3 Cellular Technology

A cellular wireless wide area network (WWAN) is a network composed of many small (3- to 5-kilometer) radio cells. Each cell is served by a fixed transmitter at the center of the cell called a base station that connects the mobile PED (via its air interface) to the cellular carrier. The security protection offered by commercial cellular providers does not meet CBP policy requirements; therefore, it is critical for the AO and system owners to ensure that PED system administrators and users are properly trained and that security controls are properly implemented.

4.6.3.a. Wireless PEDs SHALL implement strong identification and authentication controls to access CBP resources and SHALL encrypt all data-in-transit.

4.6.4 Companion Workstations

Companion workstations consist of desktop personal computers (PC), laptops, and additional mobile devices that contain NICs and are able to establish an association with a PED. PEDs can connect to these devices via wireless or wireline connections.

4.6.4.a. The traditional PED device is synchronized to a computer workstation through a universal serial bus (USB) cable. Only one interface SHOULD be active at a time.

5.0 EMERGING TECHNOLOGIES

This section examines emerging security technologies to identify future viable protections that may impact wireless security guidance for wireless PEDs.

5.1 Biometrics and Smart Cards

Biometrics has been introduced as an added layer of security, providing the ability to authenticate users by verifying identity and authorization to gain system access. Some laptops are now available with built-in fingerprint biometrics and smart cards, which allows the user immediate access to sensitive information, eliminating the necessity of having the information stored on a host computer. Although less desirable, USB fingerprint biometric readers are also commercially available to provide authentication to the device, protection of user profiles within the operating system, and encryption services for files and folders. Unlike passwords or public key infrastructure, which require exactly matching credentials for successful authentication, biometrics incorporates a sliding scale of assurance, based on a certain degree of matching, to balance false acceptance with false rejection rates.

5.1.a. Smart cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), SHALL be cost-justified through the risk assessment process.

5.2 Environmentally Adaptable Security Policies

Wireless PEDs should be configured to automatically adapt to changing network environments by switching between different authorized network security policies and applying adaptive controls.

5.2.a. Whenever a PED is outside the corporate network or communicating from an insecure location, capabilities such as VPNs and firewalls SHOULD self-configure to the changing operational environment .

Appendix A

Checklist for Securing Wireless PED

APPENDIX A—CHECKLIST FOR SECURING WIRELESS PEDS

Mobile Feature / Configuration	Required	Recommended
Security Requirements for all Wireless Systems		
1.4 4300A Policy Requirements		
1.4.a. CBP policy states that personally owned equipment and software SHALL NOT be used to process, access, or store sensitive information without the written prior approval of the AO.	X	
1.4.b. Only government furnished equipment (GFE) that has been properly configured by CBP-managed services SHALL be authorized for use on CBP wireless systems.	X	
1.4.c. All contractor-owned or personally owned PEDs are SHALL be prohibited for use on CBP wireless systems and must not be allowed to communicate directly with CBP systems.	X	
1.4.1 Security Incident Response		
1.4.1.a. The security incident response standard operating procedures (SOP) SHALL specify methods for PED users and other personnel to report security incidents, including a lost or stolen PED, in accordance with CBP 1400-05D, Attachment F.	X	
1.4.1.b. One of the methods SHALL be via a telephone call to a security operations center or on-call security operations personnel.	X	
1.4.1.c. The security incident response capability SHALL be available on a continuous basis (i.e., 24 hours a day, 365 days a year).	X	
1.4.2 Security Awareness Training		
1.4.2.a. 1400-05D requires that appropriate awareness training SHALL be provided.	X	
1.4.2.b. Any appropriate wireless security awareness training SHOULD be included in the annual training provided at the component level.		X
1.4.2.c. Each person's technical training SHALL include hands-on instruction on how to operate the PED assigned to him/her within the context of his/her roles and responsibilities.	X	
1.4.2.d. All employees who use or administer the PED SHALL complete the security awareness training prior to use of the system. The security awareness training may be combined with similar training for other systems and may be provided during an employee's orientation program.	X	
1.4.2.e. Such security awareness SHOULD be repeated on an annual basis and evidence of completion SHOULD be submitted to the CISO or the appropriate responsible security authority.		X
3.0 Securing the Physical Device		
3.1 Authentication		
3.1.a. Wireless PEDs SHALL implement password protection for device access.	X	

Comment [AU4]: Fix numbering? Should this be in order?

Mobile Feature / Configuration	Required	Recommended
3.1.b. PED authentication mechanisms should not be configured for automatic access and PEDs SHALL require device re-authentication after the 10-minute timeout.	X	
3.1.c. PED passwords SHALL use a minimum of eight characters, consisting of both alphanumeric and special characters, and SHOULD be able to resist dictionary-based attacks.	X	
3.2 Virus Protection		
3.2.a. Anti-virus software SHOULD be centrally managed and continuously updated on PEDs to prevent the transfer of malicious mobile code (e.g., viruses, Trojan horses, key loggers).		X
3.2.b. Companion devices that provide personal information management (PIM) synchronization SHOULD have anti-virus software installed so that mobile code is not transferred between the PED and the companion device.		X
3.2.c. If no suitable anti-virus software exists for a particular PED, then the AO SHOULD take this into consideration when approving or disapproving the adoption of the PED.		X
3.3 Disabling of PED Capabilities and Unwanted Applications		
3.3.a. Unapproved or unnecessary PED capabilities and applications SHOULD be disabled or removed whenever possible.		X
3.3.b. Additional integrated capabilities, such as cameras and recording mechanisms pose significant levels of risk and SHOULD be disabled, unless specifically required, in order to mitigate the risk of exposing sensitive information.		X
3.3.c. Short Message Service (SMS) and MMS pose significant levels of risk and SHOULD be disabled, unless specifically required, in order to mitigate the risk of exposing sensitive information. For example, PocketPC or Windows Mobile telephones are able to send their MMS messages over their cellular or 802.11 wireless interfaces. This enables an attacker to bypass any sanitizing that a cellular carrier may perform on MMS messages.		X
3.3.d. As wireless convergence continues to increase, capabilities or functions SHOULD be restricted to specific wireless interfaces whenever possible. Securing the wireless link is discussed in Section 4.0		X
3.3.e. CBP-issued PEDs SHALL be distributed and restricted to an approved baseline configuration.	X	
3.3 f. Personal PEDs SHALL NOT be used to connect to CBP resources, i.e. email, file shares, etc.	X	
3.4 PED Configuration Management		
2.4.a. Changes to physical PED components SHALL adhere to DHS policies and security protocols.	X	
2.4.b. The use of static IP addresses SHOULD be used for IP-based wireless PEDs (clients and access points [AP]).		X
2.4.c. Configuration management of the mobile devices SHALL be maintained, taking into account authorized network interface cards (NIC) and media access cards (MAC), and the sporadic nature of mobile device connectivity.	X	

Mobile Feature / Configuration	Required	Recommended
2.4.d. Wireless PED configuration management SHOULD include secure updates to security policies and user profiles where possible.		X
3.5 Data Protection		
3.5.a. Applications such as file sharing SHOULD be disabled on applicable PEDs, and all file sharing ports should be blocked in both directions, especially when processing sensitive information.		X
3.5.b. Where possible, data protection SHOULD be extended to include PIM databases, telephone contact lists, text messages, and temporary browser files.		X
3.5.c. Wireless PEDs SHALL encrypt all data-at-rest by securing either the individual files or the file system (operating system or storage partition), including removable media.	X	
3.6 Monitoring of System Files		
3.6.a. These mechanisms SHOULD perform system file integrity checks automatically, such as routinely comparing a cryptographic hash of the current system files on the PED to a "known good" previously recorded hash.		X
3.7 Device Synchronization and Backup		
3.7.a. PEDs SHOULD periodically synchronize and back up all stored information. Recommended intervals are daily for incremental data backups and weekly for full data backups.		X
3.7.b. A replacement device SHOULD support full restoration functionality of the archived file(s) to limit the downtime and loss of productivity possible after an attack or loss has taken place.		X
3.7.c. Wireless capabilities SHOULD be disabled during hot-synchronization operations with companion devices.		X
3.7.d. Only a single network connection (wired or wireless) SHOULD be active at any one time in order to prevent unauthorized connections among multiple networks.		X
3.8 Recommended Maintenance Activities		
3.8.a. Data SHALL be properly sanitized by degaussing, overwriting, or destroying the hardware.	X	
4.0 Securing the Wireless Link		
4.0.a. Wireless communication cannot be protected from intercept; however, controls SHALL be implemented to prevent the unauthorized disclosure of information. Not all receivers of the signal will be authorized users; therefore, security mechanisms SHALL be put into place to protect wireless resources and data.	X	
4.0.b. Users SHALL adhere to CBP policy and refrain from peer-to-peer associations unless approved by the AO.	X	
4.0.c. The AO SHOULD ensure proper authentication and encryption mechanisms are implemented to ensure data integrity, confidentiality, and availability.		X

Mobile Feature / Configuration	Required	Recommended
4.0.d. PEDs SHOULD indicate when the device is operating in encrypted versus unencrypted modes, i.e. by use of an icon, symbol, or even a blinking light. Approved PED software may be found at the CBP Technical Reference Model (TRM).		X
4.1 Authentication		
4.1.a. Authentication SHALL be required at power-up and PED network and resource access SHOULD be challenged (through re-authentication) as often as possible, dependent on the capability of the operating environment.	X	
4.1.b. CBP SHOULD configure systems to lock a user's account for 20 minutes after three consecutive failed logon attempts.		X
4.1.c. The authentication mechanisms SHALL include strong password protection and SHOULD be combined with the use of a smart card or biometrics authentication.	X	
4.1.d. Administrators SHOULD be aware that the access control mechanisms supported by many wireless systems identify client stations and not users. Unauthorized users may gain access through lost or stolen devices or by a combination of the attacks documented earlier in Section 2.0.		X
4.1.e. Authentication mechanisms SHALL be put into place to require smart cards, certificates, or security tokens to verify a user's identity.	X	
4.1 f. Identity management systems SHOULD authenticate wireless users and take full advantage of any existing public key infrastructure when accessing DHS resources. Identity Access Management is further detailed in the *DHS IT Security Program Handbook for Sensitive Wireless Systems* and *DHS IT Security Architecture Guidance Application Infrastructure Design, Volume III.*		X
4.2 End-to-End Secure Communications		
4.2.a. Users SHOULD be trained not to ignore warning messages and to report suspicious activity. For more information regarding incident response see Section 1.0.		X
4.2.b. Encryption keys stored on client stations SHALL be protected from unauthorized disclosure.	X	
4.2.b. … The use of dynamic keys is highly recommended and SHOULD include Extensible Authentication Protocol (EAP). Using dynamic keys helps to mitigate the risks associated with shared static keys.		X
4.2.c. The symmetric-encryption keys (128-bit) SHOULD be used to protect all information transmitted across the medium. Technologies such as IPSec VPN incorporate the use of public key cryptography and inherently use dynamic key exchange to set up the encrypted VPN tunnel.		X
4.2.d. Key distribution SHALL occur over a secure channel to minimize the risk of compromise. Also, Wirelss Protected Access (WPA) should be active for all WLAN connections and will only be changed by the Information Security group or other similarly authorized personnel.	X	
4.3 Personal Firewalls		
4.3.a. Personal firewalls SHOULD block access to high-risk ports.		X
4.3.b. Personal firewalls SHOULD enable audit logging.		X

Mobile Feature / Configuration	Required	Recommended
4.4 Virtual Private Network		
4.4.a. Wireless PED communications that move between third-party networks and the DHS network SHOULD be considered inherently untrustworthy, given the lack of network control and the public nature of these networks.		X
4.4.b. VPNs SHOULD be implemented with NIST FIPS 140-2 validated encryption and appropriate key management mechanisms. A list of FIPS 140-2 validated products may be found at http://csrc.nist.gov/cryptval/140-1/140val-all htm and at the CBP Technical Reference Model (TRM).		X
4.4.c. Remote access of personally identifiable information SHALL comply with all CBP requirements for sensitive systems, including strong authentication.	X	
4.4.d. Strong authentication SHALL be accomplished via virtual private network (VPN) or equivalent encryption (e.g., Hyper Text Transfer Protocol Secure sockets [https]) and two-factor authentication.	X	
4.5 Intrusion Systems		
4.5.a. CBP system administrators SHOULD routinely scan wireline and wireless networks to determine whether unauthorized PEDs are connected to DHS OneNet.		X
4.6 Securing the Network Interface		
4.6.a. Other components SHOULD be included into the architecture to provide additional security services, such as authentication servers, firewalls, and VPN concentrators. Refer to the *DHS IT Security Program Handbook for Sensitive Wireless Systems* and *DHS IT Security Architecture Guidance Volumes (I–III)* for more detailed guidance.		X
4.6.1 Bluetooth		
4.6.1.a. Bluetooth SHALL NOT be used for any classified data or voice communications and is discouraged for unclassified use because of its inherently insecure modes of operation.	X	
4.6.2 WLANs		
4.6.2.a. PED devices SHALL use authentication and encryption mechanisms as required in the *DHS Sensitive Program Handbook for Sensitive Wireless Systems*.	X	
4.6.3 Cellular Technology		
4.6.3.a. Wireless PEDs SHALL implement strong identification and authentication controls to access CBP resources and SHALL encrypt all data-in-transit.	X	
4.6.4 Companion Workstations		
4.6.4.a. The traditional PED device is synchronized to a computer workstation through a universal serial bus (USB) cable. Only one interface SHOULD be active at a time.		X
5.0 Emerging Technologies		
5.1 Biometrics and Smartcards		
5.1.a. Smart cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), SHALL be cost-justified through the risk assessment process.	X	

Mobile Feature / Configuration	Required	Recommended
5.2 Environmentally Adaptable Security Policies		
5.2.a. Whenever a PED is outside the corporate network or communicating from an insecure location, capabilities such as VPNs and firewalls SHOULD self-configure to the changing operational environment.		X

Appendix B

Referenced Publications

APPENDIX B—REFERENCED PUBLICATIONS

1) Department of Homeland Security. 2004. ISSO Guide to the DHS Information Security Program. ver. 0.6.

2) Department of Homeland Security. 2004. ISSM Guide to the DHS Information Security Program. ver. 2.0.

3) Department of Homeland Security. 2005. DHS 4300A Sensitive Systems Handbook. ver. 4.0.

4) Department of Homeland Security. 2005. DHS 4300A Sensitive Systems Policy Directive. ver. 4.0.

5) Department of Homeland Security. 2005. IT Security Architecture Guidance Volume I: Network and System Infrastructure. ver. 2.0.

6) Department of Homeland Security. 2005. IT Security Architecture Guidance Volume II: Security Operations Support. ver. 2.0.

7) Department of Homeland Security. 2005. IT Security Architecture Guidance Volume III: Application Infrastructure Design. Draft, ver. 1.0.

8) Department of Defense. Defense Information Systems Agency. 2005. Wireless Security Technical Implementation Guide. ver. 4, rel. 1.

9) 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.

10) Department of Defense. Defense Information Systems Agency. 2005. Wireless LAN Security Framework Addendum to the Wireless Security Technical Implementation Guide. ver. 2, rel. 1.

11) National Security Agency. 2006. National security agency/central security service website. National Security Agency. http://www nsa.gov.

12) Committee on National Security Systems. August, 2005. National Information Assurance (IA) Policy on Wireless Capabilities. http://www.cnss.gov/policies.html.

13) National Institute of Standards and Technology. 2006. National vulnerability database. National Institute of Standards and Technology. http://nvd nist.gov.

14) 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.

15) 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.

16) National Institute of Standards and Technology. February, 2005. NIST SP 800-53: Recommended Security Controls for Federal Informatoin Systems. National Institute of Standards and Technology. http://www.nist.gov.

17) National Information Assurance Partnership. 2005. Wireless protection profiles. National Institute of Standards and Technology. http://niap nist.gov.

18) Network Working Group. May, 2000. Request for Comments: 2828, Internet Security Glossary. Network Working Group. http://www.faqs.org/rfcs/rfc2828.html.

Appendix C

Acronyms and Definitions

APPENDIX C—ACRONYMS AND DEFINITIONS

Acronym	Definition
AO	Authorizing Official
AP	Access Point
C&A	Certification and Accreditation
CBP	Customs and Border Protection
CISO	Chief Information Security Officer
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
DoD	Department of Defense
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
FOMA	Freedom of Mobile Multimedia Access
GFE	Government Furnished Equipment
I&A	Identification and Authentication
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IR	Infrared
ISSM	Information System Security Manager
IT	Information Technology
J2ME	Java 2 Platform Micro Edition
MAC	Media Access Card
MMS	Multimedia Messaging Service
NIC	Network Interface Card
NIST	National Institute of Science and Technology
NSA	National Security Agency
PAN	Personal Area Network
PC	Personal Computer
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PED	Portable Electronic Device
PIM	Personal Information Management

Acronym	Definition
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RF	Radio Frequency
SMS	Short Message Service
SOP	Standard Operating Procedure
SSH	Secure Shell
SSL	Secure Sockets Layer
TRM	Technical Reference Model
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WMO	Wireless Management Office
WPA	Wireless Protected Access
WSB	Wireless Security Board
WWAN	Wireless Wide Area Network

Appendix D

Rules of Behaviors for PEDs

APPENDIX D—PED RULES OF BEHAVIOR USER AGREEMENT

The following rules describe how and when to use or not use your PED.

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

PED Protection

- Assume responsibility for taking all necessary precautions to protect the PED against loss, theft, damage, abuse, or unauthorized use by employing lockable cases and keyboards, locking cables, and removable media drives.
- Keep the PED 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 PEDs.

- Follow CBP policy on password management.
- Protect passwords from disclosure.
- Ensure that no one can observe the entry of passwords.
- Promptly change a password whenever the 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 PED.
- Do not record passwords on paper or in electronic form and store them with or on the PED.

Data Protection

- Protect sensitive information from disclosure to unauthorized persons or groups.
- Use only Government-issued PEDs to access **CBP** information.
- Do not access, process, or store classified information on the PED.

Encryption and Public Key Infrastructure (PKI)

- Comply with CBP encryption and PKI requirements.
- Transmit data using Web-enabled laptops or PEDs that rely on wireless encryption protocol (WEP) and/or use commercial wireless network providers only if the data is encrypted end-to-end using a FIPS-validated crypto module.
- 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 PEDs to access **CBP** information or connect to CBP systems.
- Follow **CBP** policy on connecting computers and PEDs to networks, including the Internet.
- Use only CBP-authorized Internet connections that conform to DHS security and communications standards.

Incident Reporting

- Immediately report security-related issues (e.g., operational anomalies, security violations, a missing or stolen PED, compromise of the encryption software) to the CBP or Computer Security Incident Response Center (CSIRC).

Traveling with a PED

- Back up all files before traveling.
- Keep the PED under your physical control at all times when traveling.
- Never place the PED in checked luggage.
- Never store the PED in an airport, train station, bus station, or any public locker.
- If leaving the PED in a car, lock it in the trunk out of sight.
- Avoid leaving the PED in a hotel room. If necessary, lock it inside another piece of luggage.
- Be prepared for airport security checks. Have the PED'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 PED 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 PED.
- Exercise diligence when traveling in foreign countries because criminals or local intelligence may target your PED for the information it contains.
- Do not display any sensitive information on the PED 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 PED 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 **CBP** reviews telecommunications logs, computer logs, and telephone records and that it conducts spot-checks to determine compliance with controls placed on **CBP** 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 PEDs will be directed to my supporting Information Systems Security Officer (ISSO).

I acknowledge receipt of and understand my responsibilities for the use of **CBP** 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.