MOBILE AND WIRELESS DEVICE
ADDENDUM to the WIRELESS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

31 October 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

Mobility is an important capability for our military forces. It provides convenience and the ability to connect to a network to fulfill a task, duty, or mission. Because mobile wireless devices are becoming a more prevalent component in current architectures, emphasis on properly configuring and securing devices within networks has become a dominant priority.

The mobile device is considered a critical component within the WLAN and is often overlooked as a network component. The mobile device can be looked on as an extension of the network. This extension consists primarily of mobile devices (e.g., cellular devices, personal digital assistants [PDA], laptops, and tablet personal computers [PC]). A critical risk associated with the device lies in the actual authentication of the user to the device. Although most mobile devices do ship with some form of user-authentication capability, these mechanisms are usually weak and easily exploitable and should not be relied on to provide optimal levels of security. Some of the weaknesses identified are as follows:

- Inadequate encryption algorithms for protection of user credentials
- Password mechanisms that can be by-passed
- Lack of usable encryption mechanisms for end users
- Lack of virus protection
- Lack of security for data at rest.

This addendum provides a technical overview for properly securing the various types of mobile wireless devices currently available to users connecting to the DOD enclave. This addendum also discusses the functionality of the security components. DOD entities using this framework should be able to select the solution that best fits the requirements of their environment and successfully implement a secure network.

1.2 Authority

DOD Directive 8500.1 requires that “all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines” and tasks DISA to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.” This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this Addendum will provide an environment that meets or exceeds the security requirements of DOD systems operating at the MAC II Sensitive level, containing sensitive information.

1.3 Scope

This Addendum is designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls for mobile and wireless devices connected to DOD networks.

1.4 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

The NIPRNet URL for the IASE site is http://iase.disa.mil/. The Secret Internet Protocol Router Network (SIPRNet) URL is http://iase.disa.smil.mil/. Access to the STIGs on the IASE web server requires a network connection that originates from a **.mil** or **.gov** address. The STIGs are available to users that do not originate from a **.mil** or **.gov** address by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to **fso_spt@disa.mil**.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to **fso_spt@disa.mil**. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

2. WIRELESS POLICY OVERVIEW

The first and most important line of defense when securing wireless systems is a sound wireless policy. The following section summarizes existing policies, which are relevant to Mobile and Wireless Devices.

2.1 Policy

The DOD is promoting the sharing of vulnerability mitigation strategies throughout the various DOD entities; consequently, policies have been developed to provide a balanced approach to mitigating risks in unclassified and in sensitive-but-unclassified environments. DOD policy mandates that all wireless technologies include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques. Figure 2-1, *Security Engineering Approach—Document Relationship Diagram*, illustrates the recommended security engineering approach for implementation of wireless communications in the DOD space.

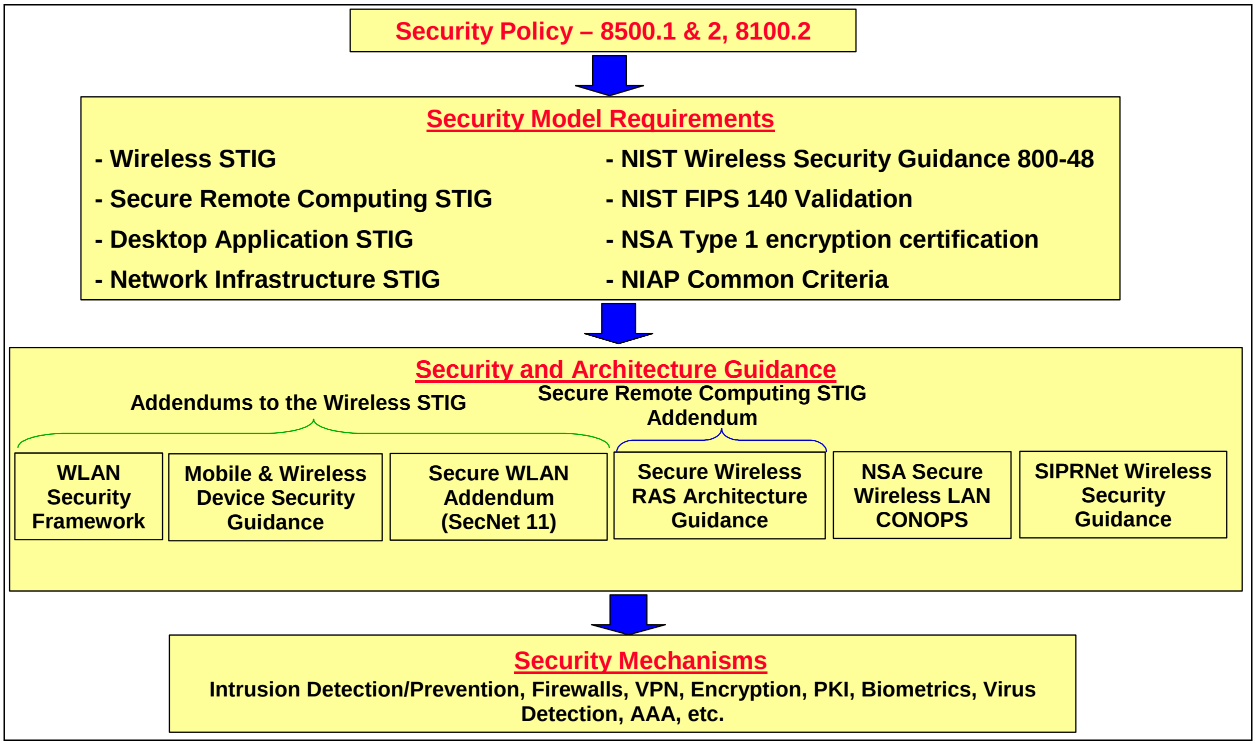
Security Policy – 8500.1 & 2, 8100.2
Security Model Requirements
- Wireless STIG
- Secure Remote Computing STIG
- Desktop Application STIG
- Network Infrastructure STIG
- NIST Wireless Security Guidance 800-48
- NIST FIPS 140 Validation
- NSA Type 1 encryption certification
- NIAP Common Criteria
Security and Architecture Guidance
Addendums to the Wireless STIG
Secure Remote Computing STIG Addendum
WLAN Security Framework
Mobile & Wireless Device Security Guidance
Secure WLAN Addendum (SecNet 11)
Secure Wireless RAS Architecture Guidance
NSA Secure Wireless LAN CONOPS
SIPRNet Wireless Security Guidance
Security Mechanisms
Intrusion Detection/Prevention, Firewalls, VPN, Encryption, PKI, Biometrics, Virus Detection, AAA, etc.

Figure 2-1. Security Engineering Approach—Document Relationship Diagram

This addendum is based on existing policy, including DODD 8500.1, DOD 8500.2, and DOD Wireless Security Policy 8100.2. Additionally, the *Wireless Security Technical Implementation Guide (STIG)*; the *Securing Remote Computing STIG*; and the National Institute of Standards and Technology (NIST) Special Publication 800-48, *Wireless Security of 802.11, Bluetooth, and Handheld Devices*, are used as references, providing specific requirements for defining secure wireless local area network (WLAN) architecture. A list of relevant documents is provided in Appendix A, *Publications*.

According to *DOD Wireless Security Policy* 8100.2, Section 4.1.3, wireless devices shall not be used to store, transmit, or process classified information without written approval from the Designated Approving Authority (DAA). Wireless systems can be used and brought into classified areas if the conditions set by the DAA are followed. The directives in this policy specifically related to wireless devices are as follows.

- In Section 4.2, "Cellular/PCS and/or other RF or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA)."

- In Section 4.3, "Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures."

- In Section 4.4, "Pursuant to subparagraph 4.1.2., DAAs shall ensure that Wireless Personal Area Network (WPAN) capability is removed or physically disabled from a device unless FIPS PUB 140-2-validated cryptographic modules are implemented (reference (g)). Exceptions may be granted on a case-by-case basis as determined by the DAA."

- In Section 4.7, "PEDs that are connected directly to a DoD-wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly while directly connected."

- In Section 4.8, "Anti-virus software shall be used on wireless-capable PEDs and workstations that are used to synchronize/transmit data, in accordance with reference (e). The network infrastructure shall update anti-virus software for all applicable PEDs and their supporting desktops from a site maintained by the Defense Information Systems Agency."

3. CLASSIFICATION OF MOBILE DEVICES

With the rapid growth of information technology, a number of significant advancements in the types of wireless devices have developed. Identifying the major types of wireless devices available will help define the features and functionalities, along with how to properly implement measures to protect the device and the information it contains. This section categorizes the major types of wireless devices available today with the capability of transmitting, storing, receiving, and managing voice and data packets.

3.1 Mobile Computers

A mobile computer can be best defined as a system with comparable features and functionalities to a traditional desktop computer. These features and functionalities include similar hardware components (e.g., microprocessors, disk drives), interoperable software applications, operating system, and external attachments (e.g., keyboard, mouse, monitor). In addition, mobile computers may or may not have components with capability to communicate wirelessly through a wireless network interface card (NIC). The following list of devices classified as a mobile computer have slight differences in hardware and software components but have similar operational features, exposing them to the same types of wireless threats and attacks.

3.1.1 Laptops

A laptop computer can be defined as a small portable computer that is light enough to carry comfortably, with a flat screen and keyboard that fold together. A laptop would have most, if not all, of the features and functionalities of the standard desktop computer. These features (e.g., keyboard, mouse, screen, power source) are consolidated for portability. Laptops are battery operated, often having a thin, backlit or side-lit liquid crystal display (LCD) screen. Some models have a compatible docking station to perform as a full-size desktop computer system. A laptop typically weighs less than 5 pounds and is about 3 inches or less in thickness. The leading manufacturers of laptops are IBM, Apple, Compaq, Dell, and Toshiba.

Laptop computers are usually more expensive than desktop computers with the same capabilities because they are more difficult to design and manufacture. A laptop can effectively be turned into a desktop computer with a docking station, a hardware frame that supplies connections for peripheral input/output devices (e.g., printer or larger monitor). The less capable port replicator enables a user to connect a laptop to a number of peripherals using a single plug.

Laptops use various approaches for integrating a mouse into the keyboard, including the touch pad, trackball, and pointing stick. A serial port allows a regular mouse to be attached. The PC card is a hardware item that can be inserted into an available slot. The distinguishing features allow it to function as a standard desktop computer with similar hardware components and compatible software applications. The available operating systems (OS) would be the same as the traditional desktop PC.

3.2 Tablet Computers

As its name implies, the Tablet PC is a computer that is about the size of a paper tablet. It is not only its name that is similar—one can now write with a digital pen directly on its screen. The

Tablet PC provides the portability, flexibility, and usability that are changing the way we work with computers. There are three types of Tablet PCs as follows:

Convertible Tablet PC—is most similar to the familiar notebook, although one very important difference exists: its screen pivots 180 degrees and then folds down on top of the keyboard, creating a special writing surface. This feature enables users to write directly on the surface using a digital pen.

Slate Tablet PC—is Tablet only, with no attached keyboard. Most have an option of using a wired or wireless keyboard if preferred.

Hybrid Tablet PC—can be used with a keyboard or detached for use as a slate only.

3.3 Portable Electronic Devices (PEDs)

Portable Electronic Devices (PEDs) consist of small electronic items used for storing, processing, or transmitting information. These devices provide several benefits: convenience of sharing information, potential to increase productivity, reduction in communication costs, and improvement in information flow. PEDs usually have less central process unit (CPU), storage capacity, memory allocation, and number of interfaces compared with standard desktops or laptops. PEDs are limited in the types and amount of applications for the OS; therefore, they would occupy less bandwidth consumption.

3.3.1 Personal Digital Assistants (PDAs)

A PDA is a handheld computer that provides numerous organizational capabilities (e.g., calendar, address list, to-do list, notepad). A PDA or handheld computer is small enough to fit into a person’s hand. Some manufacturers are working to solve the small keyboard problem by replacing the keyboard with an electronic pen. PDAs have many of the same functionalities of a laptop. The differences lie in the size, OS, applications, and hardware components. PDAs can be categorized based on the OS that is used. Two main OS platforms are available: the Palm OS by Palm and Windows Mobile (formerly, Windows CE) by Microsoft. Another less common platform is Symbian OS (originally called EPOC) by Symbian, which is a joint venture between Ericsson, Motorola, Nokia, and Psion. Java and Linux platforms are also available for PDAs. Most PDA OSs provide security application programming interfaces (API) that application developers can use to enhance the security of their applications.

3.4 Wireless Keyboards and Mice

Interest in using wireless keyboards and mice by DOD offices has been increasing. These systems use numerous wireless technologies for transmitting data to the computer (e.g., WLAN, Bluetooth, and infrared). A wireless mouse transmits telemetry data (right, left, up, and down). Wireless keyboards, on the other hand, transmit users’ keystrokes that can be easily read by a nearby receiver, thereby posing significant security risk.

The following conditions will be met before the use of wireless mice or keyboards:

- *(WIR0132: CAT II) The IAO will ensure that if WLAN or Bluetooth mice and keyboards are used, applicable requirements listed in Section 2.2.5, IEEE 802.11 WLAN Implementation Compliance Requirements, or Section 2.3, Bluetooth WPAN, are followed.*

- *(WIR0131: CAT II) The IAO will ensure that if infrared wireless mice and keyboards are used on classified or unclassified equipment and networks, the following conditions are followed:*

  - *The DAA, in consultation with the CTTA, has approved that IR wireless mice and/or keyboards are used in the facility.*

  - *When wireless mice and/or keyboards are used on classified equipment, the area is approved for processing classified information at the appropriate level.*

  - *The area is totally enclosed with walls, ceiling, and floor consisting of material opaque to IR. There will be no windows unless each window is covered with a film approved for blocking IR. All doors must remain closed when the devices are in operation.*

  - *There is no mixing of classified and unclassified equipment using IR within the same enclosed area.*

  - *When IR is used with classified equipment in the same enclosed area as unclassified equipment with IR ports, the IR ports on the unclassified equipment must be completely covered with metallic tape.*

  - *When IR is used with unclassified equipment in the same enclosed area as classified equipment with IR ports, the IR ports on the classified equipment must be completely covered with metallic tape.*

3.5 Messaging Devices and Pagers

A text-messaging device is a simple and relatively quick way to send and receive messages. The traditional wireless pagers that can receive only alphanumeric messages are still in use, but significant advancements have evolved the technology. Some vendors offer paging services with two-factor authentication and FIPS-compliant 128-bit 3DES encryption. Currently, no vendors offer two-way pagers and their associated services that provide an assured channel employing NSA-approved, Type 1 end-to-end encryption.

Government and personal pagers may be carried into Sensitive Compartmented Information Facilities (SCIF) and kept on and used; however, two-way pagers are prohibited unless a waiver is approved on a case-by-case basis.

3.5.1 Blackberry Devices

Blackberry is a wireless device used for exchanging two-way e-mails. The Secure/Multipurpose Internet Mail Extension (S/MIME) enhanced Blackberry is the only NSA-approved device for sensitive but unclassified information within the DOD. The S/MIME Blackberry can allow e-mails to be encrypted using Triple Data Encryption Standard (3DES)/Advanced Encryption Standard (AES) and signed using DOD Class 3 PKI certificates. A Smart Card Reader can be attached to specific Blackberry devices via the serial port to provide two-factor authentication. Currently, other NSA evaluations of other products by the Blackberry manufacturer have been discontinued.

As stated in the DISA Director's Policy Letter 2003-7, master cryptographic keys for encrypting Blackberry e-mail traffic should always be generated within secure U.S. Government spaces. A Blackberry user is required to update the key monthly with the local DISA system administrator. The DAA must approve non-S/MIME e-mail devices.

Note that the vendor, Research In Motion (RIM), has released a new S/MIME Support package (SSP), version 4.0. For further information, please refer to the Wireless STIG.

3.6 Mobile Phones

The traditional cellular phones could only offer the service of voice calls. In last several years, significant advancements have been made on the portable cellular phones that would provide additional functionalities to the user, including data and multimedia storage and transfer. With these added capabilities, a cellular phone should be identified as a mobile device with potential vulnerabilities and risks involved when used.

To provide proper security guidance, the identification of the various types of cellular phones needs to be distinguished. Mobile phones have internal low-power transmitters with two signal strengths: 0.6 watts and 3.0 watts.

3.6.1 Analog Cellular Phone

The original cellular or mobile phones used analog signals operating with the Advanced Mobile Phone System (AMPS) standard approved by the Federal Communications Commission (FCC). The range of frequencies is between 824 Megahertz (MHz) and 894 MHz.

Major problems with cell phone include eavesdropping on calls and cell phone cloning. In particular, analog cell phones provide no security because the transmission is through plain frequency modulation (FM).

3.6.2 Digital Cellular Phone

Digital phones are more secure because encryption is applied to secure the phone and the transmissions. The encryption process generates a key used in an algorithm that compresses the audio signal. The signal is sent to the nearest tower of the signal provider where it can be decode the transmission. If a person with a scanner were to locate the channel and time slice, the person would need to find the encryption code to make sense of the signal, making it more difficult to eavesdropping. Trillions of possible frequency-sequencing codes exist; this feature enhances privacy and makes cloning difficult.

The Global System for Mobile Communication (GSM) is a digital mobile telephone system that uses a variation of time division multiple access (TDMA). This technology is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and code division multiple access [CDMA]). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.

As referenced from the Wireless Remote Access Service Architecture Guidance, CDMA refers to any of several protocols used in so-called second-generation (2G) and third-generation (3G) wireless communications. As the term implies, CDMA is a form of multiplexing; allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in ultra-high-frequency (UHF) cellular telephone systems within the 800 MHz and 1.9 gigahertz (GHz) bands. CDMA employs analog-to-digital conversion (ADC) in combination with spread spectrum technology. Audio input is first digitized into binary elements. The frequency of the transmitted signal is then made to vary according to a defined pattern. A receiver whose frequency response is programmed with the same code can only intercept this. It follows along the exact same lines as the transmitter frequency.

Some digital GSM and CDMA phones support the use of analog signals as a backup when the primary service is unavailable. This signal switch over is often called “roaming” out of coverage area. This could make a mobile phone vulnerable to information interception during the use of analog signal because voice and data packets traveling over analog transmissions are not encrypted.

3.6.2.1 Second-Generation Cellular Technology

The 2G cellular phone operates on digital signaling with usually better quality reception compared with analog cell phones. It uses the same RF as analog phones but with better battery life, size, appearance, cost, and features along with lower rates of service. One problem with this type of phone is coverage area, which is dependent on the service provider.

3.6.2.2 Third-Generation Cellular Technology

The 3G defines a mobile handset capable of worldwide roaming and high data rate services. New handsets that support these higher data rates have included multimedia and data communications features (e.g., image and video cameras, messaging services, and content services) that can be browsed with a Web browser application.

With the addition of these advanced services and higher data rates, it becomes imperative for the DOD to ensure that 3G handsets operate in a robustly secure manner using Type 1 encryption for voice and data services. The Future Narrowband Digital Terminal (FNBDT) protocol enables Type 1 security to be established and maintained over real-time voice and data channels.

Currently, the FNBDT specifications specify only Type 1 encryption methods, although the signaling is directly applicable to vendor-defined non-Type 1 products based on the FNBDT specifications. The High-Assurance Internet Protocol Encryption (HAIPE) protocol, which provides Type 1 encryption, extends high-assurance protection to IP communications sessions. In addition, HAIPE v2 features IPv6.

FNBDT and HAIPE (as specified by High-Assurance Internet Protocol Interoperability Standard [HAPIS]) are key technologies for secure communications with the Next Generation Wireless Handset. They are part of a comprehensive suite of tools and technologies to be engineered into the next generation wireless handset.

3.6.3 Smart Phones

What makes the phone “smart” is its ability to handle data and voice calls. Internet or “Web” enabled phones would apply to this category. Smart phones have similar features and capabilities to Hybrid devices, which are classified as “all-in-one” mobile devices that offer the features of various technology devices in a single consolidated portable gadget.

The trend of consolidating multiple devices into one makes products more appealing and cost effective. Instead of carrying several separate devices all offering different services, the hybrid device can provide most or all of the functionalities. This section categorizes a hybrid device as any mobile device with combination of features and capabilities from one or more of the previous classifications or a device that does not ideally correspond to a traditional classification. A sample listing of available hybrid devices:

- Cellular phone with integrated PDA
- Blackberry with integrated cellular phone.

3.6.3.1 Smart Phone Operating System

Palm, Symbian, and Microsoft (MS) operating systems (OS) platforms are widely used by DOD users. Palm OS Cobalt delivers a host of new features to licensees and developers, creating new opportunities in demanding segments (e.g., enterprise, multimedia, and communications). PalmOS Cobalt is a complete rewrite of Palm OS resulting in a new OS architecture. Although providing major advancements for the platform, Palm was careful to maintain support for the Portable Applications Compatibility Environment (PACE), ensuring that 68K-based applications would continue to run and thrive on Palm OS Cobalt. Using platform APIs, developers can create applications, portions of which can run concurrently, or applications that can run in a background process. Examples include a maximum of 256MB each for read-only memory (ROM) and random access memory (RAM) (a more robust and stable platform). Protected memory prevents applications from “hanging” the system or causing crashes. The modular, flexible, industry-standard Surface Traffic Enhancement and Automation Support System (STREAMS) based framework provides an easy and familiar way for licensees and developers to add to or enhance their communications support.

Symbian OS includes a robust multitasking kernel, integrated telephony support, communications protocols, data management, advanced graphics support, a low-level graphical user interface (GUI) framework and various application engines.

Symbian OS is the common core of APIs and the technology that is shared by all Symbian OS phones. It describes what is provided by Symbian OS components in base, application framework, multimedia, communication infrastructure and network stacks, messaging, browsing, application protocols, services and engines, Java, connectivity, and tools. Symbian OS is designed for optimal flexibility, giving mobile phone manufacturers broad scope for differentiation and innovation in user interfaces, hardware designs, and connectivity. Symbian OS 7.0 supports 3G phones.

The Windows Smartphone OS boasts many of the Pocket PC’s PDA features, including Microsoft Outlook functionality (e-mail, calendar, and contacts), MSN Messenger (Instant Messaging [IM]), Microsoft Internet Explorer (IE), and an ability to play audio and video content through Windows Media Player (WMP). The Outlook functionality leverages the Microsoft Mobile Information Server 2002, ActiveSync Edition architecture that Pocket PC uses to synchronize e-mail, calendar, and contacts over the wireless (specifically, General Packet Radio Service [GPRS]) connection.

4. DEVICE CONFIGURATION GUIDANCE

Security is a major concern for enterprises using and deploying mobile devices and applications. This section presents configuration guidance for properly securing each class of mobile device. The different mobile device classifications consist of features that are unique and similar to one another. Therefore, a separate set of guidelines is provided to alleviate the need for generalization and provide a targeted approach for addressing the specific needs of the user operating the device and the local administrator's management.

All wireless devices must be approved by the Component DAA before being installed, deployed, and used to transfer, receive, store, or process DOD non-sensitive, unclassified, and classified information.

4.1 General Guidelines for Securing Mobile and Wireless Devices

4.1.1 Operating System Security

Applicable mobile devices with an OS would require a life cycle of upgrades and patches to become a viable and secure platform.

As a part of the OS security, a Separation Kernel is required to not only partition the subjects and resources from the system into policy-based classes but also control information flows between each partition of the computing system. Details regarding compliancy is referenced and addressed in the *U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness*, issued by the Information Assurance Directorate. http://niap.nist.gov/pp/draft_pps/pp_draft_skpp_hr_v0.621.pdf

4.1.2 Application Security

Third-party applications installed on the OS of a mobile device would provide additional security protection against threats. Examples would be personal/host-based firewalls, intrusion detection systems, and antivirus software.

4.1.3 Transmission Protection

Securing outgoing and incoming transmission traffic for either wireless or wired connections of a device is a critical requirement to protect information confidentiality. Examples would include disabling the "Internet Connection Sharing" feature and dual connection using more than one NIC.

4.1.4 TEMPEST Considerations

TEMPEST considerations are referenced from the NSA Secure Wireless Local Area Network (WLAN) Concept of Operations (CONOPS).

https://powhatan.iiie.disa.mil/wireless-secnet11-conopsv1.51.pdf (DOD PKI certificate is required for access)

For TEMPEST considerations, the separation distance of a transmitter from a classified processor is the distance separating a mobile device with its Personal Computer Memory Card International Association (PCMCIA) card from another transmitter. The Secure Wireless Local Area Network (SWLAN) will function in accordance with TEMPEST guidelines.

> "This includes National Security Telecommunications and Information Systems Security Policy (NSTISSP) 300 and NSTISS Instruction (NSTISSI) 7000 and NSTISS Advisory Memorandum (NSTISSAM) 2-95. The Certified TEMPEST Technical Authority (CTTA) will evaluate the SWLAN for TEMPEST issues. In keeping with the guidance provided by NSTISSP 300, risk management rather than risk avoidance will be implemented. The CTTA will evaluate the guidance provided and the operational environment. The CTTA will then provide a determination of the TEMPEST requirements for the system. Because executing a TEMPEST attack requires sophisticated equipment and fine-tuning of antennas to exploit a source, a number of scenarios exist where executing a TEMPEST attack is impractical if not impossible. In these cases, the CTTA is expected to allow minimal separation of processors and transmitters. Otherwise, the minimum separation distances between systems processing unclassified and classified data will be approximately 3 meters (10 feet). The CTTA will provide installation guidance on Red/Black separation in accordance with Recommendation C of NSTISSAM TEMPEST/2-95. Appropriate amount of controlled space as defined by the CTTA should surround the mobile devices based on operational environment equipment use. When organizations are not under stringent TEMPEST controls, they are allowed to utilize commercially available mobile devices approved for use in their facility. Customers who have a high risk of TEMPEST attack must use TEMPEST endorsed devices operate the SecNet 11 in a TEMPEST shielded enclosure. As of the publication of this CONOPS, only one laptop is TEMPEST approved."

For more information on NSA-endorsed TEMPEST products, go to:
http://www.nsa.gov/ia/industry/tempest.cfm .

4.1.5 Access Control

This type of mechanism grants and revokes rights to access data or a system. This would include operating system, file, data, and application permissions. Physical access control: Using locks, biometric technologies, and smart cards. Management and control of a device is the responsibility of both user and the administrator. Authentication, Authorization, Account (AAA) capabilities would apply to this section.

4.1.6 Data Protection

Implementing file, media, and data encryption for the transmission and storage of classified information provides additional preventive measures for ensuring the confidentiality of the residing information. Disabling file sharing should also be part of the minimum configuration settings imposed on applicable for mobile wireless devices. Data protection laws protect personal privacy, requiring fair and lawful processing of personal information, and restricting what can be done with it and to whom it may be disclosed.

4.1.7 User Training

Security awareness training should be a requirement for all mobile wireless device users and provided regularly. This training will ensure that users are informed on computing best practices in accordance with DOD policies and guidelines. In addition, product-specific training may be necessary to certify that mobile and wireless devices are securely configured, deployed, and used.

4.2 Mobile Wireless Computers

The default wireless settings by the manufacturers of mobile computers do not provide adequate security and are vulnerable to malicious attacks is left unchanged. Additional measures must to taken to mitigate these risks. To properly secure a mobile computer, the following guidelines are recommended to reduce the vulnerabilities and risks associated with use in an unclassified or classified environment:

The checklists provided in Tables 5-1 and 5-2 will help the administrator who is managing the network and the end user who is operating the device in securing mobile wireless computers.

Wireless Device Feature/Configuration	Required	Recommended
Access Control		
Enable strong password protection scheme for device and network user login (as instructed in the *Secure Remote Computing STIG* developed by DISA for the DOD). https://iase.disa.mil/techguid/stig/src-stig-v1r1-final-021403.doc	X	
Ensure two-factor authentication (smartcard) is used when PKI-based CAC authentication is required. http://iase.disa.mil/pki/pkim0812.pdf	X	
Enable the use of biometric reader if available and/or required. https://iase.disa.mil/documentlib.html		X
Enable password protection on screen saver	X	
Verify device use is in a physically secure location and protected against unauthorized use	X	
Verify encryption scheme used for wireless transmission is FIPS 140-2 and/or NSA Type-1 approved	X	
Wireless Network Interface Card (NIC)		
Allow only one NIC to be active on a particular device at any given time	X	
Personal/Host-Based Firewall Software		
Install and run DOD and National Information Assurance Partnership (NIAP) approved personal/host-based firewall http://niap.nist.gov/cc-scheme/vpl/vpl_type.html#firewalls	X	
Lock out network access during periods of inactivity (when the computer is not in use)	X	

Wireless Device Feature/Configuration	Required	Recommended
Block access on high-risk ports as directed by the Network Infrastructure STIG, Appendix G https://iase.disa.mil/techguid/stig/network-stig-v5r2-9-29-03.doc	X	
Enable firewall logging of suspicious activity and user alerts, including inbound and outbound connection attempts	X	
Obtain configuration and signature file updates from network administrator on a regular basis as required by Information Assurance and Vulnerability Assessment (IAVA) https://iase.disa.mil/IAalerts/iavahnbk.pdf	X	
Antivirus Software		
Install and enable DOD-approved antivirus software http://www.cert.mil/antivirus/av_info.htm	X	
Install and update latest virus definitions regularly (weekly); allow Live Updates to DOD servers	X	
Enable and run virus startup scan at each boot	X	
Operating System		
Verify OS is STIG compliant https://iase.disa.mil/techguid/stig/index.html	X	
Install all the latest OS security patches and fixes required by IAVAs	X	
Install all the latest application and software security patches and fixes	X	
Ensure media and file encryption is used for all classified information stored on and transmitted from the device	X	
Disable sharing of local files and drives	X	
Disable Internet Connection Sharing	X	
Remote Access		
Verify FIPS-140-2 certified virtual private network (VPN) client is installed and always used in conjunction with remote access service (RAS) connectivity	X	
Verify active VPN connection icon present for successful connection attempt	X	
Verify Split tunneling is disabled on the VPN client (All Internet access would go through the DOD firewall or proxy server instead of local service provider)	X	

Table 4-1. Client Checklist for Securing Mobile Wireless Computers

Wireless Device Feature/Configuration	Required	Recommended
Security Awareness		
Review NSA PED/PDA database, and ensure that all identified vulnerabilities are mitigated		X
Ensure network users are fully trained on IA awareness and risks associated with using mobile computer technology	X	
System Security		
Ensure mobile client is using strong password scheme for device and network user login (as instructed in the *Secure Remote Computing STIG* developed by DISA for the DOD)	X	
Ensure wireless NIC on client’s mobile computer are up to date with latest patches and upgrades	X	
Disable IR port(s)	X	
Wireless Settings		
Restrict wireless settings to “read only” (cannot add, change, or delete any preconfigured wireless settings from the standard DOD build)		X
Ensure “broadcast SSID” setting is disabled	X	
Ensure only an encryption scheme used for wireless transmission is FIPS 140-2 and/or NSA Type-1 approved	X	
Ensure Bluetooth is disabled	X	
Disable Ad Hoc operation mode on wireless NIC(s)	X	
Security Mechanisms		
Deploy DOD and NIAP-approved personal/host-based firewall on mobile computer http://niap.nist.gov/cc-scheme/vpl/vpl_type.html#firewalls	X	
Deploy DOD-approved antivirus software on mobile computer http://www.cert.mil/antivirus/av_info.htm	X	
Ensure FIPS-140-2 certified VPN client is installed and working on user’s machine	X	
Ensure wireless NIC on client’s mobile computer are up to date with latest patches and upgrades	X	
Application Security		
Ensure non-DOD approved applications are removed from the device	X	

Table 4-2. Client Checklist for Securing Mobile Wireless Computers

4.3 Portable Electronic Devices

PEDs are growing in use in the DOD environment. The configuration settings and safeguards in Tables 5-3 and 5-4 will help block malicious attacks, deter threats, and mitigate vulnerabilities associated with using PEDs connecting to the DISN through a wireless connection.

Wireless Device Feature/Configuration	Required	Recommended
Access Control		
Ensure secure synchronization of sync stations	X	
Ensure Power-on password is used	X	
Enable password protection on screen saver	X	
Enable strong password protection scheme for device and network user login (as instructed in the *Secure Remote Computing STIG* developed by DISA for the DOD) https://iase.disa.mil/techguid/stig/src-stig-v1r1-final-021403.doc	X	
Ensure two-factor authentication (smartcard) is used when PKI-based CAC authentication is required http://iase.disa.mil/pki/pkim0812.pdf	X	
Enable the use of biometric reader if available and/or required. https://iase.disa.mil/documentlib.html		X
Verify encryption scheme used for wireless transmission is FIPS 140-2 and/or NSA Type-1 approved	X	
Ensure Internet File Sharing is disabled	X	
Ensure media and file encryption is used for all classified information stored on and transmitted from the device	X	
Personal/Host-Based Firewall Software		
Install and run DOD and NIAP-approved personal/host-based firewall http://niap.nist.gov/cc-scheme/vpl/vpl_type.html#firewalls	X	
Lock out network access during periods of inactivity (when the computer is not in use)	X	
Block access on high-risk ports as directed by the Network Infrastructure STIG, Appendix G. https://iase.disa.mil/techguid/stig/network-stig-v5r2-9-29-03.doc	X	
Enable firewall logging of suspicious activity and user alerts, including inbound and outbound connection attempts	X	
Obtain configuration and signature file updates from network administrator on a regular basis as required by IAVAs	X	
Antivirus Software		
Install and enable DOD approved antivirus software	X	
Install and update latest virus definitions on a regular basis (weekly); allow Live Updates to DOD servers	X	
Enable and run virus startup scan at each boot	X	

Table 4-3. Client Checklist for Securing Portable Electronic Devices

Wireless Device Feature/Configuration	Required	Recommended
Security Awareness		
Review NSA PED/PDA database and ensure that all identified vulnerabilities are mitigated		X
Ensure users on the network are fully trained on IA awareness and risks associated with using mobile computer technology	X	
System Security		
Ensure mobile client is strong password protection scheme for device and network user login (as instructed in the *Secure Remote Computing STIG* developed by DISA for the DOD)	X	
Ensure OS is up to date with latest patches and upgrades	X	
Disable IR port(s)	X	
Disable Bluetooth		
Wireless Settings		
Restrict wireless settings to "read only" (cannot add, change, or delete any preconfigured wireless settings from the standard DOD build)		X
Ensure "broadcast SSID" setting is disabled	X	
Ensure only an encryption scheme used for wireless transmission is FIPS 140-2 and/or NSA Type-1 approved	X	
Application Security Mechanisms		
Deploy DOD and NIAP-approved personal/host-based firewall	X	
Deploy antivirus software	X	
Ensure latest security policy is installed and updated		
Ensure FIPS-140-2 certified VPN client is installed and working on the user's machine	X	
Verify split tunneling is disabled on the VPN client (All Internet access would go through DOD firewall or proxy server instead of local service provider)	X	

Table 4-4. Administrator Checklist for Securing Portable Electronic Devices

4.4 Messaging Devices/Pagers

To properly secure a messaging device or pager, the measures listed in Tables 4-5 and 4-6 should be implemented:

Wireless Device Feature/Configuration	Required	Recommended
Access Control		
Ensure Power-on password is used	X	
Enable password protection on screen saver	X	
Enable strong password protection scheme for device and network user login (as instructed in the *Secure Remote Computing STIG* developed by DISA for the DOD) https://iase.disa.mil/techguid/stig/src-stig-v1r1-final-021403.doc	X	
Ensure two-factor authentication (smartcard) is used when PKI-based CAC authentication is required http://iase.disa.mil/pki/pkim0812.pdf	X	
Enable the use of biometric reader if available and/or required. https://iase.disa.mil/documentlib.html		X
Verify encryption scheme used for wireless transmission is FIPS 140-2 and/or NSA Type-1 approved	X	
Lock out network access during periods of inactivity (when the computer is not in use)	X	
Obtain configuration and signature file updates from network administrator regularly as required by IAVAs	X	

Table 4-5. Client Checklist for Securing Messaging Devices

Wireless Device Feature/Configuration	Required	Recommended
Security Awareness		
Review NSA PED/PDA database and ensure that all identified vulnerabilities are mitigated		X
Ensure network users are fully trained on IA awareness and risks associated with using mobile computer technology	X	
System Security		
Enable strong password protection scheme for device and network user login (as instructed in the *Secure Remote Computing STIG* developed by DISA for the DOD)	X	
Ensure OS is up to date with latest patches and upgrades	X	
Disable IR port(s)	X	
Disable Bluetooth if applicable		
Ensure only an encryption scheme used for wireless transmission is FIPS 140-2 and/or NSA Type-1 approved	X	

Table 4-6. Administrator Checklist for Securing Messaging Devices

4.5 Mobile Phones

Limit or Restrict "Roaming." Some mobile phones have the "roaming" feature enabled. This feature should be limited as much as possible because roaming usually defeats the use of a personal identification number (PIN). This is susceptible to cell phone "cloning"; consequently, these phones are targeted at airport parking lots, airport access roads, rural interstates, and any other areas not covered by the originating service carrier. Roaming also makes it more difficult for some cellular carriers to use fraud-detection programs to monitor an account and shut it down when fraud is detected.

Turn off Cellular Phones When Not in Use. Cell phones poll the cellular base station with the strongest signal every few second. This is how the system knows which base station to route calls through. However, this polling exposes the phone to interception and cloning.

Restrict Use of Mobile Phones With Built-in Cameras. One of the growing trends of recent cellular phones is the integrated feature of digital cameras. This allows a user to take, store, share, and transmit digital images on the cellular phone. In the unlikely case that the camera phone is automatically operated from an unauthorized user, the act of disabling the feature would be a difficult task unless the hardware is removed. To help mitigate the risk of exposing unauthorized or sensitive information, a policy restricting mobile phones with built-in camera phones should be applied and enforced.

To properly secure a mobile phone, the measures listed in Tables 5-7 and 5-8 should be implemented:

Wireless Device Feature/Configuration	**Required**	**Recommended**
Access Control		
Turn off mobile phones when not in use		X
Disable camera features if at all possible and/or applicable		X
Ensure power-on password is enabled	X	
Enable strong password protection scheme for device and network user login (as instructed in the *Secure Remote Computing STIG* developed by DISA for the DOD) https://iase.disa.mil/techguid/stig/src-stig-v1r1-final-021403.doc	X	
Ensure two-factor authentication (smartcard) is used when PKI-based CAC authentication is required http://iase.disa.mil/pki/pkim0812.pdf	X	
Enable the use of biometric reader if available and/or required. https://iase.disa.mil/documentlib.html		X
Verify device use is in a physically secure location and protected against unauthorized use	X	

Table 4-7. Client Checklist for Securing Mobile Phones

Wireless Device Feature/Configuration	**Required**	**Recommended**
Security Awareness		
Ensure network users are fully trained on IA awareness and risks associated with using mobile computer technology.	X	
Review NSA PED/PDA database and ensure that all identified vulnerabilities are mitigated		X
Verify split tunneling is disabled on the VPN client (all Internet access would go through DOD firewall or proxy server instead of local service provider)	X	
Access Control		
Restrict all mobile phones from entering classified DOD areas	X	
Restrict usage of all mobile phones with integrated cameras	X	
Ensure secure mobile phones are properly configured		X

Table 4-8. Administrator Checklist for Securing Mobile Phones

4.6 Hybrid Mobile Devices

To properly secure a hybrid mobile device, the measures shown in Tables 5-9 and 5-10 should be implemented:

Wireless Device Feature/Configuration	**Required**	**Recommended**
Access Control		
Enable strong password protection scheme for device and network user login (as instructed in the *Secure Remote Computing STIG* developed by DISA for the DOD) https://iase.disa.mil/techguid/stig/src-stig-v1r1-final-021403.doc	X	
Ensure two-factor authentication (smartcard) is used when PKI-based CAC authentication is required http://iase.disa.mil/pki/pkim0812.pdf	X	
Enable the use of biometric reader if available and/or required. https://iase.disa.mil/documentlib.html		X
Ensure secure synchronization of sync stations	X	
Ensure Power-on password is used	X	
Enable password protection on screen saver	X	
Verify device use is in a physically secure location and protected against unauthorized use	X	
Verify encryption scheme used for wireless transmission is FIPS 140-2 and/or NSA Type-1 approved	X	
Turn off integrated mobile/cellular phones features when not in use		X
Disable camera features if at all possible and/or applicable		X

Wireless Device Feature/Configuration	**Required**	**Recommended**
Wireless Network Interface Card (NIC)		
Allow only one NIC to be active on a particular device at any given time	X	
Personal/Host-Based Firewall Software		
Install and run DOD and NIAP-approved personal/host-based firewall	X	
Lock out network access during periods of inactivity (when the computer is not in use)	X	
Block access on high-risk ports as directed by the Network Infrastructure STIG, Appendix G https://iase.disa.mil/techguid/stig/network-stig-v5r2-9-29-03.doc	X	
Enable firewall logging of suspicious activity and user alerts, including inbound and outbound connection attempts	X	
Obtain configuration and signature file updates from network administrator on a regular basis as required by IAVAs	X	
Antivirus Software		
Install and enable DOD-approved antivirus software	X	
Install and update latest virus definitions on a regular basis (weekly); allow Live Updates to DOD servers	X	
Enable and run virus startup scan at each boot	X	
Operating System		
Verify OS is STIG compliant	X	
Install all the latest OS security patches and fixes required by IAVAs	X	
Install all the latest application/software security patches and fixes	X	
Enable media/file/data encryption for all classified information	X	
Disable sharing of local files and drives	X	
Remote Access		
Verify FIPS-140-2 certified VPN client is installed and always used in conjunction with RAS connectivity.	X	
Verify active VPN connection icon present for successful connection attempt	X	

Table 4-9. Client Checklist for Securing Hybrid Mobile Devices

Wireless Device Feature/Configuration	**Required**	**Recommended**
Security Awareness		
Ensure users on the network are fully trained on information assurance awareness and risks associated with using mobile computer technology.	X	
Review NSA PED/PDA database and ensure that all identified vulnerabilities are mitigated.		X
System Security		
Ensure mobile client is using strong password scheme	X	
Disable infrared ports	X	
Ensure wireless NIC on client's mobile computer are up to date with latest patches and upgrades.	X	
Wireless Settings		
Restrict wireless settings to "read only"		X
Ensure "broadcast SSID" setting is disabled	X	
Ensure only an encryption scheme used for wireless transmission is FIPS 140-2 and/or NSA Type-1 approved	X	
Ensure Bluetooth is disabled	X	
Disable ad hoc operation mode on wireless NIC(s)	X	
Security Mechanisms		
Deploy personal/host-based firewall on mobile computer	X	
Deploy antivirus software on mobile computer	X	
Ensure VPN client is installed and working on the user's machine	X	
Ensure wireless NIC on client's mobile computer are up to date with latest patches and upgrades	X	
Restrict all hybrid devices with cellular phones capabilities from entering classified DOD areas	X	
Restrict usage of all hybrid devices with cellular phone + integrated cameras	X	
Ensure secure hybrid devices with cellular phone features to be properly configured		X
Verify split tunneling is disabled on the VPN client (All Internet access would go through DOD firewall or proxy server instead of local service provider)	X	
Application Security		
Ensure non-DOD approved applications are removed from the device	X	

Table 4-10. Administrator Checklist for Securing Hybrid Mobile Devices

** In addition, the following NSA reference documents should be reviewed in conjunction to this document:

- NSA Information Advisory No. IAA-003-2003: “Vulnerability of Computing Devices with Unknown Integrated Wireless Capability.” The advisory can be found at https://iase.disa.mil/documentlib.html#wirelessguid https://powhatan.iiie.disa.mil/wireless/nsaiaa-003-2003.pdf (DOD PKI required for access)

- NSA Information Advisory No. IAA-004-2003, “Virtual Private Networks (VPN) Software”

- NSA Information Advisory No. IAA-004-2004, “Vulnerability and Countermeasures Associated with Integrated Bluetooth Capability.”

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

The following table highlights the relevant policies and guidance for implementing a wireless infrastructure. These policies serve as required practices for DOD users and administrators using wireless networks.

Policy	Description
Wireless STIG	This STIG developed by DISA for the DOD is published as a tool to assist in improving the security of DOD wireless information systems and clients.
Secure Remote Computing STIG	This STIG developed by DISA for the DOD provides the requirements and guidance needed to ensure a secure remote access environment for users within the DOD.
Desktop Application STIG	This STIG developed by DISA for the DOD provides technical security policies, requirements, and implementation details for applying security concepts to Commercial-Off-The-Shelf (COTS) applications on desktop workstations.
Network Infrastructure STIG	This STIG provides security considerations at the network level along with an acceptable level of risks and some guidelines for best network technical practices.
Wireless Security Framework	This guidance provides a common conceptual framework to assist the DOD in coordinating acquisition, development, architecture design, and implementation of 802.11 wireless infrastructures connected to the NIPRNet.
Secure Wireless LAN CONOPS	CONOPS describes the security requirements and architecture of a WLAN using SecNet 11 technology. The WLAN architecture is composed of new security components and technologies that can function in various military environments. https://powhatan.iiie.disa.mil/ (DOD PKI certificate required)
DODD 8100.2	Describes the use of commercial wireless devices, services, and technologies in the DOD Global Information Grid (GIG).
DODD 8500.1	Prescribes the use of a defense-in-depth approach.
DODI 8500.2	Implements policy; assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DOD information systems and networks under DODD 8500.1.
DOD Mobile Code Policy	Categorizes mobile code technologies and restricts their application within DOD based on their potential to cause damage if used maliciously.

This page is intentionally left blank.

APPENDIX B. MOBILE AND WIRELESS STANDARDS

B.1 IEEE 802.11

The 802.11 standard developed by the Institute of Electrical and Electronics Engineers (IEEE) provides a specification for wireless transmission of information in Wireless Local Area Networks (WLAN). Currently, a variety of 802.11 specifications exist. The most widely used is 802.11b. IEEE 802.11a and 802.11g are other popular types using the Ethernet protocol and carrier sense multiple access with collision avoidance (CSMA/CA) for path sharing. The most recently ratified 802.11i standard (approved June 2004) provides an improvement to security in terms of encryption and authentication requirements.

B.2 Bluetooth

There are numerous ways devices can be connected to one another using a cable, including the following:

- Personal digital assistant (PDA) and a docking cradle
- Printer and a laptop
- Headphones and a portable compact disk (CD) player.

Bluetooth (not to be confused with Wireless Fidelity [Wi-Fi]) is a cable replacement technology that uses a short-range radio link to communicate information that typically is sent over a wire. This information may include voice or data.

Bluetooth uses the modified SAFER+ algorithm to encrypt its payload. This algorithm is not Federal Information Processing Standard (FIPS) 140-2 compliant. Unlike Wi-Fi, Bluetooth is not FIPS 140-2 compliant, nor is it permissible to use Bluetooth to transmit or receive classified information (e.g., Secret, Top Secret) unless approval by the Designated Approving Authority (DAA) is granted.

Security flaws do exist in the latest Bluetooth 1.2 standard, the most important of which is the pairing security flaw. During pairing, a personal identification number (PIN) must be entered. In many commercial off-the-shelf (COTS) Bluetooth devices, PINs are only four digits long, which may be insufficient. When possible, PINs should be made as long as possible. A four-digit pin can be cracked in <1 second and a six-digit PIN in 10 seconds; however; according to a recent publication from @Stake, Inc., a 16-digit PIN will take 1 million days to crack. An additional flaw in the latest 1.2 Bluetooth standard regards impersonation. The device hardware address (Media Access Control [MAC] address) can also be spoofed if mutual authentication does not occur. The MAC address is used in key creation, but this is not as much a concern as using no mutual authentication. MAC address spoofing is not specific to Bluetooth; it can also occur with devices using wireless 802.11 or wired Ethernet standards. As a result of these insecurities and flaws, the use of Bluetooth is prohibited in all cases for transmitting or receiving unclassified or classified information.

B.3 Infrared Radiation

Infrared (IR), which operates a frequency between microwaves and visible light, is used in various wireless devices for transmitting information, monitoring services, and controlling applications. The most commonly incorporated IR component is in laptops computers and PDAs. Many wireless device manufacturers have turned on IR functionality in their default settings, leaving these devices vulnerable to device infiltration and information hijacking.

B.4 Cellular Transmission

Cellular transmission is a form of wireless transmission defined as a type of short-wave analog or digital connection to a local cellular tower. Communication is between a mobile device (typically a mobile phone with cellular—digital or analog, Global System for Mobile Communications [GSM], Code Division Multiple Access [CDMA], or Evolution-Data Only [EV-DO] capability) and a service tower.

APPENDIX C. MOBILE AND WIRELESS THREATS

C.1 Malicious Virus and Internet Worms

The threat of computer virus exposure and infection will always exist. Preventing viruses from infiltrating into a mobile device system requires mechanisms for blocking and scanning for these threats.

Computer virus attacks may cause major harm, ranging from erasing data to corrupting files.

C.2 Passive Eavesdropping

If not properly secured, unencrypted wireless device transmissions are susceptible to passive eavesdropping. In this type of attack, an attacker monitors and listens to the wireless sessions using a variety of available hardware and software tools. If the encryption protocol is weak or vulnerable (e.g., Wired Equivalent Privacy [WEP] protocol), the attacker can unencrypt the session and examine the information for indirect or malicious attacks by pretending to be the host or clients.

C.3 Partial or Known Plaintext Attack

Information acquired through access to data transmission can be used for partial or known plaintext attack. The type of information could be a destination Internet Protocol (IP) or medial access control (MAC) address that could be spoofed to generate other forms of attacks, could be used to disrupt transmission, or could manipulate the information being transferred

C.4 Denial of Service Attacks

A Denial of Service (DoS) attack is used to prevent and/or slow down normal use of functions or resources. It is normally an intentional, but can also be an unintentional, overload of a network service or connection with excessive or disruptive data that causes the connection of service to fail. Unintentional DoS could be a mis-configured server such as a domain name service (DNS) server generating an excessive number of session relays that may cause a high amount of network utilization.

In the case of mobile device in a wireless local area network (WLAN) environment, a DoS attack placed on the wireless client can cause local memory overload or prevent connectivity to other resources within the WLAN. DoS attacks can also target wireless switches, access points, or routers preventing other devices from connecting to them.

One difficulty with DoS attacks is locating the source. The attacker may spoof an IP or MAC address, pretending to be someone else. An appropriate security measure that would help prevent some DoS attacks on a mobile device is to implement and enable personal firewall, intrusion detection system, and antivirus software. Configuring these security mechanisms is critical and should be managed by a local network security administrator.

C.5 Man-in-the-Middle Attack

In a man-in-the-middle attack, an attacker intercepts a connection between the wireless device and access point (AP) and impersonates the AP to establish a trusted session with the target.

C.6 Authorized Access

Unauthorized access can occur with or without a user's knowledge.

All mobile devices should be configured to support power-on passwords to protect against unauthorized access. Private or sensitive data should be protected via encryption and passwords if possible. If possible, users should employ different passwords on all their mobile and non-mobile systems to prevent unauthorized access if one device is compromised.

C.7 ARP Attacks

An Address Resolution Protocol (ARP) attack is a technique that uses a device or machine's hardware or MAC address to penetrate a network and access a trusted network. ARP spoofing is a type of ARP attack that alters the ARP cache containing the hardware-to-IP mapping information. The information is simultaneously sent to the target and cache, and the manipulated information is then used to impersonate a trusted host. The attack can involve either circumventing the authorization mechanism or propagating false information and credentials.

C.8 Session Hijacking

Another form of IP spoofing is Session Hijacking in which a Transmission Control Protocol (TCP) session is intercepted between a client and target. The sequencing of three-way handshake of TCP can be disrupted or impersonated between the attacker and the sender or receiver.

C.9 Operating System Vulnerabilities

There are inherent security risks to some of the available commercial mobile devices with respect to the security vulnerabilities presented by the operating system (OS) platforms. It is important for users to understand and evaluate the OS of their mobile device before accessing their network.

C.10 Lost or Stolen Devices

If a mobile device is lost or stolen, proper action should be taken to mitigate the risks of unauthorized access to the network and disclosure of stored data on the device. A supervisor and local network administrator(s) should be contacted to take appropriate actions.

APPENDIX D. SECURITY MECHANISMS

The following security mechanisms are identified, described, and recommended for use for mitigating the vulnerabilities and risks listed previously for using mobile devices. Depending on the capabilities for each mobile device, some or all of these security mechanisms will apply. For example, text-messaging devices can use encryption schemes to security its wireless transmission, but a host-based firewall may not be available or compatible to secure the device from attacks.

D.1 Identification and Authentication

For a network to be protected against unauthorized users, identification and authentication (I&A) mechanisms must be implemented. Many mechanisms exist that provide I&A and authorization when an individual connects to a wireless local area network (WLAN). Authentication solutions include username and passwords, smart cards, biometrics, or public key infrastructure (PKI). Strong authentication will provide access control to the wired network and prevent man-in-the-middle attacks. Users connecting to the wireless network must first authenticate to the wireless network itself. In this case, the user authenticates to an access point or to some form of security gateway. Once successful authentication to the wireless network is complete and the connection is encrypted, authentication to network resources must also occur. This action may include authentication to a Microsoft domain. For user-level authentication, certificate-based (e.g., PKI) or two-factor authentication is recommended.

A PKI enables users of a non-secure public network to securely and privately exchange data through the use of a public and a private cryptographic key pair. The PKI provides for a digital certificate that contains the public key and can identify an individual or an organization that can store and revoke the certificates, if necessary.

Security token devices can also be used for strong authentication. The token device and the authentication server need to be synchronized to be able to authenticate the user. This is said to be two-factor because the token device will present the user with a sequence of characters to be entered into the computer along with an additional password.

In a wireless environment, mutual authentication shall be used to prevent attackers from masquerading as an access point or security gateway. Mutual authentication mitigates the risk that an attacker could potentially masquerade as an access point or a wireless gateway to accept and establish a connection with a wireless client. This would allow the attacker to potentially access data on the client or upload hostile code. If the authentication and authorization methods were properly implemented, the attacker would be unable to use the user credentials or brute force to establish a connection to the wired network. (Note: An attacker who inserts himself or herself in the middle of a wireless connection but does not decrypt traffic or overcome the authentication scheme is not considered a more serious threat than an attacker with an antenna and a wireless sniffer.)

D.2 Personal Firewall

Personal firewalls are software-based solutions that reside on a client’s machine and are either client managed or centrally managed. Client-managed versions are best suited to low-end users because individual users can configure the firewall themselves and may not follow any specific security guidelines. Although personal firewalls offer some measure of protection, they do not protect against advanced forms of attack. Depending on the security requirement, agencies may still need additional layers of protection. Personal firewalls provide additional protection against rogue access points that can be easily installed in public places.

Personal firewalls are now considered to be a requirement on all remote access devices that are accessing a Department of Defense (DOD) system.

D.3 Virus Prevention

DOD policy suggests the use of antivirus software for all handheld devices. Virus applications should enable users to perform routine automatic scanning of e-mails and data files. Each DOD entity with independent wireless security policies should ensure that all remote devices contain the most recent vendor supported antivirus software. The software must be configured to ensure that the user will be prompted to update the virus signatures on a continuous 14-day basis.

D.4 Biometrics

Biometric technology used for authentication purposes serves to identify a user by a physical or biological trait that cannot be replicated, lost, or stolen. In wireless devices, certain biometrics is more readily used than others because of size, portability, and false detection rate. A fingerprint scan is the most common and applicable device that can be integrated into a wireless device. The fingerprint reader can be attached to a mobile device and offer two-factor authentication, along with the usual user name and password. It is relatively accurate but vulnerable to cloning or duplication.

D.5 Encryption

The wireless link and the means by which data is transmitted are primary avenues of attack. There must be an effective way to protect information as it is stored on media or transmitted through network communication paths. The ultimate goal of encryption is to hide information from unauthorized individuals and provide integrity protection. Most algorithms can be cracked, yielding the protected information to be revealed if the attacker has enough time, motivation, and resources. Thus, an approach or a more realistic goal of encryption is to make the time it takes to break the algorithm so long that it is unrealistic to execute a brute-force attack.

The Wired Equivalent Privacy (WEP) Protocol, which is used to secure the link between a wireless client and access point, was originally designed to provide security for WLANs. However, the implementation of the WEP was flawed. The Wireless Fidelity (Wi-Fi) Alliance in conjunction with Institute of Electrical and Electronics Engineers (IEEE) created Wi-Fi Protected Access (WPA) is an interim solution that is interoperable and strongly enhances wireless security. WPA uses the Temporal Key Integrity Protocol (TKIP) to improve data encryption. Although WPA-TKIP still uses the RC4 algorithm, a major difference is that it changes temporal keys every 10, 000 packets and with proper key management. However, WPA-TKIP is not approved for government use because it is not Federal Information Processing Standard (FIPS) 140-2 compliant.

WPA is forward compatible with the IEEE 802.11i security specification ratified in June 2004. The 802.11i security specification includes Advanced Encryption Standard (AES) Counter-Mode Cipher Block Chaining (CBC) Message FIPS 140-2 and is usable by the DOD.

When deploying WLANs, key management must be considered. Key management (the care and distribution of cryptographic keys) is the foundation for any cryptographic system. Without properly protecting cryptographic keys from unauthorized persons, any cryptographic solution will fail to meet its objective. When deploying WLANs, distribution and management of keys must be addressed. Some solutions will use pre-shared keys, whereas others will have a central key management infrastructure (e.g., PKI). Both scenarios have strengths and weaknesses. The use of pre-shared keys creates a challenge in key distribution and protection of keys. A key management infrastructure such as a PKI solves much of the key management and protection problems but requires a complex infrastructure be in place. Consideration should be given to using the DOD PKI when feasible and appropriate.

POLICY

Per DOD policy, all encryption algorithms and protocols must be compliant with the FIPS PUB 140-2. Note that the WEP encryption scheme that is available in most 802.11 products is not FIPS-140-2 compliant. WEP’s flaws are well documented, and tools that crack WEP are readily available via the Internet. Therefore, WEP encryption alone will be insufficient to satisfy the encryption requirement.

In DODD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG),* Section 4.1.2,

> Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the designated approving authority (DAA). At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-1 or FIPS PUB 140-2, Overall Level 1 or Level 2, as dictated by the sensitivity of the data (references (f) and (g)). Encrypting unclassified voice is desirable. PEDs (portable electronic devices) shall use file system encryption. Individual exceptions may be granted on a case-by-case basis as determined by the DAA.

IMPLEMENTATION

The framework presented in this document will use FIPS-compliant algorithms, such as AES or Triple Data Encryption Standard (3DES). All key lengths, including 128, 192, 256, are of AES and are adequate enough to protect classified information up to the Secret level; Top Secret requires key lengths of 192 or 256 (6 CNSS Policy No. 15, FS-1 June 2003). For transmitting unclassified information, AES or 3DES will still be used because the information can be critical to the conduct and operation of organizations.

The organization can choose whether to use Layer 2 or Layer 3 encryption, or both, if the encryption is for non-Joint operations. In the future, most organizations will probably migrate to the IEEE 802.11i solution.

Encryption software can be used to protect the confidentiality of sensitive information stored on handheld devices and mirrored on the desktop personal computer (PC). The information on add-on backup storage modules should also be encrypted and the modules securely stored when not in use. This additional level of security can be added to provide an extra layer of defense to further protect sensitive information stored on handheld devices. Note that if the information is sensitive, the encryption implementation is required to be FIPS 140-2 validated.

D.6 Intrusion Detection/Prevention System

An Intrusion Detection System (IDS) is a software- or appliance-based system used to automatically detect, alert, and potentially prevent unauthorized access to services or resources from trusted and untrusted hosts. Three main types of IDS exist that can be used to monitor mobile device connections: network-based, host-based, and anomaly-based IDS.

Network-based IDS (NIDS) for wireless network, raw network traffic is captured and run against a comparison analysis with a set of signature files with know attack patterns, features, and characteristics. Each packet transmitted is examined. NIDS is usually in a passive mode, but some have the capabilities to send responses to a firewall to prevent an attack or intrusion when detected.

Host-based IDS (HIDS), which resides on each device, is used to protect against intrusions or attacks generated against a device. Normally, this software is loaded onto the existing OS of the device.

Anomaly-based IDS is a pattern recognition approach to detecting intrusions within a network environment. The concept is to understand patterns of user traffic and behavior to locate deviations from what would be considered as normal patterns. The disadvantage of using anomaly-based IDS is the scalability and flexibility with the detection model. Typical networks will undergo continuous change and may lead to difficulty with configuring this type of IDS. The most common IDS systems currently used are network and host-based, but this concept has been and will continue to be incorporated as a hybrid system to other IDS devices.

A wireless IDS is highly recommended for monitoring the airwaves for adversaries, behavioral changes within the WLAN, and wireless-specific attacks. The use of a communications security (COMSEC) keyed wireless card on a NSA-certified Type-1 device presents problems for wireless device detection because it is a proprietary product that encrypts the header information of each packet.

The (Defense Information Systems Agency [DISA]) *Wireless Security Technical Implementation Guide (STIG)* requires the use of an IDS; however, it does not specify the use of a wireless IDS or a network-based IDS. For a National Security Agency (NSA) certified Type-1 device use on the Secret Internet Protocol Router Network (SIPRNET), a Network IDS (N-IDS) can be used to monitor all traffic entering the SIPRNET via each access point (AP). Note that a network-based IDS could detect card compromise if a card were lost or stolen whereas a wireless IDS cannot. A wireless IDS should be used to scan for rogue access points and to identify and locate the source of attacks on the network.

A wireless IDS/radio frequency (RF) monitor may be installed to detect active wireless attacks and DoS activities. In addition, all traffic passed from the AP to the SIPRNET will be monitored by an N-IDS. Because of the nature of the Internet Protocol (IP) address and the threat that it presents if discovered, a security policy for handling IP addresses must be presented (i.e., separate IP addresses should be used within a virtual local area network [VLAN]). The controlled space in which an AP will reside must be determined and certified for maximum protection. All APs that will connect to the SIPRNET must be protected at all times.

D.7 RF Monitoring

With the sophistication of WLANs and the numerous components needed to undertake the mountainous task of deploying a secure WLAN, it is essential that network administrators be able to effectively monitor all network security components. By constantly monitoring a network, the administrators should be able to manage the entire WLAN. The robustness and integrity of a WLAN rely on the network administrator’s ability to troubleshoot problems, respond to misconfigurations, and plan for future implementations and upgrades.

Two types of RF monitoring exist. One type is the act of physically driving or walking around certain areas, equipped with a sniffer to detect the presence of WLANs. Another more effective way is to survey wireless devices and client machines by using sensors that are strategically placed at the various components of the WLAN that report back to a centralized monitoring/management console.

Detecting rogue wireless access points is an essential capability for a secure network. Because of the inexpensive nature and availability of commercial access points, it should not be overlooked that employees may bring them into the office to offer convenient access to network resources.

Further, if a potential attacker could get in range of legitimate wireless clients and lure them to associate with his access point, attacks such as man-in-the-middle could easily be performed.

For this and many other reasons, it is highly recommended that a multipronged defense strategy for detecting unauthorized “rogue” access points be implemented. The NSA C group in accordance with the DOD policy recommends that all wireless networks use RF monitoring IDSs.

POLICY

According to DOD policy, measures must be implemented to monitor policy. Depending on the technology used, RF monitoring capabilities will help mitigate attacks, such as DoS, man-in-the-middle, and identity theft. This will satisfy the policy because the policy states that the security measures must protect not only from outside sources but also from potential attacks from friendly sources.

In DODD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG),* Section 4.1.4—

> Measures shall be taken to mitigate denial of service attacks. These measures shall address not only threats from the outside, but potential interference from friendly sources.

In Section 4.6,

> The DOD Components shall actively screen for wireless devices. Active electromagnetic sensing at DOD or contractor premises to detect/prevent unauthorized access of DOD information systems shall be periodically performed by the cognizant DAA or Defense Security Service office to ensure compliance with the DITSCAP ongoing accreditation agreement (reference (e)).

IMPLEMENTATION

When an RF monitoring scheme is employed, it should contain the necessary mechanisms to provide a real-time network survey. The use of stationary or mobile sensors will allow for the detection of rogue access points, ad hoc networks, and unencrypted traffic. RF monitoring can also provide the following:

- Monitoring of off-hours traffic
- Mitigation of DoS attacks
- Detection of ad hoc networks
- Identification of hardware failure, network interference, slow connection speeds, and network mis-configurations.

Continuously surveying the airwaves in and around the facility housing the WLAN will allow for constant monitoring of a system's components, assisting in the prevention and detection of attacks.

D.8 Access Point Configuration and Features

D.8.1 Service Set Identifier

A Service Set Identifier (SSID) is a unique identifier that stations must use to be able to communicate with an access point and use the most basic authentication mechanism for 802.11 acting as a simple password and providing a measure of security between the local access point and the wireless client. This simple password can be any alphanumeric entry up to a maximum of 32 characters. Because the SSID broadcast is transmitted in clear text, it is susceptible to SSID scanning and passive eavesdropping. SSID broadcast should be disabled on the access point.

D.8.2 Media Access Card Access List

Media access card (MAC) address filtering restricts all wireless devices, based on their MAC address, from connecting to an access point unless they are explicitly identified authorized to. This is not a scalable solution for large networks because maintaining a large access list would require extensive utilization on the AP. This method of authentication is susceptible to MAC address spoofing and DoS attacks. This may be a suitable solution for small networks and defend against an attacker limited resources and knowledge.

D.9 Encryption Methods

D.9.1 Wired Equivalent Privacy

Originally, WEP was the only 802.11 wireless protection mechanism available. The discovery of the vulnerabilities and easy of defeating WEP authentication has made this authentication mechanism an ineffective solution. WEP is not compliant with FIPS 140-2 and is not an approved encryption method to be used.

D.9.2 Wireless Fidelity Protected Access

Although WiFi WPA is a strong encryption method to use compared with WEP, it is also not FIPS 140-2 compliant.

D.9.3 Robust Secure Network Standard

Robust Secure Network (RSN) is a major component of the IEEE 802.11i wireless security standard. Specifically, it is a total redesign of the authentication and association mechanisms used in existing 802.11 standards. Because the 802.11i standard is approved and ratified, vendors can begin to provide devices that implement this product. Note that the following implementation is based on capabilities of RSN devices.

The RSN capability will be contained in devices at the wireless edge of the network (i.e., access points and wireless switches) rather than in devices further inside the WLAN as in the other implementations. Because of the significant changes in the security mechanisms of 802.11i, legacy access points and wireless network interface cards (NIC) will not be upgradeable to the RSN standard.

D.9.3.1 Advanced Encryption Standard

AES is a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. According to the Network Infrastructure STIG, Section 5.2.1,

> “NSO will ensure that all communications to/from the network will employ at a minimum a FIPS 140-2 approved data encryption algorithm (i.e., AES or 3DES) (see http://csrc.nist.gov/cryptval).”

The framework presented in this document will use FIPS-compliant algorithms, such as AES or 3DES. All key lengths, including 128, 192, 256, are of AES and are adequate enough to protect classified information up to the Secret level; Top Secret requires key lengths of 192 or 256 (6 CNSS Policy No. 15, FS-1 June 2003). For purposes of transmitting unclassified information, AES or 3DES will still be used because the information can be critical to the conduct and operation of organizations.

D.10 Extensible Authentication Protocol—Transport Layer Security

Extensible Authentication Protocol—Transport Layer Security (EAP-TLS) is mutual authentication between wireless access point and client and dynamic keying mechanism. It can use a shared secret or PKI to distribute keys from a central certificate distributing authority.

EAP-TLS can be effective in stopping man-in-the-middle attacks. An attacker cannot deceive the client into thinking that he or she is authenticated to the AP because the client also is required to authenticate the AP.

D.11 Protected Extensible Authentication Protocol

Protected Extensible Authentication Protocol (PEAP) is another mutual authentication protocol similar to EAP-TLS. The server is first authenticated and an encrypted tunnel between the client and server is established. Then instead of using the older attribute-value pair to authenticate the client, the authentication is limited to any EAP method.

D.12 Tunneled Transport Layer Security

Tunneled Transport Layer Security (TTLS) is a two-stage protocol that does not require a PKI. First, the client and server will establish an encrypted tunnel. Then, the server sends its certificate to the client for authentication followed by the client sending its certification for client validation. This process does not require digital certificates because the credentials exchange passes through an encrypted tunnel.

D.13 Physical Security/Access Control

Physical security for mobile devices is defined differently for a controlled/trusted environment and uncontrolled environment (e.g., public location, personal house, hotel).

The site and infrastructure security policy should outline the methods used for providing and controlling physical access to the mobile devices in a controlled environment. Some important elements to be considered are as follows:

- Methods of controlling physical access to a building, office, or room
- Procedures for granting physical access: keys, badges, biometric devices
- Access limitations based on level of clearance or status
- Access limitations based on set hours of operations.

D.14 Infrared Device

Depending on the mobile device type, the infrared port should be configured on the device to prevent unauthorized connection and information extraction. This may not apply to Tablet PCs because the disabling the IR port may prevent use of the electronic pen.

D.15 Virtual Private Network

Virtual private networks (VPN) provide various methods for protecting network data integrity, confidentiality, and availability using techniques such as connectionless integrity, data origin authentication, traffic analysis, and access protection. A VPN is a private data network that maintains confidentiality by using encryption and security procedures across a shared public telecommunications infrastructure. The data is transported or tunneled across a public or private network employing encryption technologies (e.g., Layer 2 Tunneling Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP], and Internet Protocol Security [IPSec]). Typically, VPN encryption is implemented at the local network entry point (i.e., firewall or Premise router), thereby freeing the end systems from having to provide the necessary encryption or communications security functions.

PPTP, an extension of the Internet’s Point-to-Point Protocol (PPP), allows a host with PPP client support to use an Internet service provider (ISP) to connect securely to a server elsewhere in the local area network. L2TP is an extension of PPTP, which enables VPN implementation by merging PPTP and Layer 2 Forwarding (L2F) protocols. L2TP does not include mechanisms for encryption or authentication and must obtain these services through use in conjunction with other devices or protocols.

IPSec is the most widely used secure network protocol. IPSec provides VPN capabilities at Layer 3 of the Open System Interconnection (OSI) model, whereas PPTP and L2TP operate at Layer 2. IPSec consists of two packet encapsulation protocols: Authentication Header (AH), which allows authentication of the sender; and Encapsulating Security Payload (ESP), which supports authentication of the sender and encryption of data. In addition, IPSec supports two encryption modes: transport and tunnel. Transport mode encrypts the data portion (payload) of each packet, but does not encrypt the header. Tunnel mode encrypts the header and the payload, making this mode more secure. In either mode, the receiving side of an IPSec-compliant device decrypts each packet.

VPNs can be divided into three categories: remote access, site-to-site, and extranet. The type of VPN technology employed is based on bandwidth requirements, resources, and differing security needs, all of which are determined by the function the technology will perform and impact the placement of the device in the network infrastructure. Placement of the VPN should not adversely impact the Enclave security, and all VPN traffic must pass through the Enclave Security Architecture. Although encrypted data (e.g., Secure Sockets Layer [SSL], Secure Shell [SSH], Transport Security Layer [TSL]) that enters the VPN tunnel does not need to be unencrypted before leaving the tunnel, the data must pass through the respective application proxy on the firewall. Host-to-gateway VPNs are preferred; however, if a host-to-host VPN is required to meet mission needs, it will be established between trusted, known hosts. (Refer to the *Network Infrastructure STIG, Section 5.2.1.*)

- The NSO will ensure that all VPN implementations adhere to Section 5.2.1, VPNs, in the Network Infrastructure STIG.
- The NSO will ensure that all broadband remote user access (with the exception of dial-in) will be encrypted via VPN.
- The NSO will ensure that VPNs are established as tunnel type VPNs that terminate outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router).
- The NSO will ensure that all communications to/from the network will employ at a minimum a FIPS 140-2 approved data encryption algorithm (i.e., AES or 3DES). (See *http://csrc.nist.gov/cryptval*)
- The NSO will ensure that VPNs will use the IPSec AH and ESP protocol in tunnel mode. For legacy support, L2TP may be used provided authentication and encryption are provided by another device or protocol.

- The NSO will ensure that data integrity is achieved with the use of 128-bit MD5 or 160-bit SHA.

For a remote access VPN to be as secure as possible, the traffic should be encrypted and integrity protected. That is to say, without encryption, an unauthorized person could access the data, and without integrity protection, encrypted traffic is susceptible to attacks and modification of data. The VPN client software communicates with a VPN device within the network infrastructure and establishes a secure connection over the Internet. It is strongly recommended that with any implemented VPN solution the VPN client be from the same vendor.

  - The remote user will ensure that Split Tunneling is disabled on the VPN Client (i.e., upon the establishment of a VPN connection to a DOD network, no other connections of any kind will be established [e.g., if home networks are used, no connection between the device and other home network devices will be established during a VPN session]).
  - The remote access user will not configure or change security settings of the VPN client without prior approval from the system or network administrator.
  - The Information Assurance Officer (IAO) will ensure that the remote user has complete instructions on the use of a VPN client used to access a DOD network or resource.

- The IAO will ensure that a VPN client supports and is configured for IPSec attributes such as 3DES, Tunnel encapsulation mode, and a FIPS 140-2 approved authentication algorithm.

APPENDIX E. LIST OF ACRONYMS

2G	Second Generation
3DES	Triple Data Encryption Standard
3G	Third Generation
AAA	Authentication, Authorization, Account
ADC	Analog to Digital Conversion
AES	Advanced Encryption Standard
AESCCMP	Advanced Encryption Standard Counter-Mode Cipher Block Chaining Message Authentication Code Protocol
AH	Authentication Header
AMP	Advanced Mobile Phone System
AP	Access Point
API	Application Programming Interface
ARP	Address Resolution Protocol
CAC	Common Access Card
CBD	Cipher Block Chaining
CD	Compact Disk
CDMA	Code Division Multiple Access
COMSEC	Communications Security
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CPU	Central Process Unit
CSA	Cognizant Security Authority
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving Authority
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DNS	Domain Name Service
DOD	Department of Defense
DODD	Department of Defense Directive
DoS	Denial of Service
EAP-TLS	Extensible Authentication Protocol–Transport Layer Security
ESP	Encapsulating Security Payload
EV-DO	Evolution–Data Only
FCC	Federal Communications Commission
FIPS PUB	Federal Information Processing Standard Publication
FM	Frequency Modulation
FNBDT	Future Narrowband Digital Terminal

GIG	Global Information Grid
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HAIPE	High-Assurance Internet Protocol Encryption
HAPIS	High-Assurance Internet Protocol Interoperability Standard
HIDS	Host-based Intrusion Detection System
I&A	Identification and Authentication
IA	Information Assurance
IAVA	Information Assurance and Vulnerability Assessment
IDS	Intrusion Detection System
IE	Internet Explorer
IEEE	Institute of Electrical and Electronics Engineers
IM	Instant Messaging
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Infrared
ISP	Internet Service Provider
IAO	Information Assurance Officer
IT	Information Technology
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LCD	Liquid Crystal Display
MAC	Media Access Control
MAC	Media Access Card
MHz	Megahertz
MS	Microsoft
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection System
NIPRNET	Unclassified But Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory Memorandum
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OS	Operating System
OSI	Open System Interconnection

PACE	Portable Applications Compatibility Environment
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications System
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PED	Portable Electronic Device
PIN	Personal Identification Number
PK	Public Key
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RAM	Random Access Memory
RAS	Remote Access Service
RF	Radio Frequency
ROM	Read-Only Memory
RSN	Robust Secure Network
S/MIME	Secure/Multipurpose Internet Mail Extension
SCIF	Sensitive Compartmented Information Facility
SIPRNET	Secret Internet Protocol Router Network
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guide
STREAMS	Surface Traffic Enhancement and Automation Support
SWLAN	Secure Wireless Local Area Network
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
TSL	Transport Security Layer
TTLS	Tunneled Transport Layer Security
UHF	Ultra High Frequency
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMP	Windows Media Player
WPA	Wi-Fi Protected Access