

UNCLASSIFIED



WIRELESS SECURITY TECHNICAL IMPLEMENTATION GUIDE STIG OVERVIEW

Version 6, Release 9

24 October 2014

Developed by DISA for the DoD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA FSO of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Background	1
1.2 Authority	1
1.3 Scope	1
1.4 Vulnerability Severity Category Code Definitions.....	1
1.5 STIG Distribution.....	2
1.6 SRG Compliance Reporting	2
1.7 Document Revisions.....	2
2. ASSESSMENT CONSIDERATIONS	3
2.1 Wireless and Mobility Policy – Applicable To All Devices	3
2.2 WLAN Compliance Requirements.....	3
2.3 Wireless Metropolitan Area Network (WMAN) Compliance Requirements.....	3
2.4 Bluetooth	4
2.5 Miscellaneous Wireless Networking Systems Compliance Requirements.....	4
2.5.1 RFID Systems	4
2.5.2 Wireless VoIP	5
2.5.3 Wireless Keyboards and Mice	5
2.5.4 ZigBee.....	5
2.6 PDA, Smartphone, and Non-Wireless Email Device Compliance Requirements	6
3. CONCEPTS AND TERMINOLOGY CONVENTIONS.....	7
4. GENERAL SECURITY REQUIREMENTS.....	8
APPENDIX A: VMS PROCEDURES.....	9

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2
Table A-1: VMS Asset Matrix	9

1. INTRODUCTION

1.1 Background

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

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that “all IT that receives, processes, stores, displays, or transmits DoD information will be [...] configured [...] consistent with applicable DoD cybersecurity policies, standards, and architectures” and tasks that Defense Information Systems Agency (DISA) “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Scope

This document is a requirement for all DoD administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

1.4 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

1.5 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is <http://iase.disa.mil/>.

1.6 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component DAA personnel for risk assessment purposes by request via email to: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil. DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

2. ASSESSMENT CONSIDERATIONS

2.1 Wireless and Mobility Policy – Applicable To All Devices

Wireless policy requirements are applicable to all wireless systems used in the DoD to connect to DoD networks or are used to store, process, receive, or transmit DoD data. Review Wireless Policy checks for all wireless devices (classified or unclassified) that are used to process, transmit, store, or connect to DoD information or enclave resources. These checks should be reviewed before other wireless equipment specific checks are reviewed. These policies are listed in VMS under the Non-Computing Assets, Wireless Policy asset posture. The reviewer should create one non-computing asset for the each wireless network (e.g., Site Q WLAN, Fort Smith BlackBerry System).

2.2 WLAN Compliance Requirements

This section applies to DoD WLAN systems (Institute of Electrical & Electronics Engineers, Inc. [IEEE] 802.11) that are owned and/or operated by DoD components and does not apply to the use of commercial, public, or home WLAN systems used for remote connections to DoD networks, which are covered in Section 2.6 of this STIG.

A WLAN client can be a laptop, desktop personal computer, or any Commercial Mobile Device (CMD) that utilizes a WLAN to connect to a network.

DoD WLAN client security controls apply to unclassified WLAN clients. Add the “Wireless LAN Client” to a workstation or Personal Digital Assistant (PDA)/Personal Electronic Device (PED) asset that has been registered in VMS. If the workstation or PED will be used for wireless remote access to a DoD network, see Section 2.6 of this STIG.

NOTE: PDA and PED are legacy terms while CMD is the current DoD term for mobile handheld devices. PDA and PED will continue to be used in this document until the next major update of the Wireless STIG.

2.3 Wireless Metropolitan Area Network (WMAN) Compliance Requirements

DoD WMAN security controls apply to WMAN systems (IEEE 802.16-2004 [formally 802.16d] and 802.16e-2005 [formally 802.16e]) that are owned and/or operated by DoD components and do not apply to the use of commercial WMAN systems for remote connections to DoD networks, which is covered in Section 2.6 of this STIG. The IEEE 802.16-2004 and 802.16e-2005 standards are sometimes referred to as fixed Worldwide Interoperability for Microwave Access (WiMAX) and mobile WiMAX, respectively. WMAN is a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links (bridge) to portable and fully mobile WMAN subscriber (client) access to Internet services.

WMAN systems are designed for medium range “last mile” connections and are primarily used with the DoD as wireless bridges to connect two sites or buildings. Recently, wireless carriers have deployed WMAN systems to provide wireless digital broadband services as an alternative to cable, fiber-optic, and cellular Third Generation (3G) systems.

The following WMAN assets should be registered in VMS:

WMAN Subscribers – client devices (such as, PDAs, laptops, etc.) that are used to connect to DoD-owned WMAN networks. Requirements for WMAN subscribers that are used for remote access to DoD networks via public WMAN access points are covered in Section 2.6.

2.4 Bluetooth

DoD Bluetooth requirements apply to all wireless clients (e.g., PDA, laptops, and desktops) with Bluetooth. These requirements also apply to Bluetooth keyboards, mice, headsets, and any other Bluetooth device that transmits or receives DoD data or voice communications.

Bluetooth-enabled electronic devices connect and communicate wirelessly via short-range (100 meters [m] or less) in ad hoc networks called piconets. Bluetooth and 802.11 wireless technologies share some characteristics and overlap slightly in some usage models, but they serve fundamentally different purposes. Additional technical information on Bluetooth systems is found in the technical references listed in “Applicable References” below.

Bluetooth systems can be operated in the DoD, provided they meet required DoD security controls. A Bluetooth client asset should be registered in VMS according to the primary purpose of the device (e.g., workstation or PDA/PED). First, register the workstation or PDA/PED asset, and then add the “Bluetooth Radio” asset posture.

NOTE: Bluetooth security requirements for Mobile OS devices are found in the corresponding Mobile OS STIG (e.g., BlackBerry, Windows Phone, Android, and iOS smartphone and tablets).

2.5 Miscellaneous Wireless Networking Systems Compliance Requirements

2.5.1 RFID Systems

Radio Frequency Identification (RFID) systems are primarily used to track an object, animal, or person by storing ID information on an electronic “tag” that is attached to the asset being tracked. The tag is then read by a “scanner,” which reads the ID information on the tag. See the list of technical references for more information on the types of RFID systems in “Applicable References” below.

When an RFID scanner is connected to a DoD computer or PDA/PED for the purpose of downloading RFID tag data, the workstation should be registered in VMS and the asset posture “RFID Workstation” assigned to that workstation. In addition, the OS and any installed applications should also be added to the asset posture. The asset posture “RFID Scanner” should be assigned to a PDA/PED asset. There is no requirement to register RFID tags. See Appendix A for additional details.

2.5.2 Wireless VoIP

Wireless VoIP phones are PDAs or smartphones that use a site WLAN or WMAN for voice

transmission. Requirements for wireless VoIP phones are found in the WLAN or WMAN client sections of this document and in the VoIP STIG.

In VMS, assign the PDA/PED posture to the VoIP phone asset. In addition, assign either the “Wireless LAN Client” posture or “WMAN Subscriber” posture to the asset based on the type of wireless system the VoIP phone is connecting to. Also, assign the VoIP posture as defined in the VoIP STIG and checklist. There are no wireless VoIP specific security requirements. See Appendix A for additional details.

2.5.3 Wireless Keyboards and Mice

These devices must be documented on the site’s wireless equipment list. Also apply Wireless Policy checks. These assets are entered into VMS as part of a wired or wireless workstation asset posture. Register the workstation asset and add the “Wireless Peripheral” as part of the asset posture. In addition, either the “Wireless LAN Client” or “Bluetooth Radio” asset posture must be added to the workstation posture, based on the type of wireless network that is used by the wireless keyboard and mouse.

Workstation assets are computing assets. If a wired keyboard or mouse is used on a wireless workstation, ensure the workstation is STIG compliant.

If the radio system used on the wireless mouse and keyboard is not neither WLAN nor Bluetooth, use the “Bluetooth radio” asset posture.

2.5.4 ZigBee

ZigBee is a low-cost, low-power, wireless mesh networking standard. ZigBee and Bluetooth are both Wireless Personal Area network (WPAN) technologies and both are sub-sets of the same IEEE 802.15 standard. (ZigBee is covered in the IEEE 802.15-4 standard, while Bluetooth is covered by the IEEE 802.15-1 standard.)

ZigBee is targeted at radio frequency (RF) applications that require a low data rate, long battery life, and secure networking including wireless control and monitoring applications. ZigBee radios are now being integrated in some DoD systems. ZigBee is typically used for device-to-device communications as opposed to Bluetooth, which is used frequently for human interface devices.

A ZigBee client asset should be registered in VMS according to the primary purpose of the device (e.g., workstation or PDA/PED). First, register the workstation or PDA/PED asset, and then add the “ZigBee Radio” asset posture. See Appendix A for additional details.

2.6 PDA, Smartphone, and Non-Wireless Email Device Compliance Requirements

PDA/PED security controls apply to DoD-owned, personally-owned, or contractor-owned handheld PDAs that are used to store, process, receive, and/or transmit DoD information, as follows:

- Cellular phones (non-smartphone) which are not used as wireless email devices
- Two-way pagers

- Handheld barcode scanners
- Cordless phones
- Commercial two-way radios

The checks in this section do not apply to smartphones that are used for wireless email, and the Secure Mobile Environment Portable Electronic Device (SME PED). Smartphone requirements are found in product-specific STIGs or in the MOS SRG. Use the appropriate wireless email system STIG to perform a security review or to review required security controls for these systems.

Register a PDA, handheld barcode scanner, cordless phone, commercial two-way radio, or pager in VMS by selecting “PDA/PED” as the asset posture.

NOTE: If the handheld PDA/ is used to remotely access DoD networks, see additional requirements in Section 2.6. Not all PDA/PED checks apply to every type of PDA; applicability comments exist in many of the checks.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

The benchmarks contained in this STIG are the remnants of the previous release that are non-network infrastructure. They are devices that employ wireless technologies and interact either with each other or network infrastructure capabilities. Future releases of these benchmarks will be in individual STIG releases or will be combined into other existing mobility-related STIG releases. Necessary details, concepts, and terminology are contained within the specific benchmark files associated with this STIG.

4. GENERAL SECURITY REQUIREMENTS

Since the benchmarks contained within this STIG are a consolidation of non-networking wireless capabilities and devices, specific security requirements are maintained within the individual benchmark for the technology required, and will not be stated here. Future releases of these benchmarks will be in individual STIG releases or will be combined into other existing mobility related STIG releases.

APPENDIX A: VMS PROCEDURES

Use the following matrix to select the appropriate asset type for each wireless asset. **NOTE:** A wireless network/system is registered as a separate Non-computing Computing asset, but the network hardware components must also be registered as Computing assets. Both assets must be included in the SRR of a wireless network to ensure a complete review of all applicable security policies.

Table A-1: VMS Asset Matrix

Wireless Technology	VMS Asset	Asset Posture
Non-computing – Used for registering wireless networks and systems. Applies general networking environment policies.		
General Mobil/Wireless Device		
Create a site Non-Computing Wireless System asset (example: DISA FSO Wireless System)	Non-Computing	<p>Assign the following posture to the site wireless system:</p> <p>Non-Computing > Policy > Wireless Pol > General Wireless Policy</p> <p>If smartphones (blackberry, iphone, ipad, pdas, etc.) are used at the site, also assign the following posture:</p> <p>Non-Computing > policy > wireless pol > Smartphone Handheld Policy</p> <p>If the site has wlan access points, also assign the following posture:</p> <p>Non-Computing > policy > wireless pol > Wireless LAN Access Point policy</p> <p>If the site has wlan clients, also assign the following posture:</p> <p>Non-Computing > policy > wireless pol > Wireless Remote Access Policy</p>
Computing – Used for registering wireless hardware assets (such as, PEDs, Access Points (APs), and client workstations with wireless NICS installed)		
WLAN Systems		
WLAN Client -For WLAN computers, the Windows reviewer must review and register the asset prior to the wireless review being entered into VMS. -Register a sample of clients only.	Computing	<p>Add the following asset posture to a workstation or PDA/PED asset that has been registered in VMS:</p> <p>Network > Data Network > Wireless > Wireless Client > Wireless LAN Client</p> <p>NOTE: Apply the “WLAN Client” posture to any wireless device, including cameras, printers, and keyboards that use an IEEE 802.11 WLAN to connect to a DoD network.</p>

WMAN Systems		
WMAN Access Point	Computing	<p>Network > Data Network > Wireless > WMAN Access Point</p> <p>Operating System > Embedded OS > Other Network OS (mark these checks as N/A)</p> <p>Network > Data Network > Network Appliance</p>
Bluetooth Systems		
Bluetooth Radio	Computing	<p>Add the following asset posture to a workstation or PDA/PED asset that has been registered in VMS:</p> <p>Network > Data Network > Wireless > Wireless Client > Bluetooth Radio</p> <p>NOTE: Apply the “Bluetooth Radio” posture to any wireless device, including cameras, printers, and keyboards that use Bluetooth to connect to a DoD network or workstation. Also, apply the “Bluetooth Radio” posture to wireless USB devices.</p>
Other Wireless Networking Systems		
RFID Workstation (workstation RFID scanner connects to download scanned data)	Computing	<p>Add the following asset posture to a workstation asset that has been registered in VMS:</p> <p>Network > Data Network > Wireless > RFID > RFID Workstation</p>
RFID Scanner	Computing	<p>Add the following asset posture to a PDA/PED asset that has been registered in VMS:</p> <p>Network > Data Network > Wireless > RFID > RFID Scanner</p>
Wireless VoIP Phone	Computing	<p>Add the following asset postures to a PDA/PED asset that has been registered in VMS:</p> <p><u>Either</u></p> <p>Network > Data Network > Wireless > Wireless Client > Wireless LAN Client</p> <p><u>Or</u></p>

		Network > Data Network > Wireless > Wireless Client > <i>WMAN Subscriber</i> <u>And</u> VoIP Posture, refer to the VoIP STIG or checklist for the VMS condition/target.
Wireless Keyboards and Mice	Computing	Add the following asset postures to a workstation or PDA/PED asset that has been registered in VMS: Network > Data Network > Wireless > <i>Wireless Peripheral</i> <u>Either</u> Network > Data Network > Wireless > Wireless Client > <i>Wireless LAN Client</i> <u>Or</u> Network > Data Network > Wireless > Wireless Client > <i>Bluetooth Radio</i> If the radio system used on the wireless mouse and keyboard is not WLAN or Bluetooth compatible, the “Bluetooth Radio” asset posture must be added to the workstation posture.
Zigbee Radios	Computing	Add the following asset posture to a workstation or PDA/PED asset that has been registered in VMS: Network > Data Network > Wireless > Wireless Client > <i>ZigBee Radio</i>
PDAs/Cell Phones/Bar Code Scanners/Cellular Boosters		
PDA/Smartphones/Cell Phones/Bar code scanners/two-way radios/cordless phones/two-way pagers This posture does not apply to wireless e-mail PDAs.	Computing	NOTE: Do not mark as a workstation Network > Data Network > Wireless > <i>PDA/PED</i> Operating System > Embedded OS > <i>Other Network OS</i> (mark these checks as N/A)
Cell Phone Boosters	Computing	Register device as a network appliance. Network > Data Network > <i>Network Appliance</i>
Smartphone and Tablet CMDs and Servers		

Smartphone and Mobile Device Management Server Blackberry, BlackBerry Enterprise server Windows Mobile wireless email PDAs and servers SME PED PDAs and servers	Computing	See the appropriate Smartphone or MDM STIG.
--	-----------	---