



# WIRELESS SECURITY CHECKLIST

Version 5, Release 2.2

26 March 2008

**Developed by DISA for the DoD**

Database Reference Number: \_\_\_\_\_

CAT I: \_\_\_\_\_

Database entered by: \_\_\_\_\_ Date: \_\_\_\_\_

CAT II: \_\_\_\_\_

Technical Q/A by: \_\_\_\_\_ Date: \_\_\_\_\_

CAT III: \_\_\_\_\_

Final Q/A by: \_\_\_\_\_ Date: \_\_\_\_\_

CAT IV: \_\_\_\_\_

TOTAL: \_\_\_\_\_

**UNCLASSIFIED**

Unclassified UNTIL FILLED IN

CIRCLE ONE

**FOR OFFICIAL USE ONLY** (mark each page)

**CONFIDENTIAL and SECRET** (mark each page and each finding)

**Classification is based on classification of system reviewed:**

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

## TABLE OF CONTENTS

	<b>Page</b>
<b>SUMMARY OF CHANGES.....</b>	<b>VII</b>
<b>1. HOW TO PERFORM A WIRELESS REVIEW.....</b>	<b>1</b>
<b>2. WIRELESS POLICY – APPLICABLE TO ALL DEVICES.....</b>	<b>3</b>
<b>WIR0010 All Wireless systems must have DAA approval.....</b>	<b>4</b>
<b>WIR0011 Personally owned PEDs are used .....</b>	<b>5</b>
<b>WIR0016 Maintain an equipment list of all approved PED devices.....</b>	<b>6</b>
<b>WIR0030 Document equipment in the SSP.....</b>	<b>7</b>
<b>WIR0072 Wireless network devices must be physically protected .....</b>	<b>7</b>
<b>WIR0076 Require signed user agreement .....</b>	<b>8</b>
<b>WIR0180 Wireless devices allowed into SCIFs must be DCID compliant.....</b>	<b>10</b>
<b>WIR0225 CTTA coordination and proper separation required .....</b>	<b>11</b>
<b>3. WLAN COMPLIANCE REQUIREMENTS.....</b>	<b>12</b>
3.1 WLAN Network Devices .....	12
<b>WIR0070 Obtain US Forces or host nation approval, if applicable .....</b>	<b>12</b>
<b>WIR0075 All DoD sites must perform periodic WLAN discovery .....</b>	<b>13</b>
<b>WIR0140 Change default SSID .....</b>	<b>14</b>
<b>WIR0150 Disable SSID broadcast mode .....</b>	<b>14</b>
<b>WIR0160 Enable MAC address filtering for WLAN.....</b>	<b>15</b>
<b>WIR0230 WLAN session time out capability set to 15 minutes or less .....</b>	<b>16</b>
<b>WIR0250 AP transmit power controlled to minimize service to unneeded areas .....</b>	<b>17</b>
<b>WIR0270 Encryption requirements for unclassified WLAN .....</b>	<b>18</b>
<b>WIR0275 WLAN network and client device NICs are both Wi-Fi and WPA2 certified.....</b>	<b>19</b>
<b>WIR0290 Install WLAN network devices in an isolated network .....</b>	<b>20</b>
<b>WIR0300 Use wireless IDS to monitor unauthorized WLANs on DoD networks.....</b>	<b>22</b>
<b>WIR0330 Management access must use compliant password.....</b>	<b>23</b>
3.2 WLAN Clients – General Requirements.....	24
<b>WIR0040 Use STIG compliant OS configuration on all client devices.....</b>	<b>24</b>
<b>WIR0050 Configure Antivirus software on all wireless clients.....</b>	<b>25</b>
<b>WIR0100 Use an approved and properly configured personal firewall.....</b>	<b>26</b>
<b>WIR0125 Enable mutual authentication for peer-to-peer (ad hoc) WLANs.....</b>	<b>27</b>
<b>WIR0130 WLAN is used; do not use NICs that cannot disable peer-to-peer .....</b>	<b>28</b>
<b>WIR0161 Wired and wireless NICs are not active simultaneously.....</b>	<b>29</b>
<b>WIR0163 Disable WZC service on Windows clients .....</b>	<b>30</b>
<b>WIR0167 Change default setting for WLAN NIC radio to “Off” .....</b>	<b>31</b>
<b>WIR0168 For wireless client, do not set preferred network to auto-connect .....</b>	<b>31</b>
<b>WIR0240 Use strong authentication .....</b>	<b>32</b>
<b>WIR0260 Use FIPS 140-2 encryption for wireless clients (data at rest).....</b>	<b>33</b>
<b>WIR0275 WLAN network and client device NICs are both Wi-Fi and WPA2 certified.....</b>	<b>34</b>
<b>WIR0280 Wireless clients connecting via the Internet must be compliant.....</b>	<b>35</b>

3.3	Classified WLANs .....	36
	<b>WIR0190 Do not use embedded NICs for classified</b> .....	36
	<b>WIR0203 Use NSA Type 1 WLAN devices for transmitting classified data</b> .....	37
	<b>WIR0204 SWLAN must have SCAO approval before connecting to SIPRNet</b> .....	38
	<b>WIR0206 Document hardware and key management procedures</b> .....	40
	<b>WIR0220 Use NSA Type 1 encryption for classified WLAN laptops (data-at-rest)</b> .....	40
<b>4.</b>	<b>OTHER WIRELESS NETWORKING SYSTEMS</b> .....	<b>41</b>
4.1	Bluetooth Clients.....	41
	<b>WIR0080 Use FIPS 140-2 encryption with unclassified Bluetooth (data in transit)</b> .....	42
	<b>WIR0182 Do not use Bluetooth devices for classified.</b> .....	43
4.2	Broadband (WiMax) Clients .....	44
	The following checks apply to all wireless client devices (PDAs, laptops, etc.) with WiMax. .....	44
	<b>WIR0040 Use STIG compliant OS configuration on all client devices</b> .....	44
	<b>WIR0050 Configure Antivirus software on all wireless clients</b> .....	45
	<b>WIR0240 Use strong authentication</b> .....	46
	<b>WIR0260 Use FIPS 140-2 encryption for wireless clients (data at rest)</b> .....	47
	<b>WIR0280 Wireless clients connecting via the Internet must be compliant</b> .....	48
	<b>WIR0330 Management access must use compliant password</b> .....	49
	<b>WIR0373 Do not use WWAN systems for classified</b> .....	49
	<b>WIR0374 Do not permit WWAN in a SCIF</b> .....	50
	<b>WIR0378 Authentication and Encryption for WiMax systems</b> .....	50
4.3	Radio Frequency Identification (RFID).....	51
	<b>WIR0495 RFID systems must comply with DoD security requirements</b> .....	51
4.4	Free Space Optic (FSO) Terminal Devices.....	52
	<b>WIR0330 Management access must use compliant password</b> .....	52
	<b>WIR0390 Use encryption for FSO network communications (data in transit)</b> .....	53
	<b>WIR0391 Install FSO bridges in an isolated network</b> .....	53
4.5	Wireless VoIP .....	54
	<b>WIR0133 Wireless VoIP systems must comply with applicable requirements</b> .....	54
4.6	Wireless Keyboards and Mice .....	55
	<b>WIR0131 Infrared keyboards and mice must comply with requirements</b> .....	56
	<b>WIR0132 Wireless keyboards and mice must comply with WLAN requirements</b> .....	57
<b>5.</b>	<b>PDA AND SMARTPHONE COMPLIANCE REQUIREMENTS</b> .....	<b>58</b>
	<b>WIR0012 Display required DoD logon banner on PDA</b> .....	58
	<b>WIR0050 Configure Antivirus software on all wireless clients</b> .....	59
	<b>WIR0280 Wireless clients connecting via the Internet must be compliant</b> .....	60
	<b>WIR0340 Do not discuss classified/sensitive information on unclassified cell phones</b> ....	61
	<b>WIR0371 PDAs/Smartphones with cameras must be approved</b> .....	61
	<b>WIR0372 PDAs and Smartphones with a cameras not allowed in classified areas</b> .....	62
	<b>WIR0380 Use NSA Type-1 end-to-end encryption classified PDAs (data in transit)</b> .....	62
	<b>WIR0410 Do not connect PDAs/Smartphones to classified workstations</b> .....	63
	<b>WIR0420 Do not install PDA synchronization software on classified workstation</b> .....	63
	<b>WIR0425 Encrypt classified data on PDAs (data at rest)</b> .....	64

**WIR0450 Password protect PDA/Smartphone devices.....65**  
**WIR0460 Use FIPS 140-2 encryption to protect unclass data on PDA (data at rest) .....66**  
**WIR0465 Do not download mobile code from non-DoD sources .....66**  
**WIR0470 Disable wireless radios/IR ports on PDAs/Smartphones when not in use .....67**  
**WIR0540 PDAs with text messaging cannot be used for sensitive data .....67**  
**WIR0545 PDA/Smartphone connected to network has managed security policy .....68**  
**APPENDIX A. VMS PROCEDURES.....70**  
**APPENDIX B. SRR WORKSHEETS.....78**

## LIST OF TABLES

	<b>Page</b>
Table 1-1. Sample Interview Questions.....	1
Table 1-2. Wireless Process Matrix.....	2
Table A-1. VMS Asset Matrix.....	73
Table B-1. Network Device SRR Reviewer Worksheet.....	79
Table B-2. Wireless Network Clients: Laptops using WWLAN, WPAN and Cellular 3G NICs Worksheet .....	80
Table B-3. Standalone PDAs, Cellular Telephones, SMS Devices, and Two-Way Pagers .....	81

## TABLE OF FIGURES

Figure 3.1. LAN Extension.....	38
Figure 3.2. Wireless Bridging.....	39
Figure 3.3. Wireless Peer-to-Peer .....	39

## SUMMARY OF CHANGES

### ***GENERAL CHANGES:***

- The previous release was Version 5, Release 2.1, dated 15 November 2007.

### ***SECTION CHANGES***

#### ***SECTION 1. HOW TO PERFORM A WIRELESS REVIEW***

- Minor editorial changes.

#### ***SECTION 2.***

- Section 2. added VMS information
- WIR0010: changed to clarify requirement.
- WIR0225: added note to clarify requirement for classified WLAN systems.
- Minor editorial changes: WIR0016, WIR0076, and WIR0180.
- Moved WIR0011 to this section from section 5.1.

#### ***SECTION 3.***

- Reorganized section: 3.2.1 and 3.2.3 combined with 3.2.
- Minor editorial changes: WIR0050, WIR0100, WIR0125, WIR0160, WIR0180, WIR0190, WIR0203, WIR0204, WIR0206, WIR0230, WIR0240, WIR0275, WIR300, and WIR0330.
- WIR0330: clarified password requirement.
- WIR0168: clarified that requirement is applicable for all wireless client management applications and added reference to MS VISTA
- WIR0204: added new use case.
- WIR0270: clarified what WLAN system components requirement applies to.
- WIR0280: added notes and more detail to the check procedure.
- WIR0161, WIR0163, and WIR168: added information to clarify requirement.
- Deleted WIR0170 and WIR0200. Requirements added to WIR0220.
- Deleted WIR0164. Requirement added to WIR0163.
- Moved note from WIR0140 to WIR0150.

#### ***SECTION 4.***

- Minor changes to WIR0131, WIR0132, WIR0378 and WIR0391.
- WIR0080: updated based on current OSD policy.
- WIR0083: deleted. Requirement included in WIR0080.
- Deleted WIR0392 and WIR0450. Requirements added to WIR0330.
- Deleted WIR0490. Requirements added to WIR0280.
- Deleted WIR0455 and replaced with WIR0260. Checks were duplicative.
- WIR0378: revised to comply with DoD MiMax policy.

#### ***SECTION 5.***

- Moved WIR0011 to section 2.
- Minor changes to: WIR0011, WIR0371, WIR0372, WIR0410, WIR0470, WIR0380, and WIR0420.

- Deleted WIR0370 and WIR0394 and replaced with WIR0225. Checks were duplicative.
- WIR0450: updated requirement based on current policy.
- Merged checks in sections 5.1, 5.1.1 and 5.1.2 into section 5.
- Deleted WIR0350 and replaced with WIR0340. Checks were duplicative.
- Deleted WIR0240 and replaced with WIR0450. Checks were duplicative.
- Deleted WIR0365. Was duplicative to Section 3 checks.
- Deleted WIR0455, WIR0480, and WIR490 replaced with WIR0280. Checks were duplicative.

***APPENDIX A.***

Added note to clarify non-computing VMS asset procedures.

***APPENDIX B.***

No changes.



The page is intentionally blank.

## 1. HOW TO PERFORM A WIRELESS REVIEW

The Wireless Security Checklist has separate sections for each wireless technology. A single reviewer may cover all technologies or they may be divided among several reviewers. The network reviewer, the traditional reviewer, and/or the Windows reviewer should work together to obtain the required information in the checks.

Check procedures for wireless devices will differ for each vendor; therefore screen prints and step-by-step verification procedures are not possible for most policies herein. Where applicable, the reviewer must work with the SA to navigate to the correct configuration screen to view the required settings.

**NOTE:** If the site indicates that wireless email devices are used at the site, the wireless reviewer will perform the Blackberry wireless email checks using the appropriate wireless email system checklist.

Step1. Prior to arrival at the site, the Team Lead should ask the site if any of the following devices are used.

Do you have any of the following devices?	Y/N
Wireless networking device such as access points or bridges	
Laptops used by remote users to connect using a wireless communications card (e.g., from the office or from a hotel or home)	
Desktops or laptops with wireless keyboards and/or mouse	
Personal Digital Assistants (PDAs)	
Two-way pagers	
Wireless telephones	
Personal devices that can be used for Short Message Texting	
Laptops with Bluetooth radio installed	
Wireless VoIP access points or telephone units	
Bridges using FSO terminals for communicating between buildings.	
Desktops or laptops with RFID installed.	
SecNet 11 or other system used for classified processing with a wireless NIC installed.	

**Table 1-1. Sample Interview Questions**

Step 2. Get a list of wireless equipment. Request a copy of the site's wireless equipment inventory and SSAA/SSP. Or use the inventory worksheets located in Appendix C if these documents are not available.

Step 3. Upon arrival at the site, identify a sampling of wireless clients for review. Ask the Team Lead to have the Windows reviewer include a sampling of wireless stations and scan these stations using the Gold Disk.

Step 4. Perform a wireless review if any of the listed devices is used by the site.

Step 5. Interview the site representative to ensure each policy applies to all applicable equipment.

Step 6. Register a non-computing asset using the Wireless Policy using the SSID or other device identifier for PEDs.

Step 7. For VMS entry Use the Gold Disk to register a sampling of the wireless clients. Then add the Wireless Client posture to the asset IAW the matrix in Appendix C.

<b>Type of Review</b>	<b>Purpose</b>	<b>Procedure</b>	<b>Applicable Sections</b>
Wireless SRR	Site reports that wireless devices are used.	Wireless SRR scheduled by DISA FSO. Team lead requests equipment list. Should include wireless discovery.	Wireless Policy and all other applicable sections
Self Assessment	Site performs review	Performed by properly trained site representative. (e.g., may attend DISA FSO Wireless SRR training.	Wireless Policy and all other applicable sections

**Table 1-2. Wireless Process Matrix**

## **2. WIRELESS POLICY – APPLICABLE TO ALL DEVICES**

Perform these checks for all wireless devices (Classified or Unclassified) that are used to process, transmit, store, or connect to DoD information or Enclave resources. Perform these general checks first, and then perform all other applicable subsections depending on hardware and wireless transmission method used.

**For VMS users:** 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).

**WIR0010 All Wireless systems must have DAA approval**

**VMS Vulnerability Key:** V0008283

**Long Name:** The IAO will ensure all wireless systems (including associated peripheral devices, operating system, applications, network/PC connection methods, and services) are approved by the DAA prior to installation and use for processing DoD information.

**Severity:** CAT I

**Checks:** Work with the site POC to verify documentation. Performed with WIR0016 (equipment list).

1. Request copies of written DAA approval documentation.
  - o A signed wireless inventory list, SSAA/SSP, or DAA approval documents as proof of compliance.
  - o DAA approval letter and SSAA may be a general statement of approval rather than list each device.
2. Verify DAA approval for each device used (i.e., wireless connection services, peripherals, and applications).

Mark this check as a finding for any of the following reasons.

- Wireless systems, devices, services, or accessories are in use but DAA approval letter(s) do not exist.
- If in the judgment of the reviewer, configuration differs significantly from that approved by the DAA approval letter.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0011 Personally owned PEDs are used**

**VMS Vulnerability Key:** V0015872

**Long Name:** The IAO will ensure personally owned PEDs are not used to transmit, receive, store, or process DoD information unless approved by the DAA and the owner signs a forfeiture agreement in case of a security incident.

**Severity:** CAT III

**Checks:** Interview the IAO.

1. Ask if users are using personally owned devices such as PDAs, Blackberries, laptops, or home computers to access sensitive Enclave resources. Access to publicly available resources in the DMZ can be accessed via personal devices, depending on the INFOCON level.
2. If personally owned devices are allowed, verify written DAA approval exists and the SSAA is annotated.
3. Verify a **forfeiture agreement** is being used at the site and users are trained to report security incidents on personally owned devices.
4. Mark as a finding if:
  - o CAT I finding if personally owned devices are used for classified access.

**Hint:** This check includes any non-DoD owned or approved devices such as computers, PEDs/PDAs, and wireless NICs. This applies to administrative and end-user access. Use for end-user is discouraged but may be approved by DAA.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0016 Maintain an equipment list of all approved PED devices**

**VMS Vulnerability Key:** V0008284

**Long Name:** The IAO will maintain a list of all DAA approved wireless and non-wireless PED devices that store, process, or transmit DoD information. The list will be stored in a secure location and will include the following at a minimum.

- Access point Media Access Control (MAC) address (WLAN only)
- Access point IP address (WLAN only)
- Wireless client IP address
- Wireless client MAC address
- Wireless channel set for each access point (WLAN only)
- Access point DHCP range (WLAN & WWLAN only)
- Type of encryption enabled
- Encryption key used
- Access point SSID
- Manufacturer, model number, and serial number of wireless equipment
- Equipment location
- Assigned users with telephone numbers

**Severity:** CAT III

**Checks:** Work with the site POC to verify.

1. Request copies of site's wireless equipment list.
  - o SRR worksheets in Appendix B of the Wireless Security Checklist may be used
  - o Detailed SSAA/SSP or database may be used.
2. Verify that all minimum data elements listed in the STIG policy are included in the equipment list.
3. Verify that all WLAN devices used, including infrared mice/keyboards are included.
4. Verify procedures are in place for ensuring that the list is kept updated.
5. Note the date of last update and if the list has many inaccuracies.
6. Mark as a finding if the equipment list does not exist; all data elements are not tracked; or the list is outdated.

**Hint:** This check applies to:

- Wireless networking devices such as access points, bridges and switches
- WLAN client devices (i.e., laptop computers and PDAs if used with WLAN NICs)
- Wireless peripherals such as Bluetooth, and Infrared mice and keyboards
- Communications devices such as VoIP, cellular/satellite telephones, and Broadband NICs
- Non-wireless PEDs that store, process, or transmit DoD information

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0030 Document equipment in the SSP**

**VMS Vulnerability Key:** V0008297

**Long Name:** The IAO will ensure wireless devices connecting directly or indirectly (e.g., hotsync, ActiveSync, wireless) to the network are added to the site System Security Plan (SSP).

**Severity:** CAT III

**Checks:** Review the SSP.

1. Wireless network devices such as access points, laptops, PEDs, and wireless peripherals (keyboards, pointers, etc.) that use a wireless network protocol such as Bluetooth, 802.11, or proprietary protocols must be documented in the SSP.
2. A general statement in the SSP permitting the various types of wireless network devices used by the site is acceptable rather than a by-model listing (e.g., a statement that “wireless devices of various models are permitted but only when configured in accordance with the Wireless STIG or other such specified restriction”).

Mark as a finding if a DAA approved SSP does not exist or if it is not updated.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0072 Wireless network devices must be physically protected**

**VMS Vulnerability Key:** V0014894

**Long Name:** The NSO will ensure all network devices (i.e., Intrusion Detection System (IDS), routers, servers, Remote Access System (RAS), firewalls, WLAN access points, etc.) are located in a secure room with limited access or otherwise secured to prevent tampering or theft.

**Severity:** CAT II

**Checks:** The NSO will ensure all network devices (i.e., Intrusion Detection System (IDS), routers, servers, Remote Access System (RAS), firewalls, WLAN access points, etc) are located in a secure room with limited access or otherwise secured to prevent tampering or theft.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**



## **WIR0076 Require signed user agreement**

**VMS Vulnerability Key:** V0013982

**Long Name:** For mobile and remote users of the DoD enclave and resources, the IAM will develop a written security policy or checklist for secure wireless remote access to the site and an agreement between the site and remote user. These documents will include relevant security requirements, including (but not limited to) the following.

- The agreement will contain the type of access required by the user (privileged, end-user, etc.).
- The agreement will contain the responsibilities, liabilities, and security measures (e.g., malicious code detection training) involved in the use of the wireless remote access device.
- Incident handling and reporting procedures will be identified along with a designated point of contact.
- The remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act.
- The policy will contain general security requirements and practices and are acknowledged and signed by the remote user.
- If classified devices are used for remote access from an alternative work site, the remote user will adhere to DoD policy in regard to facility clearances, protection, storage, distributing, etc.
- Government owned hardware and software is used for official duties only. The employee is the only individual authorized to use this equipment.

DoD CIO Memorandum "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," dated 2 Nov 2007 requires the following additional information in all User Agreements:

### *STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS*

*By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:*

You are accessing a U.S. Government information system (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only.

- You consent to the following conditions:
  - o The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.
  - o At any time, the government may inspect and/or seize data stored on this information system and any device attached to this information system.
  - o Communications occurring on or data stored on this information system, or any device attached to this information system, are not private. They are subject to routine monitoring and search.

- Any communications occurring on or data stored on this information system, or any device attached to this information system, may be disclosed or used for any U.S.

**Severity:** CAT III

**Checks:**

1. Inspect a copy of the site's user agreement.
2. Verify user agreement has the minimum elements described in the STIG policy.
3. User agreements are particularly important for mobile and remote users since there is a high risk of loss, theft, or compromise thus this signed agreement is a good best practice to help ensure the site is making the user is aware of the risks and proper procedures.

Mark as a finding if site user agreements do not exist or are not compliant with the minimum requirements.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0180 Wireless devices allowed into SCIFs must be DCID compliant**

**VMS Vulnerability Key:** V0012072

**Long Name:** The IAO will ensure wireless devices are not permitted in a permanent, temporary, or mobile SCIFs unless approved in accordance with Director Central Intelligence Directive (DCID) 6/9 or 6/3.

**Severity:** CAT II

**Checks:** Work with the traditional reviewer or interview the IAO or SM.

1. Determine if site SCIF security policy/procedures allow users to bring wireless PEDs into SCIFs.
2. If No, determine if procedures are in place to prevent users from bringing PEDs into SCIFs and users are trained on this requirement. Posted signs are also evidence of compliance.
3. If Yes,
  - o Determine if site has written procedures that describe what type of PEDs and under what type of conditions (e.g., turned off, SCIF mode enabled)
  - o If PED devices are allowed, then users should receive proper training on the handling of these devices in a SCIF.
4. Mark this as a finding if:
  - o Required procedures or training policies are not in place or
  - o Required user training has not been documented.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0225 CTTA coordination and proper separation required**

**VMS Vulnerability Key:** V0012106

**Long Name:** The IAO will ensure wireless devices are not operated in areas where classified information is electronically stored, processed, or transmitted unless:

- Approved by the DAA in consultation with the Certified TEMPEST Technical Authority (CTTA).
- The wireless equipment is separated from the classified data equipment the distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.

**Note:** this requirement does not apply to SWLAN SecNet 11/54 equipment.

**Severity:** CAT II

**Checks:** Review documentation. Work with the traditional security reviewer to verify the following.

1. If classified information is not processed at this site, or site has a written procedure prohibiting the use of wireless devices in areas where classified data processing occurs, then mark as not a finding.
2. Ask for documentation showing the CTTA was consulted about operation and placement of wireless devices. Acceptable proof would be coordination signature or initials of the CTTA on the architecture diagram or other evidence of coordination. IAW DoD policy, the CTTA must have a written separation policy for each classified area.
3. Review written policies, training material, or user agreements to see if wireless usage in these areas is addressed.
4. Verify proper procedures for wireless device use in classified areas is addressed in training program.
5. Mark as a finding if any of the following is found.
  - o CTTA has not designated a separation distance in writing
  - o DAA has not coordinated with the CTTA
  - o Users are not trained or made aware (using signage or user agreement) of procedures wireless device usage in and around classified processing areas.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

### 3. WLAN COMPLIANCE REQUIREMENTS

Checks in this section apply to WLAN (IEEE 802.11) systems. These are in addition to the general checks in the Wireless Policy section.

#### 3.1 WLAN Network Devices

Perform these additional checks for both classified and unclassified WLAN (IEEE 802.11) network level devices (i.e., gateways, APs, or bridges).

**Note:** Checks in this section (except when noted in the check) apply to Secure WLAN systems (SecNet 11/54).

For VMS users: Select the Computing asset, Wireless Access Point asset posture.

#### **WIR0070 Obtain US Forces or host nation approval, if applicable**

**VMS Vulnerability Key:** V0014844

**Long Name:** The IAO will ensure WLAN devices installed outside the Continental United States (CONUS) are approved by the local U.S. Forces Command (USFORSCOM) and/or host nation.

**Severity:** CAT III

**Checks:** Review documentation.

1. Verify existence of approval documentation signed by US Forces Command and/or host nation representatives.
2. In accordance with DoD policy, users of non-licensed devices that are intended for use Outside United States & Possessions (OUS&P) must submit appropriate forms for host nation coordination/approval.

Mark as a finding if approval documentation does not exist or is not available for verification.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0075 All DoD sites must perform periodic WLAN discovery**

**VMS Vulnerability Key:** V0014845

**Long Name:** The IAO will ensure the organization periodically screens for unauthorized or rogue access points, stations, and bridges. Local security policy addresses the frequency for which these screenings should occur.

**Note:** Organizations are required to perform scans regardless of whether they have an approved WLAN. Recommend scan be performed quarterly as with the Retina scan.

**Severity:** CAT III

**Checks:** Interview the IAO.

Ask if wireless discovery tests are conducted at least quarterly. By whom? Is a log of tests available?

For classified systems, verify that discovery procedure results are independently certified by an outside organization IAW 8500.2, IA Control ECMT-2) (e.g., periodic SRRs).

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0140 Change default SSID**

**VMS Vulnerability Key:** V0014846

**Long Name:** The IAO will ensure SSIDs are changed from the manufacturer's default to a pseudo random word that does not identify the unit, base, organization, etc. It is recommended that the SSID consist of a combination of upper and lower case characters, numbers, and special characters.

**Severity:** CAT III

**Checks:** Review device configuration.

1. View the SSID using an AP or the security gateway configuration screen
2. Verify the name is not meaningful (e.g., site name, product name, room number, etc).

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0150 Disable SSID broadcast mode**

**VMS Vulnerability Key:** V0014885

**Long Name:** The IAO will ensure the SSID broadcast mode is disabled and WLAN access points that do not allow the SSID broadcast mode to be disabled will not be used.

**Note:** This setting is based on a common industry best practice. SSID information can still be viewed using wireless packet capture tools. However, this policy prevents the attacker from obtaining information about the physical or local placement of the AP and is similar to accepted naming convention practices in place for DoD wired networks.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT II

**Checks:** Review device configuration.

1. View the WLAN configuration for the AP or security gateway.
2. Navigate to the correct AP configuration screen to verify that the setting to **disable SSID broadcast mode** is selected.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0160 Enable MAC address filtering for WLAN**

**VMS Vulnerability Key:** V0003506

**Long Name:** The IAO will ensure that MAC address filtering is enabled at each access point.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Check:** Review device configuration.

1. View the MAC address filter page on one of the WLAN access points or security gateway.
2. Verify that the filter page is configured with a list of allowed and/or disallowed addresses.

**Severity:** CAT III

**Checks:** Review device configuration.

1. View the MAC address filter page on one of the WLAN access points or security gateway.
2. Verify that the filter page is configured with a list of allowed and/or disallowed addresses.

**Hint:** Sites may indicate that this is too difficult to implement with a large or dynamic number of addresses. This is still a finding. These sites may have to upgrade to a security gateway or other equipment with advanced features which allows easier management of a large number of MAC addresses.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**



**WIR0230 WLAN session time out capability set to 15 minutes or less**

**VMS Vulnerability Key:** V0014888

**Long Name:** The IAO will ensure the WLAN provides a session timeout capability and the timeout is set for 15 minutes or less depending on local security policy.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Note:** This policy applies to inactivity timeout for client sessions with the WLAN.

**Severity:** CAT II

**Checks:**

1. Review the configuration screen of the wireless security gateway (e.g., VPN appliance) or other applicable network device.
2. Verify that the session timeout setting is set for 15 minutes or less.
3. Normally, this is not in the access point configuration but is set in the wireless security gateway. (This setting may also be set in the AP but this is not the best method of implementation).
4. Mark as a finding if any of the following is found.
  - Session timeout is not set to 15 minutes or less for the entire WLAN.
  - The WLAN does not have the capability to enable the session time-out feature.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0250 AP transmit power controlled to minimize service to unneeded areas**

**VMS Vulnerability Key:** V0014889

**Long Name:** The IAO will ensure the WLAN access point is set to the lowest possible transmit power setting which meets the required signal strength of the area serviced by the access point.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT II

**Checks:** Review documentation and inspect AP locations

1. Request and review documentation showing signal strength analysis from site survey activities, if available.
2. If available, use testing equipment or WLAN clients to determine if signal strength is, in the reviewer's judgment, excessively outside the required area (e.g., strong signal in the parking area, public areas, or uncontrolled spaces).
3. Lower end APs will not have this setting available—in this case, the site should locate the APs away from exterior walls to achieve compliance with this requirement.
4. Mark as a finding if any of the following is found.
  - Visual inspection of equipment shows obvious improper placement of APs where it will emanate into uncontrolled spaces (e.g., next to external walls, windows, door, uncontrolled area, public areas).
  - Building walk-through testing shows signals of sufficient quality and strength to allow wireless access to exist in areas that are not authorized for WLAN access.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0270 Encryption requirements for unclassified WLAN**

**VMS Vulnerability Key:** V0003515

**Long Name:** The IAO will ensure that the WLAN system meets the following encryption and authentication requirements:

- The encryption modules for data-in-transit of the WLAN equipment are validated as meeting FIPS 140-2 overall Level 1 validated (at a minimum) and the information assurance component of the WLAN system is NIAP Common Criteria validated for basic or medium robustness (as determined by the DAA).
  - o This requirement applies to any component of the WLAN system that does encryption (access point, client, security gateway).
- If the WLAN infrastructure device (access point, bridge, wireless switch or gateway) is used in an unprotected public area, the encryption module of the device is validated as meeting FIPS 140-2 Level 2, at a minimum.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT II

**Checks:**

- Interview IAO and review documentation.
- Obtain the product's FIPS certificate and NIAP validation documentation or vendor documentation from the IAO or the vendor. Use this documentation to verify compliance with the policy requirements for robustness levels, NIAP, and FIPS.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0275 WLAN network and client device NICs are both Wi-Fi and WPA2 certified**  
**VMS Vulnerability Key:** V0014004

**Long Name:** The IAO will ensure that for all new WLAN acquisitions, the WLAN-enabled devices (e.g., NICs and access points) that store, process, or transmit unclassified information are Wi-Fi Alliance certified and WPA2 Enterprise certified.

- The Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP) will be implemented in the WLAN system encryption modules.
- The EAP component of WPA2 will implement EAP-TLS mutual authentication. (This requirement is not applicable to connections between WLAN bridges.)
- Mitigation plans for legacy WLAN systems that do not meet these requirements must be reported to the DoD CIO by Dec 29, 2006.

**Note:** Wi-Fi (ensures interoperability and standardization across products). WPA2 (security standardization across products).

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT III

**Checks:** Review documentation.

- Verify that WLAN client NICs and access points are Wi-Fi and WPA2 certified. Certification sticker on devices or packaging is acceptable. The manufacturer's documentation or web site (exact model only) is also acceptable.
- Mark as a finding if products were procured in or after FY2007 and are not **both** Wi-Fi and WPA2 certified.

**Note:** All WLAN equipment purchased after March 2006 that is WiFi certified is also WPA2 compliant.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

## **WIR0290 Install WLAN network devices in an isolated network**

**VMS Vulnerability Key:** V0014886

**Long Name:** The IAO will ensure wireless access points and bridges are placed in a screened subnet (Demilitarized Zone (DMZ) on firewall separating intranet and wireless network) or Virtual LAN (VLAN) or otherwise separated from the wired internal network by using a wireless Virtual Private Network (VPN) concentrator or wireless gateway/firewall/switch placed between the access point and the local DoD network.

**Note:** Sites must also comply with the Network Infrastructure STIG configuration requirements for DMZ, VLAN, and VPN configurations as applicable

**Severity:** CAT II

**Checks:** Review network architecture with the network administrator.

1. Verify compliance by inspecting the site network topology diagrams and the firewall interface configurations.
2. Since many network diagrams are not kept up-to-date, walk through the connections with the network administrator to verify the diagrams are current.

Mark as a finding if the wireless network device does not use an approved network isolation method (e.g., DMZ, VLAN, or VPN, WLAN concentrator).

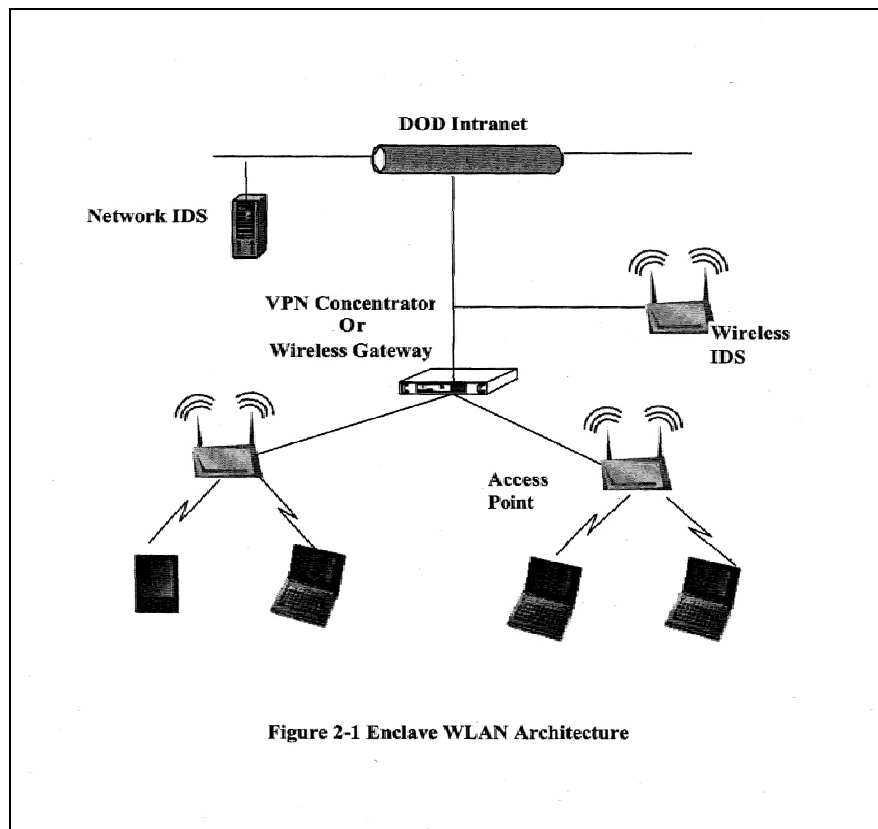


Figure 2-1. DoD Intranet

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0300 Use wireless IDS to monitor unauthorized WLANs on DoD networks**

**VMS Vulnerability Key:** V0014887

**Long Name:** The IAO will ensure that the wired and wireless network will be monitored by a wireless IDS. The system will have the following capabilities:

- Continuous-scanning. The WIDS will scan continuously 24 hours/day, 7 days/week to detect authorized and unauthorized activity.
- Location-sensing WIDS. The WIDS will include a location sensing protection scheme for authorized and unauthorized wireless devices.
- The WIDS are validated under the NIAP Common Criteria, as meeting U.S. Government protection profiles for basic or medium robustness environments, as determined by the DAA.

**Note:** Sites must also comply with the Network Infrastructure STIG configuration requirements for IDS

**Severity:** CAT II

**Checks:** Interview network administrator and review network architecture

1. Inspect the site network topology and dataflow diagrams. Verify use of a WIDS to monitor both wired and wireless LANs by checking the positioning in the architecture and interviewing the administrator.
2. Ask what the DAA has determined as the robustness level of the system and verify that the WIDS is validated at this level of the NIAP CC.
3. Have IAO provide wireless IDS product specification or data sheets showing required features/certifications.
4. The wired and wireless IDS may be one IDS management device with wireless sensors.
5. Mark as a finding if a WIDS is:
  - o Not installed or used to protect both the wired and wireless networks,
  - o Not configured for continuous-scanning and location-sensing, or
  - o The product does not meet or exceed the robustness level of as determined by the DAA.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0330 Management access must use compliant password**

**VMS Vulnerability Key:** V0014890

**Long Name:** The IAO will ensure wireless network device management interfaces and management consoles are password protected and the password is compliant with DoD password policies. Password length and complexity will be in accordance with requirements of current DoD policies and INFOCON level.

**Severity:** CAT I

**Checks:** Inspect the network diagram and device configuration. Network level wireless devices such as access points, bridges, VoIP, WLAN controllers, WLAN management/authentication servers, and security gateways must have password and access control IAW DoD policy. Management password compliance.

- Ask the IAO if the password requirements associated with different INFOCON levels are followed.
- Ask if passwords are created and maintained IAW requirements of DoDI 8500.2, IAIA-1, and IAIA-2. <http://www.dtic.mil/whs/directives/corres/html/850002p.htm>
  - Passwords are, at a minimum, a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each.
  - At least four characters must be changed when a new password is created.
- Are passwords for these devices recorded and stored in accordance with local procedures for wired network devices.
- Record the devices that have this finding in the comments area by serial and model number.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**



### 3.2 WLAN Clients – General Requirements

Perform these additional checks for classified or unclassified clients using WLAN NICs to connect to DoD resources directly or remotely.

**Note:** Checks in this section (except when noted in the check) apply to Secure WLAN systems (SecNet 11/54).

For VMS users: Select the Computing asset, Wireless Client asset posture.

#### **WIR0040 Use STIG compliant OS configuration on all client devices**

**VMS Vulnerability Key:** V0014274

**Long Name:** The IAO will ensure all wireless devices are configured according to applicable operating system STIGs.

**Severity:** CAT II

**Checks:** Review procedures and verify compliance.

1. Verify existence of applicable operating system SRR, Gold Disk review, and/or self assessment results.
2. If some type of compliance report has not been performed, work with the Team Lead and Windows reviewer to run the Gold Disk or SRR scripts on a 10% representative sample of the wireless laptops.
3. Mark this as a finding if:
  - The site has not regularly performed a Gold Disk/self assessment **or**
  - The Windows reviewer determines that the laptop is not STIG-compliant.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0050 Configure Antivirus software on all wireless clients**

**VMS Vulnerability Key:** V0014275

**Long Name:** The IAO will ensure DoD licensed anti-virus software is installed on all wireless clients (e.g., laptops, PDAs, and smartphones) and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signatures every 14 days or less.

**Severity:** CAT I

**Check:** Verify that laptop computers, PDAs, and smartphones are protected by anti-virus software.

1. For laptops, work with the Team Lead and Windows reviewer to run the Gold Disk or SRR scripts on a 10% representative sample of the clients.
2. For PDAs and cell phones, inspect a 10% sampling of the devices. Verify the software is:
  - o Configured to scan upon startup (once daily) or the user trained to scan at least once per week.
  - o Configured to automatically update at least every 14 days or the user trained to manually update once every two weeks.
  - o Enabled for Web browser download protection.
  - o If DoD approved antivirus products (e.g. downloaded from the JTF GNO antivirus portal) are not available for the wireless device, sites must select commercial products which are from major vendors with preference given to products tested or already used by other DoD organizations.
  - o The DAA must give written approval of this product.
3. Mark as a finding if any of the following are true:
  - o The Gold Disk results indicate this is a finding.
  - o No antivirus software is installed; update procedures are not configured or used; or the software is not configured IAW the Wireless STIG policy.
  - o If the software used on a laptop but is not DoD approved, then mark as a **CAT III** finding.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0100 Use an approved and properly configured personal firewall**

**VMS Vulnerability Key:** V0003501

**Long Name:** The IAO will ensure a personal firewall is implemented on each 802.11-enabled wireless device to block unauthorized access to the device and the software is configured in accordance with the *Desktop Application STIG*. Personal firewall software is NIAP Common Criteria validated as meeting U.S. Government protection profiles.

**Severity:** CAT III

**Checks:** Inspect a 10% representative sampling of laptops, PDAs, and smartphones **used for WLAN access**.

1. For laptops with WLAN access use one of the following verification methods.
  - Work with the Team Lead and Windows reviewer to run the Gold Disk or SRR scripts on a 10% representative sample of the clients.
  - **Or** review the results of the Desktop Application from previous SRR or site's self-assessment
2. For PDAs and smartphones with WLAN access, manually inspect a 10% sampling of devices. Verify the software is:
  - Able to block both inbound and outbound ports and services as needed
  - Configured for automatic updates from trusted site every 14 days (if this feature is available) or the user has been trained to manually download updates every 14 days (check user agreement or training records).
  - Configured to block known DDoS ports and unneeded services as identified by the local SA.
  - NIAP validated.
  - If NIAP approved software is not available for this OS, sites must select commercial products which are from major vendors with preference given to products tested or already used by other DoD organizations.
  - The DAA must give written approval of this product.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0125 Enable mutual authentication for peer-to-peer (ad hoc) WLANs**

**VMS Vulnerability Key:** V0004628

**Long Name:** If the DAA has approved the use of peer-to-peer WLAN networking, the IAO will ensure strong mutual authentication and FIPS 140-2 encryption between each station on the peer-to-peer network occurs before data is transmitted between stations. IEEE 802.1x authentication with EAP-TLS and AES-CCMP is required.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT II

**Checks:** Review the configuration of the WLAN NIC using WZC or the NIC management utility (depending on which is used to manage the card configuration by the site).

1. See if peer-to-peer connections are permitted by site policy.
2. Client devices that permit peer-to-peer communications should require authentication before a wireless connection can be established (e.g., the setting may say **require mutual authentication** or try connecting to a peer to see if authentication is requested).
3. Peer-to-peer configurations are not encouraged as they by-pass the network security infrastructure, but they are not disallowed when configured correctly using sound best practices, including use of products with FIPS 140-2 encryption modules. Most DoD sites prohibit peer-to-peer networking but may not know the setting is incorrect.
4. Mark as a finding if both of the following are true:
  - o The DAA has not approved peer-to-peer networking and wireless clients are found that are configured to allow peer-to-peer connections (client WLAN communication is not limited to infrastructure mode only).
  - o The DAA has approved peer-to-peer networking but wireless client is not using IEEE 802.1x authentication with EAP-TLS or FIPS 140-2 encryption with AES-CCMP prior to permitting access by another client.

Interview the IAO and check vendor documentation or wireless system management configuration screens.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0130 WLAN is used; do not use NICs that cannot disable peer-to-peer**

**VMS Vulnerability Key:** V0003503

**Long Name:** The IAO will ensure WLAN Network Interface Cards (NICs) that do not have the capability to turn off or otherwise disable peer-to-peer WLAN communications are not used.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT II

**Checks:** Review device configuration.

1. Check each model of NIC to determine if peer-to-peer communications can be disabled in the management software.
2. Alternatively, the SA may provide a copy of documentation showing that this feature is available in all NICs authorized for use.
3. This feature does not have to be disabled; the check verifies that the client has the capability to turn off the wireless NIC.
4. On some WLAN client devices are disabled by selecting “Infrastructure mode only” or “Connect to access point only”.
5. Mark this as a finding if:

The WLAN NIC the management utility used does not have an option to prevent the client from establishing ad-hoc or peer-to-peer connections (e.g., the setting may be labeled **network infrastructure mode only** or **connect only to access points**—depending on the vendor).

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0161 Wired and wireless NICs are not active simultaneously**

**VMS Vulnerability Key:** V0014002

**Long Name:** The IAO will ensure computer/PED wired network interfaces (e.g., Ethernet) are disconnected or otherwise disabled when wireless network connections are being used.

**Severity:** CAT II

**Checks:** Review client devices and verify that there is some technical procedure to disable the wireless NIC when the wired NIC is active (i.e. connected to a network via an Ethernet cable).

**Note:** Examples of compliant implementations:

- The Juniper Odyssey Access Management client and Air Defense Personal have a configuration settings that disables wireless connections when a wired connection is active.
- Set up a Windows hardware profile that with disable a hardware device when the Ethernet NIC is active and assign the wireless NIC to this profile.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0163 Disable WZC service on Windows clients**

**VMS Vulnerability Key:** V0004629

**Long Name:** The IAO will ensure the Windows Zero Configuration (WZC) service is disabled in any Windows computer that is used on a WLAN. This setting should be verified whenever new software or operating system updates are installed on the computer.

**Note:** a FIPS 140-2 certified Wireless LAN client should be used to manage the wireless NIC. WZC is not FIPS 140-2 certified.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT III

**Checks:** Apply to all WLAN laptops with Windows installed. Use the following procedures to verify that WZC is disabled.

- Right click Start, then Control Panel, then Performance and Maintenance, then Administrative Tools, and then double click Services.
- Double click on the Wireless Zero Configuration icon.
- Select the General tab.
- Under Startup Type check to see that startup type is set to Disabled.
- Under Service Status, check to see that the status is set to Stopped.
- Click OK and close the Services screen.

Mark as a finding if WZC is enabled on Windows wireless computer.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0167 Change default setting for WLAN NIC radio to “Off”**

**VMS Vulnerability Key:** V0004632

**Long Name:** The IAO will ensure that laptops with WLAN cards will have the WLAN card radio set to OFF as the default setting.

**Severity:** CAT III

**Checks:** Have the IAO demonstrate the configuration of the WLAN card in the NIC management utility.

1. Observe that the card is set to off by default upon startup of the operating system.
2. Verify this is standard practice by sample checking 10% of laptops. Laptops can be checked by verifying the status of the wireless NIC upon boot-up in each profile used on the laptop.
3. The user should be able to enable and disable the NIC in accordance with site policy.
4. Mark as a finding if either of the following is found:
  - o The WLAN NIC radio functionality (transmit/receive setting) is enabled upon system boot.
  - o Mark this as a finding if the WLAN NIC management utility does not provide the ability to set the radio to OFF by default.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0168 For wireless client, do not set preferred network to auto-connect**

**VMS Vulnerability Key:** V0007072

**Long Name:** The IAO will ensure that the wireless client management application (e.g. Odyssey Access Manager, Cisco wireless client, etc.) on a wireless client computer, the “Preferred Network” connection is configured such that the “Connect when this network is in range” selection is disabled on the Connection tab. The requirement is the following:

- The wireless client manager does not automatically connect to non-preferred networks.
- The wireless client manager does not automatically connect to preferred networks.

**Severity:** CAT III

**Checks:** Review the configuration settings of the client and make sure the client is not configured so that:

- The wireless client manager does not automatically connect to non-preferred networks.
- The wireless client manager does not automatically connect to preferred networks.

Mark as a finding if any of these conditions are found.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**



**WIR0240 Use strong authentication**

**VMS Vulnerability Key:** V0003692

**Long Name:** The IAO will ensure the wireless system uses strong authentication for identification and authentication of the user or WLAN client. IEEE 802.1x authentication with EAP-TLS is required for WLAN systems.

**Note:** This requirement is referring to user/device authentication prior to the establishment of the wireless link by the wireless system, not authentication to the DoD network. When the wireless system authentication is tied into the DoD network authentication system (interfaces with AD/NT logon) and supports CAC authentication, the user may authenticate to the wireless system and the DoD network simultaneously (e.g., enter CAC PIN only once).

**Note:** SecNet 11 and SecNet 54 perform strong mutual authentication independent of any user action. This check is N/A for these devices.

**Severity:** CAT II

**Checks:** Work with the IAO and NSO.

Verify IEEE 802.1x authentication with EAP-TLS has been implemented on the wireless LAN system. Interview the IAO and check vendor documentation or wireless system management configuration screens.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0260 Use FIPS 140-2 encryption for wireless clients (data at rest)**

**VMS Vulnerability Key:** V0014202

**Long Name:** The IAO will ensure all sensitive data (e.g., For Official Use Only (FOUO), Privacy Act information) stored on wireless clients (i.e., laptops, PDAs) are encrypted using either encryption of the file system or individual files. The encryption system is FIPS 140-2 overall Level 1 or 2 validated (as directed by the DAA based on the sensitivity of the data).

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT II

**Checks:** Interview IAO and review documentation.

1. Obtain the product's FIPS certificate or vendor documentation from the IAO or the vendor. Use this documentation to verify compliance with the policy requirement for FIPS, Level 1 or 2 as directed by the DAA.
2. Work with the IAO to determine if encryption is enabled on the client and configured to use AES or 3DES on wireless client devices.
3. Verify that temp files with sensitive information are also protected with encryption.

Mark as a finding if encryption is not used or is not FIPS 140-2 certified at the Level required.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0275 WLAN network and client device NICs are both Wi-Fi and WPA2 certified**  
**VMS Vulnerability Key:** V0014004

**Long Name:** The IAO will ensure that for all new WLAN acquisitions, the WLAN-enabled devices (e.g., NICs and access points) that store, process, or transmit unclassified information are Wi-Fi Alliance certified and WPA2 Enterprise certified.

- The Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP) will be implemented in the WLAN system encryption modules.
- The EAP component of WPA2 will implement EAP-TLS mutual authentication. (This requirement is not applicable to connections between WLAN bridges.)
- Mitigation plans for legacy WLAN systems that do not meet these requirements must be reported to the DoD CIO by Dec 29, 2006.

**Note:** Wi-Fi (ensures interoperability and standardization across products). WPA2 (security standardization across products).

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT III

**Checks:** Review documentation.

- Verify that WLAN client NICs and access points are Wi-Fi and WPA2 certified. Certification sticker on devices or packaging is acceptable. The manufacturer's documentation or web site (exact model only) is also acceptable.
- Mark as a finding if products were procured in or after FY2007 and are not **both** Wi-Fi and WPA2 certified.

**Note:** All WLAN equipment purchased after March 2006 that is WiFi certified is also WPA2 compliant.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0280 Wireless clients connecting via the Internet must be compliant**

**VMS Vulnerability Key:** V0003516

**Long Name:** The IAO will ensure if a wireless device is to be used to access a DoD network via the Internet through a public wireless Internet gateway (e.g., airport or hotel “hotspot”), the following requirements are met:

- The requirements in the Secure Remote Computing STIG are followed.
- The wireless client device has an approved personal firewall, antivirus, and VPN client installed and is operational with the latest updates installed before the wireless connection is enabled.
- After connecting to the hotel wireless portal, users will be trained to immediately connect to the DoD network via the VPN client. All connections for Government official business to the Internet via the hotel wireless network will be through the DoD VPN connection only.
- Users are trained to turn-off wireless cards immediately after a VPN connection is disconnected.

**Note:** OSD NII (wireless) has determined that connecting to a public hot spot today, if allowed by DoD Component level policy, is permitted per DoDD 8100.2. Minimum requirements: FIPS 140-2 validated data-in-transit, FIPS 140-2 validated data-at-rest, anti-virus, and strong authentication. OSD NII is currently developing a DoD Remote Access policy that will place restrictions on the use of public WLAN systems by DoD wireless users.

**Note:** DISA FSO and NSA recommend that DoD WLAN users do not connect to public WLAN systems (public hot spots and hotel WLAN systems). It is impossible, using currently available security tools, to provide 100% assurance that a user is connecting to a legitimate public hotspot or hotel WLAN access point rather than a hacker controlled access point or to stop a hacker from exploiting a WLAN laptop after a user connects to a hacker controlled hotspot.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT II

**Checks:** Interview the IAO. This check refers to remote access to DoD non-publicly available resources.

Ask the IAO if devices with WLAN NICs are permitted to connect to the DoD network remotely using a public Internet connection. If so, perform the following.

- Verify that the site has applied the Secure Remote Computing STIG by asking for evidence (e.g., Desktop/Network Infrastructure checklists or demonstration of a setting) and users have been trained on how to connect securely to a public WLAN system.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

### 3.3 Classified WLANs

Perform checks in this section for WLANs processing classified information and/or connecting to the SIPRNet. Also perform checks for networking and/or client that are applicable to the device being reviewed.

Currently, the only devices approved for classified WLAN communications are the Harris Corporation SecNet 11 and 54 that include an AP and a removable PCMCIA NIC. The SecNet 54 is approved to transmit classified information up to Top Secret and the SecNet 11 is approved to transmit classified information up to Secret.

**Note:** Checks in section 3.1 and 3.2 (except when noted in the check) also apply to Secure WLAN systems (SecNet 11/54).

VMS users only: Register a workstation asset using the Gold Disk. Add “Wireless Client” and, if applicable, SecNet 11 to the asset posture.

#### **WIR0190 Do not use embedded NICs for classified**

**VMS Vulnerability Key:** V0003509

**Long Name:** The IAO will ensure computers with embedded WLAN systems that cannot be removed by the user are not used to transfer, receive, store, or process classified information.

**Severity:** CAT II

**Checks:** Interview the IAO and inspect the WLAN client.

1. Ask if there are laptops, which are used to process classified information and have embedded wireless NICs.
2. The NIC should be physically removed. Use of methods such as tape or software disabling is not acceptable.

If this is a finding, recommend to the DAA that this is a critical finding requiring immediate action.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0203 Use NSA Type 1 WLAN devices for transmitting classified data**

**VMS Vulnerability Key:** V0015300

**Long Name:** The IAO will ensure that only NSA Type 1 certified WLAN systems are used for wireless transmission of classified information.

**Severity:** CAT I

**Checks:** Visually verify that Harris Corporation SecNet 11 or SecNet 54 products are used for classified WLANs.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

## **WIR0204 SWLAN must have SCAO approval before connecting to SIPRNet**

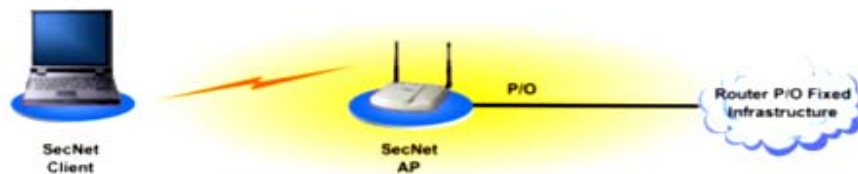
**VMS Vulnerability Key:** V0004636

**Long Name:** The IAO will ensure before a Secure WLAN (SWLAN) becomes operational and is connected to the SIPRNet the following occurs.

- The SWLAN conforms to the SWLAN CONOPS as follows:
  - o The SWLAN architecture conforms to one of the approved Scenarios / Use Cases (see below).
  - o SWLAN equipment is physically or electronically inventoried daily by serial number or MAC address. APs not stored in a COMSEC-approved security container must be physically inventoried.
  - o MAC filtering at the AP will be implemented. The MAC address of all approved wireless cards will be entered stored on each AP.
  - o SWLAN system will be rekeyed according to the following schedule:
    - Seaborne: Every 30 days at a minimum
    - Fixed Site: Every 90 days at a minimum
    - Airborne: Every 90 days at a minimum
    - Air Force Special Operations: Every 90 days at a minimum
    - Deployed Forces in Tactical: Every 90 days at a minimum
- The site SSAA has been approved by the DAA and includes the SWLAN system.
- A SIPRNet connection approval package on file with the SIPRNet Connection Approval Office (SCAO) has been updated to include the SWLAN system.
- Operational use/configuration of the SWLAN system is adjusted based on guidance issued by the SCAO.

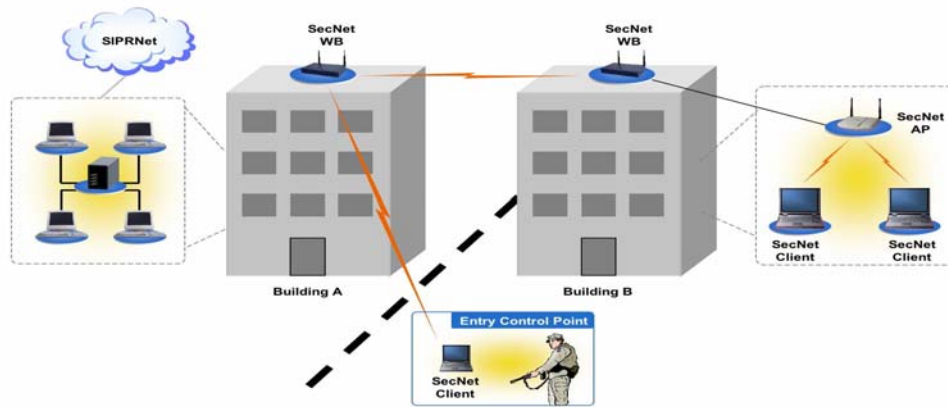
### **Approved SWLAN Use Cases**

**LAN Extension:** This architecture provides wireless access to the wired infrastructure using a Harris SecNet 11 or 54. In this architecture, the boundary is controlled either with fencing or inspection.



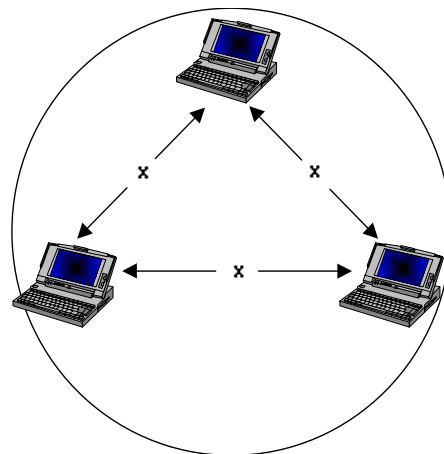
**Figure 3.1. LAN Extension**

**Wireless Bridging:** This architecture provides point-to-point bridging using Harris SecNet 11 or 54. In this architecture, the boundary is controlled either with fencing or inspection.



**Figure 3.2. Wireless Bridging**

**Wireless Peer-to-Peer:** This architecture provides point-to-point communications between wireless clients using Harris SecNet 11 or 54. In this architecture, the boundary is controlled either with fencing or inspection.



**Figure 3.3. Wireless Peer-to-Peer**

**Severity:** CAT I

**Checks:** Review documentation.

1. Inspect system architecture and SCAO approval documentation exists and has been approved.
2. Have IA/O show all requirements in checklist have been met.

Verify system has a SIPRNet or NIPRNet Interim Approval to Operate (IATO) or Approval to Operate (ATO) in GIAP database.



**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0206 Document hardware and key management procedures**

**VMS Vulnerability Key:** V0007075

**Long Name:** The IAO will ensure written operating procedures or policies exists describing procedures for the protection, handling, accounting, and use of NSA Type-1 certified WLAN hardware and key material in a SWLAN operational environment.

**Severity:** CAT III

**Checks:** Interview the IAO.

1. Verify that written operating procedures exist.
2. Procedures must describe methods for protecting, handling, accounting, and using NSA Type-1 certified WLAN hardware and key material in the SWLAN operational environment.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0220 Use NSA Type 1 encryption for classified WLAN laptops (data-at-rest)**

**VMS Vulnerability Key:** V0003512

**Long Name:** The IAO will ensure tools are used to encrypt classified data at rest on the wireless device used on a classified WLAN. Encryption tools must be NSA Type-1 certified.

**Severity:** CAT II

**Checks:** Work with the SA.

1. Verify use of file system encryption by inspecting the WLAN client configuration.
2. Note the software or technique used for encryption in the Comments and, if applicable, request documentation showing that it is NSA and DAA approved.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

## 4. OTHER WIRELESS NETWORKING SYSTEMS

The following are wireless connections technologies. Perform only when used by the site. Also perform the checks in the Wireless Policy Section.

### 4.1 Bluetooth Clients

The following checks apply to all wireless clients (PDA, laptops, and desktops) with Bluetooth.

**Note:** Bluetooth security requirements for BlackBerry and Windows Mobile wireless email devices are found in the BlackBerry Checklist and appropriate Windows Mobile email system checklist (Apriva Sensa, Windows Mobile Messaging, and Good Mobile Messaging).

With Bluetooth, each device acts like an access point, and is therefore an entry point into the local area network. Bluetooth devices are often embedded into laptops, PEDs, headsets, and other wireless peripherals used with wired/wireless network access devices. These often overlooked connections are an attractive target for attackers. Using very inexpensive sniffers, a hacker can eavesdrop on a Bluetooth communication session. Combined with Bluetooth PIN-hacking tools (e.g., BTCrack), an attacker could potentially control Bluetooth devices or access encrypted data (if a non-DoD compliant encryption module is used).

VMS users only: Register a PED (laptop, PDA, etc.) or workstation computing asset as appropriate. Add “Wireless Client”, Operating System, and any installed applications to the asset posture. This procedure will accommodate situations where Bluetooth devices are found but there is no WLAN.

**WIR0080 Use FIPS 140-2 encryption with unclassified Bluetooth (data in transit)**

**VMS Vulnerability Key:** V0003499

**Long Name:** The IAO will ensure Bluetooth devices are not used to store, process, or transmit DoD information, unless FIPS 140-2 validated cryptographic modules are used to encrypt the data during transmission.

**Note:** OASD NII (Wireless) has approved a limited exception to the requirement above: Bluetooth headsets under the following conditions do not have to use FIPS 140-2 certified encryption:

- The Bluetooth headset is used for voice only (no data).
- The design and implementation conforms to the DISA Bluetooth Headset Security Requirements Matrix found at <http://iase.disa.mil/stigs/checklist/index.html>.

**Severity:** CAT II

**Checks:**

- Verify that a written policy or training materials exists stating that Bluetooth will be disabled on all applicable devices unless compliant with this requirement.
- If Bluetooth is being used, verify it is using FIPS 140-2 encryption (except as noted in policy statement).
- Verify the site has a policy to ensure products with Bluetooth are not purchased unless compliant with this requirement.
- Check configuration of a sampling of the wireless or mobile devices (PEDs).

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0182 Do not use Bluetooth devices for classified.**

**VMS Vulnerability Key:** V0004634

**Long Name:** The IAO will ensure that Bluetooth devices are not used to send, receive, store, or process classified messages.

**Severity:** CAT I

**Checks:** Verify compliance by reviewing the user agreement or security briefing to see if personnel have been properly instructed in the policy that devices with Bluetooth radios cannot be used for or around classified.

**Note:** This check does not apply to wireless email devices (BlackBerry, Windows Mobile, etc.). See the appropriate wireless email device checklist for Bluetooth requirements for these devices.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

## 4.2 Broadband (WiMax) Clients

The following checks apply to all wireless client devices (PDAs, laptops, etc.) with WiMax.

**Note:** If the site indicates that BlackBerry wireless email devices are used at the site, the wireless reviewer will perform the Blackberry wireless email checks using the *Wireless STIG, BlackBerry Checklist*.

**Note:** These checks also apply to cellular broadband systems (i.e. cellular aircards).

VMS users only: Register a Computing Asset, as appropriate (laptop, PED/PDA). Add “Wireless Client”, Operating System, and any installed applications to the asset posture. This procedure will accommodate situations where Bluetooth devices are found but there is no WLAN.

### **WIR0040 Use STIG compliant OS configuration on all client devices**

**VMS Vulnerability Key:** V0014274

**Long Name:** The IAO will ensure all wireless devices are configured according to applicable operating system STIGs.

**Severity:** CAT II

**Checks:** Review procedures and verify compliance.

1. Verify existence of applicable operating system SRR, Gold Disk review, and/or self assessment results.
2. If some type of compliance report has not been performed, work with the Team Lead and Windows reviewer to run the Gold Disk or SRR scripts on a 10% representative sample of the wireless laptops.
3. Mark this as a finding if:
  - o The site has not regularly performed a Gold Disk/self assessment **or**
  - o The Windows reviewer determines that the laptop is not STIG-compliant.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0050 Configure Antivirus software on all wireless clients**

**VMS Vulnerability Key:** V0014275

**Long Name:** The IAO will ensure DoD licensed anti-virus software is installed on all wireless clients (e.g., laptops, PDAs, and smartphones) and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signatures every 14 days or less.

**Severity:** CAT I

**Check:** Verify that laptop computers, PDAs, and smartphones are protected by anti-virus software.

1. For laptops, work with the Team Lead and Windows reviewer to run the Gold Disk or SRR scripts on a 10% representative sample of the clients.
2. For PDAs and cell phones, inspect a 10% sampling of the devices. Verify the software is:
  - o Configured to scan upon startup (once daily) or the user trained to scan at least once per week.
  - o Configured to automatically update at least every 14 days or the user trained to manually update once every two weeks.
  - o Enabled for Web browser download protection.
  - o If DoD approved antivirus products (e.g. downloaded from the JTF GNO antivirus portal) are not available for the wireless device, sites must select commercial products which are from major vendors with preference given to products tested or already used by other DoD organizations.
  - o The DAA must give written approval of this product.
3. Mark as a finding if any of the following are true:
  - o The Gold Disk results indicate this is a finding.
  - o No antivirus software is installed; update procedures are not configured or used; or the software is not configured IAW the Wireless STIG policy.
  - o If the software used on a laptop but is not DoD approved, then mark as a **CAT III** finding.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0240 Use strong authentication**

**VMS Vulnerability Key:** V0003692

**Long Name:** The IAO will ensure the wireless system uses strong authentication for identification and authentication of the user or WLAN client. IEEE 802.1x authentication with EAP-TLS is required for WLAN systems.

**Note:** This requirement is referring to user/device authentication prior to the establishment of the wireless link by the wireless system, not authentication to the DoD network. When the wireless system authentication is tied into the DoD network authentication system (interfaces with AD/NT logon) and supports CAC authentication, the user may authenticate to the wireless system and the DoD network simultaneously (e.g., enter CAC PIN only once).

**Note:** SecNet 11 and SecNet 54 perform strong mutual authentication independent of any user action. This check is N/A for these devices.

**Severity:** CAT II

**Checks:** Work with the IAO and NSO.

Verify IEEE 802.1x authentication with EAP-TLS has been implemented on the wireless LAN system. Interview the IAO and check vendor documentation or wireless system management configuration screens.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0260 Use FIPS 140-2 encryption for wireless clients (data at rest)**

**VMS Vulnerability Key:** V0014202

**Long Name:** The IAO will ensure all sensitive data (e.g., For Official Use Only (FOUO), Privacy Act information) stored on wireless clients (i.e., laptops, PDAs) are encrypted using either encryption of the file system or individual files. The encryption system is FIPS 140-2 overall Level 1 or 2 validated (as directed by the DAA based on the sensitivity of the data).

**Severity:** CAT II

**Checks:** Interview IAO and review documentation.

- Obtain the product’s FIPS certificate or vendor documentation from the IAO or the vendor. Use this documentation to verify compliance with the policy requirement for FIPS, Level 1 or 2 as directed by the DAA.
- Work with the IAO to determine if encryption is enabled on the client and configured to use AES or 3DES on wireless client devices.
- Verify that temp files with sensitive information are also protected with encryption.

Mark as a finding if encryption is not used or is not FIPS 140-2 certified at the Level required.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**



**WIR0280 Wireless clients connecting via the Internet must be compliant**

**VMS Vulnerability Key:** V0003516

**Long Name:** The IAO will ensure if a wireless device is to be used to access a DoD network via the Internet through a public wireless Internet gateway (e.g., airport or hotel “hotspot”), the following requirements are met:

- The requirements in the Secure Remote Computing STIG are followed.
- The wireless client device has an approved personal firewall, antivirus, and VPN client installed and is operational with the latest updates installed before the wireless connection is enabled.
- After connecting to the hotel wireless portal, users will be trained to immediately connect to the DoD network via the VPN client. All connections for Government official business to the Internet via the hotel wireless network will be through the DoD VPN connection only.
- Users are trained to turn-off wireless cards immediately after a VPN connection is disconnected.

**Note:** OSD NII (wireless) has determined that connecting to a public hot spot today, if allowed by DoD Component level policy, is permitted per DoDD 8100.2. Minimum requirements: FIPS 140-2 validated data-in-transit, FIPS 140-2 validated data-at-rest, anti-virus, and strong authentication. OSD NII is currently developing a DoD Remote Access policy that will place restrictions on the use of public WLAN systems by DoD wireless users.

**Note:** DISA FSO and NSA recommend that DoD WLAN users do not connect to public WLAN systems (public hot spots and hotel WLAN systems). It is impossible, using currently available security tools, to provide 100% assurance that a user is connecting to a legitimate public hotspot or hotel WLAN access point rather than a hacker controlled access point or to stop a hacker from exploiting a WLAN laptop after a user connects to a hacker controlled hotspot.

**Note:** This check does not apply to secure WLAN systems (SecNet 11/54).

**Severity:** CAT II

**Checks:** Interview the IAO. This check refers to remote access to DoD non-publicly available resources.

Ask the IAO if devices with WLAN NICs are permitted to connect to the DoD network remotely using a public Internet connection. If so, perform the following.

- Verify that the site has applied the Secure Remote Computing STIG by asking for evidence (e.g., Desktop/Network Infrastructure checklists or demonstration of a setting) and users have been trained on how to connect securely to a public WLAN system.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0330 Management access must use compliant password**

**VMS Vulnerability Key:** V0014890

**Long Name:** The IAO will ensure WLAN network device management interfaces and management consoles are password protected and the password is compliant with DoD password policies. Password length and complexity will be in accordance with requirements of current DoD policies and INFOCON level.

**Severity:** CAT I

**Checks:** Inspect the network diagram and device configuration. Network level wireless devices such as access points, bridges, VoIP, WLAN controllers, WLAN management/authentication servers, and security gateways must have password and access control IAW DoD policy. Management password compliance.

- Ask the IAO if the password requirements associated with different INFOCON levels are followed.
- Ask if passwords are created and maintained IAW requirements of DoDI 8500.2, IAIA-1, and IAIA-2. <http://www.dtic.mil/whs/directives/corres/html/850002p.htm>
  - o Passwords are, at a minimum, a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each.
  - o At least four characters must be changed when a new password is created.
- Are passwords for these devices recorded and stored in accordance with local procedures for wired network devices.
- Record the devices that have this finding in the comments area by serial and model number.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0373 Do not use WWAN systems for classified**

**VMS Vulnerability Key:** V0014206

**Long Name:** The IAO will ensure WWAN systems are not used to store, process, or transmit classified information.

**Severity:** CAT I

**Checks:** Interview the IAO. Inspect the user training materials or user agreement to verify users have been told of this requirement.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0374 Do not permit WWAN in a SCIF**

**VMS Vulnerability Key:** V0004643

**Long Name:** The IAO will ensure that WWAN devices are not permitted in a permanent, temporary, or mobile SCIF.

**Severity:** CAT I

**Checks:** Work with the traditional reviewer or interview the IAO or SM.

1. Verify the site's existing physical security policy addresses wireless devices in SCIFs.
2. The policy should prohibit WWAN devices since they are not DCID compliant.
3. Posted signs or security/training materials are also evidence of compliance.

Mark as a finding if wireless devices are not addressed in the SCIF procedures or if users are not trained.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0378 Authentication and Encryption for WiMax systems**

**VMS Vulnerability Key:** V0014207

**Long Name:** The IAO will ensure that site WiMax (IEEE 802.16d &e) systems implement strong authentication and encryption as follows:

- Encryption: All information traveling over point-to-point links that are providing backhaul or site-to-site connectivity shall be minimally protected with data-in-transit encryption using FIPS 140-2 validated modules for unclassified information, or minimally protected with data-in-transit encryption using HAIPE devices for classified information. Encryption should be at OSI layer 2 or 3.
- Authentication: WiMax systems will use strong authentication (i.e. two factor) at the device and network level.

**Severity:** CAT II

**Checks:** Interview the IAO and review system network diagrams and data sheets. Verify required encryption and authentication mechanisms are being used.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

### 4.3 Radio Frequency Identification (RFID)

The following checks apply to computer systems that process DoD information and are connected to an RFID device. If the RFID reader is connected to a networked or standalone workstation, perform OS review.

Current DoD RFID policies do not address security and privacy of data stored on RFID tags or of data in transit while being read by an RFID scanner. (DoD RFID policies can be found at [http://www.acq.osd.mil/log/rfid/rfid\\_policy.htm](http://www.acq.osd.mil/log/rfid/rfid_policy.htm).) Industry standards have not been developed for storing encrypted data on RFID tags. Currently, there are no RFID products that provide FIPS 140-2 validated encrypted data on the tag or encrypt data in transit between the tag and reader. Several companies provide RFID systems where tag data is encrypted before it is stored on the tag.

#### **WIR0495 RFID systems must comply with DoD security requirements**

**VMS Vulnerability Key:** V0014034

**Long Name:** The IAO will ensure appropriate operating system and network STIGs are followed for RFID systems that connect to computers that store, process or transmit DoD information or is connected to a DoD network.

**Severity:** CAT III

**Checks:** Interview the SA to verify compliance.

If an RFID system is connected to computer that stores, processes or transmits DoD information or is connected to a DoD network, then each component (e.g., database server, operating system, network component checks) must be evaluated using the applicable DISA STIG.

**VMS users only:** This check is a high level check which ensures that the proper policies will be applied to systems using this technology. The reviewer/site must:

- Register the entire asset posture based on the type of devices within which the RFID transceiver is installed (e.g., a laptop or PDA).
- For laptops, register a workstation asset and add the “Wireless Client” element to the asset posture.
- For PDAs, register a PDA asset and add the “PED/PDA” element to the asset posture.

For servers associated with the RFID system, register a server asset. Generally, there is no RFID installed in the server.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

#### 4.4 Free Space Optic (FSO) Terminal Devices

The following checks apply to all terminal devices that use FSO as the wireless transmission method to connect to the DoD network.

The reviewer may encounter these devices used for point-to-point wireless network bridging between buildings.

##### **WIR0330 Management access must use compliant password**

**VMS Vulnerability Key:** V0014890

**Long Name:** The IAO will ensure wireless network device management interfaces and management consoles are password protected and the password is compliant with DoD password policies. Password length and complexity will be in accordance with requirements of current DoD policies and INFOCON level.

**Severity:** CAT I

**Checks:** Inspect the network diagram and device configuration. Network level wireless devices such as access points, bridges, VoIP, WLAN controllers, WLAN management/authentication servers, and security gateways must have password and access control IAW DoD policy. Management password compliance.

- Ask the IAO if the password requirements associated with different INFOCON levels are followed.
- Ask if passwords are created and maintained IAW requirements of DoDI 8500.2, IAIA-1, and IAIA-2. <http://www.dtic.mil/whs/directives/corres/html/850002p.htm>
  - Passwords are, at a minimum, a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each.
  - At least four characters must be changed when a new password is created.
- Are passwords for these devices recorded and stored in accordance with local procedures for wired network devices.
- Record the devices that have this finding in the comments area by serial and model number.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0390 Use encryption for FSO network communications (data in transit)**

**VMS Vulnerability Key:** V0014891

**Long Name:** The IAO will ensure FIPS 140-2 compliant encryption is used to secure the link between the two FSO terminal devices (e.g., VPN or security gateway).

**Severity:** CAT II

**Checks:** To verify use of FIPS 140-2 compliant encryption, request IAO provide the FIPS certificate or vendor documentation. This check applies only to unclassified systems.

Mark as a finding if encryption is not used or is not FIPS compliant.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0391 Install FSO bridges in an isolated network**

**VMS Vulnerability Key:** V0014892

**Long Name:** The IAO will ensure FSO bridges are placed in a screened subnet (DMZ or firewall separating intranet and wireless network), or VLAN and/or otherwise separated from the wired internal network.

**Severity:** CAT II

**Checks:** Review network architecture with the network administrator.

1. Verify compliance by inspecting the site network topology diagrams and the firewall interface configurations.
2. Since many network diagrams are not kept up-to-date, walk through the connections with the network administrator to verify the diagrams are current.

Mark as a finding if the wireless network device does not use an approved network isolation method (e.g., DMZ, VLAN, VPN).

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

## 4.5 Wireless VoIP

Perform the following checks for wireless APs and clients used for VoIP services.

### **WIR0133 Wireless VoIP systems must comply with applicable requirements**

**VMS Vulnerability Key:** V0004640

**Long Name:** The IAO will ensure all wireless VoIP systems comply with applicable requirements in the Wireless STIG, Section 2.2.4, IEEE 802.11 WLAN Implementation Compliance Requirements, and the VoIP STIG.

**Severity:** CAT II

**Checks:**

1. Perform all applicable checks in Section 2.0 of the Wireless Checklist.
2. The purpose of this check is to ensure that the reviewer or self-checker has performed the general Wireless Policy checks as part of the review of a VoIP system.

Mark this check as a finding if any CAT I or II checks in the VoIP STIG or any vulnerability of the Wireless Checklist, Section 2 are marked as a finding. (Also mark the individual checks in Section 2 as findings).

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

## **4.6 Wireless Keyboards and Mice**

These devices must be documented on the site's wireless equipment list. Also apply Wireless Policy checks.

For VMS users: These assets are entered into VMS as part of a wired **or** wireless workstation asset posture. Register the workstation asset (SRR reviewers may use the Gold Disk) and add the wireless peripherals as part of the wired desktop/laptop's asset posture.

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



**WIR0131 Infrared keyboards and mice must comply with requirements**

**VMS Vulnerability Key:** V0007073

**Long Name:** The IAO will ensure 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 IR wireless mice and/or keyboards for use 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 are no windows unless each window is covered with a film approved for blocking IR. All doors will 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 is 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 is completely covered with metallic tape.

**Severity:** CAT II

**Checks:** Review documentation.

1. Verify that the IR device is DAA approved and in compliance with CTTA separation requirements.
2. Visually and electronically survey the area to test if emanations from the IR device is transmitting beyond the allowed area as per CTTA (or ask for documentation showing that this testing has to be done).
3. Verify that the policy requirements listed in the policy above are in place and users are trained on the requirements by interviewing the SM or IAO.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0132 Wireless keyboards and mice must comply with WLAN requirements**

**VMS Vulnerability Key:** V0004639

**Long Name:** The IAO will ensure if WLAN or Bluetooth mice and keyboards are used, applicable requirements listed in the Wireless STIG, Section 2.2.4, IEEE 802.11 WLAN Implementation Compliance Requirements, or Section 2.3, Bluetooth WPAN, are followed.

**Severity:** CAT II

**Checks:** The verification procedure used depends on which transmission protocol is used by the keyboard, 802.11 or Bluetooth. Annotate the specific issues found in the Comments section.

For keyboards and mice that use the **802.11** protocol, the following policies are enforced and documented.

1. DAA approval is obtained prior to use.
2. Wireless keyboards and mice must be documented on the wireless equipment list and SSAA.
3. 802.11 wireless keyboards/mice must not be used for Classified TS/SCI processing.
4. Wireless keyboards and mice must not be used in SCIFs of any type.
5. 802.11 wireless keyboards and mice shall not be used to process classified information.
6. Wireless keyboards and mice must use FIP 140-2 certified encryption.

For keyboards and mice that use the **Bluetooth** protocol, the following policies are enforced and documented.

1. Perform the checks in the **Bluetooth Compliance Requirements section** of this checklist.
2. This is an automatic CAT II finding if Bluetooth keyboards and mice (and most 802.11 are used, since FIPS 140-2 compliant encryption is not available for Bluetooth. However, downgrade to a CAT III if some form of encryption is used.

**Hint:** Currently, no wireless keyboards or mice meet these requirements. If the wireless mouse/keyboard is using a proprietary RF protocol (i.e., not Bluetooth or 802.11), then apply the Bluetooth checks.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

## 5. PDA AND SMARTPHONE COMPLIANCE REQUIREMENTS

Perform checks in wireless policy section and this section for PDAs regardless of operating system; wireless telephones (e.g., single function cellular phones, PCS phones, and SMS devices); 2-way pagers; and multifunctional cellular devices (e.g., voice, SMS, MMS and 2-way pagers).

**For VMS users:** Select **PDA/PED** as the asset posture.

### **WIR0012 Display required DoD logon banner on PDA**

**VMS Vulnerability Key:** V0015399

**Long Name:** The IAO will ensure all PDAs display the following banner during device unlock/logon: "I've read & consent to terms in IS user agreement."

**Severity:** CAT III

**Checks:** Work with the SA to review the configuration of the PDA security management server or security policy configured on the PDA.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0050 Configure Antivirus software on all wireless clients**

**VMS Vulnerability Key:** V0014275

**Long Name:** The IAO will ensure DoD licensed anti-virus software is installed on all wireless clients (e.g., laptops, PDAs, and smartphones) and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signatures every 14 days or less.

**Severity:** CAT I

**Check:** Verify that laptop computers, PDAs, and smartphones are protected by anti-virus software.

4. For laptops, work with the Team Lead and Windows reviewer to run the Gold Disk or SRR scripts on a 10% representative sample of the clients.
5. For PDAs and cell phones, inspect a 10% sampling of the devices. Verify the software is:
  - o Configured to scan upon startup (once daily) or the user trained to scan at least once per week.
  - o Configured to automatically update at least every 14 days or the user trained to manually update once every two weeks.
  - o Enabled for Web browser download protection.
  - o If DoD approved antivirus products (e.g. downloaded from the JTF GNO antivirus portal) are not available for the wireless device, sites must select commercial products which are from major vendors with preference given to products tested or already used by other DoD organizations.
  - o The DAA must give written approval of this product.
6. Mark as a finding if any of the following are true:
  - o The Gold Disk results indicate this is a finding
  - o No antivirus software is installed; update procedures are not configured or used; or the software is not configured IAW the Wireless STIG policy.
  - o If the software used on a laptop but is not DoD approved, then mark as a **CAT III** finding.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0280 Wireless clients connecting via the Internet must be compliant**

**VMS Vulnerability Key:** V0003516

**Long Name:** The IAO will ensure if a wireless device is to be used to access a DoD network via the Internet through a public wireless Internet gateway (e.g., airport or hotel “hotspot”), the following requirements are met:

- The requirements in the Secure Remote Computing STIG are followed.
- The wireless client device has an approved personal firewall, antivirus, and VPN client installed and is operational with the latest updates installed before the wireless connection is enabled.
- After connecting to the hotel wireless portal, users will be trained to immediately connect to the DoD network via the VPN client. All connections for Government official business to the Internet via the hotel wireless network will be through the DoD VPN connection only.
- Users are trained to turn-off wireless cards immediately after a VPN connection is disconnected.

**Note:** OSD NII (wireless) has determined that connecting to a public hot spot today, if allowed by DoD Component level policy, is permitted per DoDD 8100.2. Minimum requirements: FIPS 140-2 validated data-in-transit, FIPS 140-2 validated data-at-rest, anti-virus, and strong authentication. OSD NII is currently developing a DoD Remote Access policy that will place restrictions on the use of public WLAN systems by DoD wireless users.

**Note:** DISA FSO and NSA recommend that DoD WLAN users do not connect to public WLAN systems (public hot spots and hotel WLAN systems). It is impossible, using currently available security tools, to provide 100% assurance that a user is connecting to a legitimate public hotspot or hotel WLAN access point rather than a hacker controlled access point or to stop a hacker from exploiting a WLAN laptop after a user connects to a hacker controlled hotspot.

**Severity:** CAT II

**Checks:** Interview the IAO. This check refers to remote access to DoD non-publicly available resources.

Ask the IAO if devices with WLAN NICs are permitted to connect to the DoD network remotely using a public Internet connection. If so, perform the following.

- Verify that the site has applied the Secure Remote Computing STIG by asking for evidence (e.g., Desktop/Network Infrastructure checklists or demonstration of a setting) and users have been trained on how to connect securely to a public WLAN system.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0340 Do not discuss classified/sensitive information on unclassified cell phones**

**VMS Vulnerability Key:** V0014011

**Long Name:** The IAO will ensure if non-secure (devices are not FIPS 140-2 certified or NSA Type-1 certified) cellular phones, cordless phones, and two-way radios are used for voice communications, users are trained not to discuss classified or sensitive information on these devices.

**Severity:** CAT III

**Checks:** Interview IAO and work with the traditional security reviewer.

Verify users are trained on this requirement. Posted signage, has a sticker on each phone, user training, or user agreement is acceptable.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0371 PDAs/Smartphones with cameras must be approved**

**VMS Vulnerability Key:** V0004840

**Long Name:** The IAO will ensure PDAs and Smartphones with digital cameras (still and video) are allowed in a DoD facility only if specifically approved by site physical security policies.

**Severity:** CAT III

**Checks:** Work with traditional reviewer to review site's physical security policy.

1. Verify that it addresses PDA devices with embedded cameras.
2. Mark this as a finding if there is no written physical security policy outlining whether wireless phones with cameras are permitted or prohibited on or in this DoD facility.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0372 PDAs and Smartphones with a cameras not allowed in classified areas**

**VMS Vulnerability Key:** V0012165

**Long Name:** The IAO will ensure PDAs or Smartphones with digital cameras (still and video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted, or processed.

**Severity:** CAT I

**Checks:** Work with the traditional reviewer to interview the Security Manager.

1. Review site's physical security policy.
2. Verify that users are informed of this policy by reviewing user agreement, posted signs, or training material.
3. Powering off, removal of batteries or blocking IR ports is not acceptable for disabling camera functionality, as this method has not been tested for efficacy.

Mark as a finding if a written policy and user training does not prohibit these devices in classified areas.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0380 Use NSA Type-1 end-to-end encryption classified PDAs (data in transit)**

**VMS Vulnerability Key:** V0003525

**Long Name:** The IAO will ensure PDAs used to transmit, receive, store, or process Classified data use NSA, Type-1 certified end-to-end encryption for data being transmitted, received, stored, or processed.

**Severity:** CAT I

**Checks:** Interview the IAO. Ask if there is classified use of PDA devices. Mark as a finding if PDA is used for classified process since there is currently no NSA, Type-1 PDAs.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0410 Do not connect PDAs/Smartphones to classified workstations**

**VMS Vulnerability Key:** V0003528

**Long Name:** The IAO will ensure PDAs and Smartphones are not connected to any workstation that stores, processes, or transmits classified data.

**Note:** This check does not apply to the SME PED.

**Severity:** CAT II

**Checks:** Review documentation or spot check.

1. Review training and user agreement to verify users have been informed of this requirement.
2. Reviewer may spot check a few workstations in classified area for hotsync or ActiveSync software or PED docking hardware.

Site may also choose to disable unused IR and USB ports and configure workstations in these areas so users cannot load hotsync/ActiveSync utilities and hardware drivers.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0420 Do not install PDA synchronization software on classified workstation**

**VMS Vulnerability Key:** V0003529

**Long Name:** The IAO will ensure synchronization software is not loaded on systems processing classified information. (Classified information will not be synched. PDAs will not be connected via hot-sync or ActiveSync to a classified workstation.)

**Note:** This check does not apply to the SME PED.

**Severity:** CAT II

**Checks:** Documentation review. Consult the traditional reviewer.

1. Verify the local physical security procedures, training materials, or posted signs inform the users of the need to disable voice recording and that hotsync or Activesync software is not to be used or loaded on classified PCs.
2. Reviewer may also physically check for synchronization cable on device or docking station.

Mark as a finding if syncing to classified workstations is allowed or users are not trained.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**



**Comments:**

**WIR0425 Encrypt classified data on PDAs (data at rest)**

**VMS Vulnerability Key:** V0004649

**Long Name:** The IAO will ensure classified data stored on PDAs is encrypted using NSA Type-1 certified encryption consistent with the classification level of the data stored on the device.

This requirement does not apply to the SME PED.

**Severity:** CAT II

**Checks:** Ask the IAO if PDAs are used to store classified data. If this is done, mark this as a finding since there is currently no NSA, Type-1 PDAs.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0450 Password protect PDA/Smartphone devices**

VMS Vulnerability Key: V0015814

**Long Name:** The IAO will ensure PDAs and Smartphones are protected by authenticated login procedures to unlock the device. Either CAC or PIN authentication is required.

When PIN authentication is used, the following procedures will be enforced.

- The device password /PIN is set to five or more characters. The system security policy must be configured to enforce this policy. If five characters are used, both a letter (lower or upper case) and a number must be used in all device passwords (the wireless email server must be configured to enforce this policy). If six or more characters are used, only numbers may be used for the password. It is recommended that eight or more characters be used.
- The number of incorrect passwords entered before a device wipe occurs is set to 10 or less. The system security policy must be configured to enforce this policy.
- The password is changed at least every 90 days. The system security policy must be configured to enforce this policy.

**Severity:** CAT I

**Checks:** Interview the IAO and administrator.

1. Verify CAC authentication or PIN authentication is used.
2. If PIN authentication is used, verify correct settings.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0460 Use FIPS 140-2 encryption to protect unclass data on PDA (data at rest)**

**VMS Vulnerability Key:** V0015816

**Long Name:** The IAO will ensure FIPS 140-2 certified encryption tools are used to encrypt unclassified data at rest on the wireless device.

**Severity:** CAT II

**Checks:** Interview IAO and review documentation

1. Obtain the product's FIPS certificate or vendor documentation from the IAO or the vendor. Use this documentation to verify compliance with the policy requirement for FIPS.
2. Verify that temp files with sensitive information are also protected with encryption.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0465 Do not download mobile code from non-DoD sources**

**VMS Vulnerability Key:** V0004650

**Long Name:** The IAO will ensure mobile code is not downloaded from non-DoD sources and is downloaded from only trusted DoD sources over assured channels.

**Severity:** CAT II

**Checks:** Review device configuration.

1. Verify site has performed a self-assessment.
2. Work with the SA to examine the site's method of enforcing this policy.
3. Internet browsers should be configured to prevent download of mobile code and other unauthorized programs.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

**WIR0470 Disable wireless radios/IR ports on PDAs/Smartphones when not in use**  
**VMS Vulnerability Key:** V0003533

**Long Name:** The IAO will ensure that wireless radios and IR ports on the PDAs and Smartphones:

- Have wireless radios and IR ports disabled when wireless / IR transmissions are not being used.
- Data exchange via the IR port should be limited to trusted DoD devices.

**Severity:** CAT II

**Checks:** Review documentation.

Interview IAO and ask if there is a written site policy and training program which ensures that users are aware of the policy to disable wireless radios and IR ports when not in use.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

**WIR0540 PDAs with text messaging cannot be used for sensitive data**

**VMS Vulnerability Key:** V0014190

**Long Name:** The IAO will ensure that if PDAs or Smartphones are used to send or receive cellular Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) messages, only unclassified, public releasable (i.e., not FOUO, sensitive information, or Classified) information will be sent or received.

**Severity:** CAT III

**Checks:**

1. Verify compliance by reviewing user agreements/training materials.
2. Ask if this service is available to the user and how the IAO ensures that the users with sensitive DoD data on their PDAs or Smartphones are not using these services.
3. Mark this as a finding if users are not trained on this requirement.

**SRR/ECV Finding (circle one):**

**OPEN            NOT A FINDING            NOT REVIEWED            NOT APPLICABLE**

**Comments:**

## **WIR0545 PDA/Smartphone connected to network has managed security policy**

**VMS Vulnerability Key:** V0014014

**Long Name:** The IAO will ensure that an IT policy manager is used to centrally manage the security policy on PDAs and Smartphones used for wireless remote connections (e.g., VPN, thin client (e.g., Citrix), Outlook Web Access via WLAN, cellular, etc.) to DoD networks or to send, receive, or save in memory DoD information, including email.

The IT policy manager will be configured to control the following functions on the PDA/Smartphone:

- Enable/disable wireless services (IR, Bluetooth, WLAN, cellular, etc.).
- Enable/disable camera and voice recording.
- Select user authenticated logon to the device via password/PIN or Smart Card Login (SCL) (user cannot bypass device authentication).
- When password authentication is enabled, the handheld device will automatically perform a “Data Wipe” command after X number of unsuccessful password authentication attempts. The value of X is set by IT policy management control. Data Wipe will delete all data/information in addressable memory on the device.
- Password authentication setting of the IT policy manager is configurable as needed to meet both DoD and local mission requirements. Thus, the following features are required:
  - o Ability to set maximum password age (e.g., 30 days, 90 days, 180 days)
  - o Ability to set minimum password length. A range of 5 to 15 characters is the minimum requirement.
  - o Ability to set maximum password attempts. Device will perform a Data Wipe after a set number of incorrect passwords are entered. A range of 3-10 incorrect passwords before a Data Wipe is performed is the minimum requirement.
  - o Ability to set minimum password history (0-5 is the minimum requirement)
- The handheld device inactivity timeout setting will be configurable to between 3 to 60 minutes range). This setting requires the user to unlock the device by reentering their password or Smart Card PIN after the configured period of inactivity. The administrator will choose a specific setting based on mission/user requirements, however, a setting of 15 minutes is recommended based on current NSA operating system inactivity requirements.
- The system shall control the capability of the user to install or de-install third party applications on the handheld device.
- If SCL is supported, the Smart Card Reader (SCR) is fully interoperable with DoD PKI and CAC.

**Note:** The Wireless Checklist Windows Mobile Messaging Checklist shows one example of a system that is compliant with this requirement.

**Severity:** CAT II

**Checks:** PDAs and Smartphones must be managed using automated security policy software. Verify that the application is compliant with the configuration settings above. Mark as a finding if PDAs/Smartphones are not centrally managed or if the application configuration is not compliant.

**SRR/ECV Finding (circle one):**

**OPEN**

**NOT A FINDING**

**NOT REVIEWED**

**NOT APPLICABLE**

**Comments:**

## **APPENDIX A. VMS PROCEDURES**

The following information applies only to teams and sites that use VMS to enter and track DoD assets. When conducting a Wireless SRR, the Team Lead and the assigned Reviewer identify security deficiencies, provide data from which to predict the effectiveness of proposed or implemented security measures associated with the wireless system and operating environment. Security Readiness Review (SRR) of a DoD wireless system requires that the results of the SRR be tracked using the VMS database.

The Team Lead begins by completing both the Visit and the Visit Summary forms under the appropriate Organization in VMS. During a site review, Reviewers update findings for a requested set of site assets. Reviewers enter findings in VMS by updating the same compliance status screens used by the site's System Administrators (SAs). For wireless assets, Reviewers will update assets and findings manually using VMS screen rather than an XML script. When the Reviewer is finished updating SRR results associated with each asset, the Team Lead will compile an executive summary, finalize the Visit information screen in VMS, and request visit approval. Following a review, the Team Lead reports the results back to the Director who requested the review. After reviewing the results of the Visit, the Director can then access VMS to provide any required approvals.

### **ADDING AN ORGANIZATION**

When Team Leads arrange a visit, if the site does not exist in VMS, a new organization may be requested.

1. Click Organization Maint. in the VMS navigation pane and then click Request to access the Request Organization form.
2. Complete all of the required fields on the form.
3. Click Submit.

### **REGISTERING AND MANAGING WIRELESS ASSETS**

In VMS, an asset is defined as a hardware device or an operating system image that hosts an application (or workload) that is accessed by more than one user. An asset may also include physical locations or other non-computing assets, such as a SWLAN or WLAN. Unclassified asset components are registered in VMS via the NIPRNet and confidential or secret asset components are registered via the SIPRNet. The Team Lead or the SA must register assets.

Both the Reviewer and the SA will create, maintain, and track assets in VMS. The reviewer will use the Asset and Finding Maintenance screen to perform these functions. The SA will use the By Location navigation chain to perform the same function. When Reviewers access the Asset and Finding Maintenance screen, the Navigation pane displays a white Visits folder. Expand this Visits folder to display its subfolders. Each subfolder represents an individual visit in VMS that has been assigned for review. Click (+) to expand the visit and display the location summaries for the visit. Within the location wireless assets are tracked using one of the following asset types.

- Computing – Assets which have an OS such as PEDS and network devices and clients.
- Non-Computing – Used for registering wireless networks

Use the following matrix to select the appropriate asset type for each wireless asset. Note that a wireless network is registered as a separate Non-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.

Wireless Technology	VMS Asset Type	Asset Posture
<b>Computing</b> – Assets with an OS such as PEDs, APs, and client workstations with wireless NICS installed. <b>Non-Computing</b> – Used for registering wireless networks. Applies general networking environment policies.		
All wireless devices (WLAN, WiMax, Bluetooth, FSO, SWLAN)	Non-Computing	<b>Network Policy Requirements -&gt; Wireless Policy</b>  <i>Note:</i> These checks apply to the network or concern site policy rather than to a specific access point or PDA.  The reviewer should create one non-computing asset for the each wireless network.
WLAN Access Point	Computing	<b>Network -&gt;Data Network -&gt; Wireless -&gt; Wireless Access Point</b> <b>Operating System</b> - Embedded OS->Other Network OS (mark these checks as N/A)
WLAN Switch/Controller	Computing	<b>Network -&gt;Data Network -&gt; Wireless Switch</b>
Free Space Optics (FSO Device)	Computing	<b>Network -&gt;Data Network -&gt; Wireless-&gt; Free Space Optics (FSO) Device</b>
Wireless IDS device	Computing	<b>Network -&gt;Data Network -&gt; Wireless-&gt; Wireless IDS</b>
SecNet 11 Access Points	Computing	<b>Network -&gt;Data Network -&gt; Wireless Access Point</b>
Classified Network Client Device with SecNet 11 or SecNet 54 PCMCIA NIC installed	Computing	<b>Network:</b> Data Network → Wireless -> Harris SecNet 11 -> Harris SecNet 54  <b>Application</b> – Select all that apply (e.g., Browsers, Office Automation, etc). See the VMS procedures for the operating system SRR and the Desktop Checklist for more details.  <b>Role:</b> Workstation
Network Client Device with WLAN (802.11) (with OS) (laptop only)  <i>Note:</i> laptops that connect via the Internet must comply with PDA/PED policies.	Computing	<b>Operating System</b> – drill down to OS then further down into service pack or version OS as applicable.  <b>Network -&gt;Data Network – Wireless -&gt; Wireless Client-&gt; Wireless LAN Client</b>  <b>Network -&gt;Data Network -&gt; Wireless -&gt; Wireless</b>



Wireless Technology	VMS Asset Type	Asset Posture
<p>*the windows reviewer must review and register the asset using the gold disk prior to the wireless review is entered into VMS. This will create the windows asset posture and perform the gold disk script checking the client security stance.</p> <p>* register a sample of clients only.</p>		<p>PDA/PED (<i>only if connects via internet</i>)</p> <p><b>Application</b> – Select Antivirus and then applicable version installed.</p> <p><b>Role</b> - Workstation</p>
<p>Network Client Device with WLAN (802.11) (PDA only)</p> <p>* register a sample of clients only.</p>	Computing	<p><b>Network</b> -&gt;Data Network – Wireless -&gt; Wireless Client-&gt; Wireless LAN Client</p> <p><b>Network</b> -&gt;Data Network -&gt; Wireless -&gt; Wireless PDA/PED</p> <p><b>Application</b> – Select Antivirus and then applicable version installed.</p> <p><b>Role</b> - Workstation</p>
<p>Network Client Device with WWAN (broadband) Network Client (with OS)</p> <p><b>Note:</b> This applies to cellular broadband systems (i.e. cellular aircards).</p> <p><b>Note:</b> laptops that connect via the Internet must comply with PDA/PED policies.</p> <p>* register a sample of clients only.</p>		<p><b>Operating System</b> – drill down to OS then further down into service pack or version OS as applicable.</p> <p><b>Network</b> -&gt;Data Network – Wireless -&gt; Wireless Client-&gt; Wireless Broadband WWAN Client</p> <p><b>Network</b> -&gt;Data Network -&gt; Wireless -&gt; Wireless PDA/PED (<i>only if connects via internet</i>)</p> <p><b>Application</b> – Select Antivirus and then applicable version installed.</p> <p><b>Role</b> - Workstation</p>
<p>PDA with NIC/wireless radio (if PDA used for wireless email, see Blackberry Handheld Devices, Windows Mobile Email Devices, or SME-PED Devices below)</p>	Computing	<p><b>Note:</b> Do not mark as a workstation</p> <p><b>Operating System</b> – Embedded OS-&gt;Other Network OS</p> <p><b>Application</b> -&gt; Select Antivirus and then applicable version installed.</p> <p><b>Network</b> -&gt;Data Network -&gt;Wireless -&gt; PDA/PED</p>

Wireless Technology	VMS Asset Type	Asset Posture
PDA without NIC/wireless radio	Computing	<b>Note:</b> Do not mark as a workstation or enter IP or MAC address  <b>Operating System</b> – Embedded OS->Other Network OS.  <b>Network</b> – Data Network -> Wireless -> PDA/PED
Blackberry Enterprise Server	Computing	See Wireless STIG, BlackBerry Checklist
Wireless Email System servers (other than Blackberry)	Computing	See either Apriva Sensa Checklist, Windows Mobile Messaging Checklist, or Good Mobile Messaging Checklist (when published)
SME-PED Servers	Computing	See SME-PED Checklist (when published)
Blackberry Handheld Devices	Computing	See Wireless STIG, BlackBerry Checklist
Windows Mobile Email Devices	Computing	See either Apriva Sensa Checklist, Windows Mobile Messaging Checklist, or Good Mobile Messaging Checklist (when published)
SME-PED Devices	Computing	See SME-PED Checklist (when published)
Wireless Telephone	Computing	<b>Note:</b> Do not enter IP or MAC address  <b>Network</b> ->Data Network -> Wireless -> PDA/PED  <b>Operating System</b> – Embedded OS->Other Network OS
Wireless Voice-Over-IP system and Telephone Instrument	Computing	If WLAN, follow Network Client Device with WLAN (802.11) above. If WWAN, follow Network Client Device with WWAN (broadband) Network Client above
Wireless NIC (Not in a laptop)	N/A	Not required to enter this type of asset in VMS
Wireless SCRs, keyboards, mice	Computing	<b>Network</b> ->Data Network – Wireless -> Wireless Client  <b>Operating System</b> – Embedded OS->Other Network OS

**Table A-1. VMS Asset Matrix**

VMS also provides icons to help you identify important review items. For example, the red exclamation point icon, located near the bottom of the navigation tree on the right, identifies an item that must be reviewed. Assets are also listed according to the following categories.

- Must Review – Assets that must be reviewed (also marked with a red exclamation point).
- Reviewed – Site assets modified by the Reviewer
- Not Selected for Review – Other site assets that were not targeted for review


**NOTE:** If you save changes to assets or findings in the Must Review area, VMS will automatically log those assets as reviewed and move them to the Reviewed area.

The asset icon color in the Navigation pane indicates the severity of an open finding for the asset. The cubes on the right describe what each of the colors signifies.

- Red – CAT I
- Orange CAT II
- Yellow – CAT III
- Light Green CAT IV
- Dark Green – No open or not reviewed items.
- Updating SRR Findings to VMS

### **CREATING NON-COMPUTING WIRELESS ASSETS**

To create a wireless network **Non-Computing** asset, perform the following steps.

1. Expand Asset Findings Maint.
2. Click Assets/Findings.
3. Reviewer Only: Expand Visits and skip to Step 5.
4. SA only: Expand Location then the required organization. Then skip to Step 7.
5. Reviewer Only: Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review. If the Visit is not visible, you have not been designated at the visit level as a reviewer. See your Team Lead.
6. Reviewer Only: Expand the visit and display the location summaries for the visit.
7. Click the  Create icon located next to Non-Computing. The asset form is displayed.
8. Click the General tab and enter information into all required fields

Host Name

Managed By – use for remote locations being managed.

Owner Field – use to register asset to parent or child location.


Mac level, Confidentiality, and Use – change or verify default values as required.

**NOTE:** The Asset Identification tab is not used for Non-Computing assets.

9. Click the Asset Posture tab to add functions to the asset.  
Expand Non-Computing then Network Policy Requirements  
Click Wireless Policy (required)  
Click the >> button to the selected option(s) to the Selected window  
Click Save

## CREATING COMPUTING WIRELESS ASSETS

To create a wireless Computing asset, perform the following steps.

1. Expand Asset Findings Maint.
2. Click Assets/Findings.
3. Reviewer Only: Expand Visits and skip to Step 5.
4. SA only: Expand Location then the required organization. Then skip to Step 7.
5. Reviewer Only: Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review. If the Visit is not visible, you have not been designated at the visit level as a reviewer. See your Team Lead.
6. Reviewer Only: Expand the visit and display the location summaries for the visit.
7. Click the  Create icon located next to Computing. The asset form is displayed.
8. Click the General tab and enter information into all required fields

Host Name

Managed By – use for remote locations being managed.

Owner Field – use to register asset to parent or child location.

Mac level, Confidentiality, and Use – change or verify default values as required.

Status – select Online or Offline

Workstation – If Yes is selected, then also enter entry for Additional workstations with this image field. Change to Yes only for laptops and desktops used with wireless NICs, including SecNet 11 and 54 PC cards.

9. Click the Asset Identification tab

Enter IP address and click Add

Enter the MAC address and then click Add

10. Click the Asset Posture tab. In the Available pane, expand Computing and drill down to select the following functions as indicated in the Table 1.2, Asset Posture Matrix in a previous section of this document.

Operating System – drill down to required selection

Role – drill down to required selection

Network - drill down to required selection

Click the >> button to the selected option(s) to the Selected window

Click Save

## ASSET FINDING MAINTENANCE

As part of the Wireless SRR, Reviewers enter findings manually into VMS as follows.

1. Expand Asset Findings Maint.
2. Expand Assets/Findings
3. Expand Visits to display its sub-folders. (Reviewer Only SA will expand Location and proceed to step 6.
4. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

5. Expand the visit and display the location summaries for the visit.
6. Expand either Computing or Non-Computing depending on the asset type registration.
7. Expand Must Review *(Reviewer Only. SA will not see 'Must Review', but will proceed to step 8.)*
8. Expand Asset to Review. Ready to review is colored in RED
9. Expand the asset and then each Vulnerability Key.
10. Update the 'Status' of the vulnerability
11. Identify details on all open vulnerabilities
12. If applicable: Apply the same Status and comments to other assets by using the 'apply to other Findings' pane.

### **VERIFY ALL REQUIRED ASSETS ARE UPDATED**

1. Asset Findings Maint
2. Visits
3. Expand visit
4. Expand CCSD
5. Expand location
6. Expand computing or non-computing as applicable.
7. Expand Must Review. Verify checkmarks are gone from all vulnerabilities, indicating the asset is updated/reviewed.
8. If checkmarks remain from previous step, update findings using the procedures for Updating SRR Findings to VMS procedures given in a previous subsection.

### **PRINTING COMPLIANCE AND SUMMARY REPORTS**

Compliance and summary reports can be helpful in preparing for an SRR or for SAs in tracking and monitoring findings status.

### **VC06 ASSET COMPLIANCE REPORT**

1. Navigate to the Reports Menu and select the VC06 report.
2. Select to do the report by asset or an by organization as needed
3. Select "open" status
4. Sort on desired fields as required
5. Select the following to Display
  - Finding Comments
  - Finding Long Name
  - Because it's truncated otherwise
  - Finding Details
  - Vulnerability Discussion

### **VC03 SEVERITY SUMMARY REPORT**

Same steps as above but the report will give only the vulnerability numbers, which match the criteria selected. These reports can provide a quick check of status.

### **AS01 REPORT**

The AS01 report assists the reviewer or SA by quickly identifying the assets at the location the review is being performed. In the section “Looking at Network Assets” is a quick step by step instruction in creating the report. The site may want to do other reports, if your site manages or owns assets, which are not located at the site. Check Child Locations if applicable. Navigate to the Reports menu, Select the AS01 Report, and select the desired criteria for the report.

### **VL01 REPORT**

The VL03 report assists the reviewer or SA by quickly identifying the IAVMs that will be identified to the asset when you select the operating system of the asset. Navigate to the Reports menu, Select the VL01 Report, and select the desired criteria for the report.

**APPENDIX B. SRR WORKSHEETS**

**Date of Wireless:** \_\_\_\_\_ **SRR:** \_\_\_\_\_

<b>Network Reviewer</b>		<b>Phone/Location</b>		
<b>Previous SRR (circle)</b>	Y N	<b>Date of Previous SRR</b>		
<b>Number of Current Open Findings</b>				
<b>Site Name</b>				
<b>Address</b>				
<b>Phone</b>				
<b>Position</b>	<b>Name</b>	<b>Phone Number</b>	<b>Email</b>	<b>Area of Responsibility</b>
SM				
IAM				
NSO				





**Table B-2. Wireless Network Clients: Laptops using WWLAN, WPAN and Cellular 3G NICs Worksheet**

#	<b>CLIENT INFORMATION</b> <b>Function: Laptop, PDA, Desktop, etc</b> <b>Manufacturer/Model</b> <b>OS/Service Pack</b> <b>NIC type (802.11, 3G, Bluetooth</b> <b>Embedded or removable?</b> <b>PKI? FIPS encryption?</b>	<b>Host Name</b>	<b>MAC and IP</b> <b>Addresses</b>	<b>Accessories/ Software:</b> <b>Firewall</b> <b>(Y/N)</b> <b>Antivirus</b> <b>version</b>	<b>Sensitivity (U, S, TS, SCI)</b>	<b>Approved/ Coordinated</b> <b>(DAA, CTTA, DCID)</b>
<p>10% of the site's wireless client devices (laptops, PDAs, etc) must be reviewed. The entire posture of the client, to include the OS and non-wireless roles must entered into VMS as part of the asset posture (e.g., if the wireless device is also a database server). If laptops are created using an <b>image</b>, they may be entered S using one entry using the duplicate feature of VMS. Host Name, MAC, and IP must be entered into VMS. NICs, keyboard, mice, and 3G cards are not tracked separately in VMS but must be documented.</p>						

**Table B-3. Standalone PDAs, Cellular Telephones, SMS Devices, and Two-Way Pagers**

#	<b>CLIENT INFORMATION</b> <b>Function: Laptop, PDA, Desktop, etc</b> <b>Manufacturer/Model</b> <b>OS/Service Pack</b> <b>NIC type (802.11, 3G, Bluetooth</b> <b>Embedded or removable?</b> <b>PKI? FIPS encryption?</b>	<b>Host Name</b>	<b>MAC and IP</b> <b>Addresses</b>	<b>Accessories/ Software:</b> <b>Firewall</b> <b>(Y/N)</b> <b>Antivirus</b> <b>version</b>	<b>Sensitivit y (U, S, TS, SCI)</b>	<b>Approved/ Coordinated</b> <b>(DAA, CTTA, DCID)</b>
5% of the site's Standalone PDAs, Cellular Telephones, SMS Devices, and Two-Way Pagers must be reviewed. The review may be done via IAO interview or a physical inspection of the devices. Accessories used with these devices such as SCRs, keyboards, headphones, and mice are not tracked separately in VMS but must be documented.						

This page is intentionally blank