

UNCLASSIFIED



# **WIRELESS STIG REVISION HISTORY**

**Version 6, Release 9**

24 October 2014

Developed by DISA for the DoD

UNCLASSIFIED



REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V6R9	Wireless STIG, V6R8	– Added missing requirement WIR0235 to WLAN Client	24 October 2014
V6R8	Wireless STIG, V6R7	<ul style="list-style-type: none"> <li>– Corrected WIR-MOS-PDA-011 to reflect consistent Check and Fix text to align with MOS-SRG requirements; for device unlock on mobile operating systems with no access to sensitive or classified information, the requirement is a minimum of 4 numbers. For access to security containers and mobile devices with sensitive information, the minimum length is 8 numbers with complexity.</li> <li>– Remove WIR-MOS-PDA-013, maximum password/passcode age.</li> <li>– Corrected WIR0170: provided non-specific examples of client side software to detect simultaneous wired and wireless network connections.</li> <li>– Removed the following STIG benchmarks and policies from Wireless STIG: <ul style="list-style-type: none"> <li>– CMD Policy – removed and moved to Standalone CMD Policy Version 2 Release 3 STIG</li> <li>– Mobility Policy – removed and moved to Standalone Mobility Policy Version 2 Release 2 STIG</li> <li>– WMAN-Bridge – removed and moved to Network WMAN package</li> <li>– WMAN-Access-Point – removed and moved to Network WMAN Package</li> <li>– WLAN-Sensor-Server – removed and moved to Network Infrastructure Policy</li> </ul> </li> </ul>	25 April 2014

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		STIG/Benchmark <ul style="list-style-type: none"> <li>– WLAN-Controller – removed and moved to Network WLAN package</li> <li>– WLAN-Bridge – removed and moved to Network WLAN package</li> <li>– WLAN-Authentication-Server – removed and moved to Network Other Devices STIG/Benchmark</li> <li>– WLAN-Access-Point-Internet-Gateway – removed and moved to Network WLAN package</li> <li>– WLAN-Access-Point-Enclave-NIPRNet – removed and moved to Network WLAN package</li> <li>– Wireless Remote Access Policy – removed and moved to SRC Remote Access Policy STIG/Benchmark</li> <li>– KOV-26-Talon – removed and moved to Network</li> <li>– SECNET-11/54 – removed and moved to Network</li> <li>– CSfC-Campus-WAN – removed and moved to Network Infrastructure Policy/STIG</li> <li>– Free-Space-Optics-Device – Deleted</li> </ul>	
V6R7	Wireless STIG, V6R6	– Updated cross reference table item WIR0130 to reflect updated short title: WLAN devices JTIC certified.	26 July 2013
V6R6	Wireless STIG, V6R5	– Added new component in the STIG based	12 March 2013

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<p>on the Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package. New checks have been added in the STIG and section 2.2.4 and table A-1 in the Overview have been updated.</p> <ul style="list-style-type: none"> <li>Updated section 2.2.3 of the Overview to introduce the term "CMD".</li> <li>Added a new section to the Overview on Cellular Hotspots (section 2.9).</li> <li>V-3499/WIR0400 (FIPS validation for Bluetooth data/voice) has been updated to clarify the applicability of the requirement.</li> <li>V-3692/WIR0115-01 (WLAN EAP authentication) has been updated to provide exception information.</li> <li>V-25319/WIR0123 (Internet-only WLAN Access Point network connection) has been updated to clarify logical separation requirements for the WLAN subnet.</li> <li>The following checks have been updated with minor editorial changes: V-30257/WIR0116 (WLAN DoD authentication), V-3515/WIR0125-01 (Transmitted WLAN AES-CCMP), V-19894/WIR0125-02 (AES-CCMP implementation FIPS validated), and V-14004/ WIR0130 (WLAN devices JITC certified).</li> </ul>	
V6R5	Wireless STIG,V6R4	<ul style="list-style-type: none"> <li>WIR0015 (List of approved wireless devices): Removed several items required to be recorded on the list (wireless client IP address, wireless channel set for each access point, and encryption key used).</li> <li>WIR0116 (WLAN DoD CAC authentication): Added check to Wireless Client STIG. It had previously been included in the access point and controller STIGs only.</li> </ul>	28 October 2011

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> <li>- WIR0120 (Interception of WLAN signals): Recast check to emphasize various methods of avoiding signal interception rather than just setting power to the “lowest possible” level. These methods include proper placement of access points and use of directional antenna.</li> <li>- WIR0124 (Internet-only WLAN Access Point firewall rules): Added more specific firewall rule guidance for WLAN infrastructure supporting guest access to Internet.</li> <li>- WIR0130 (WLAN JTIC interoperability certification): Recast existing check on interoperability to focus on JTIC certification. Removed Wi-Fi Alliance requirements, which were redundant with other check checks.</li> <li>- WIR0135 (WLAN network devices in an isolated network): Removed direct connection of APs to a WLAN controller (without other defense-in-depth-mechanisms) from the list of acceptable network architectures.</li> <li>- WIR0210 (SWLAN architecture): Modified check so that it is applicable at all times and not just prior to network connection.</li> <li>- WIR-SPP-006-01 (Smartphone users receive required training): Added that training should include procedures for verifying that the smartphone’s active connection is to a known access point.</li> <li>- Updated text fields throughout Wireless STIG:               <ul style="list-style-type: none"> <li>- Replaced generic vulnerability discussions and fix text with language tailored to each check</li> <li>- Updated technical terminology to comply with NIST, NSA, IEEE,</li> </ul> </li> </ul>	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> <li>and Wi-Fi Alliance standards</li> <li>- Additional clarifying guidance provided in check content where applicable</li> <li>- “Will” changed to “must” in long name</li> <li>- Notes removed from long name</li> <li>- Created new checks when an existing check covered more than one independent requirement:               <ul style="list-style-type: none"> <li>- WIR0010-02 (Forfeiture agreement for personally-owned PEDs)</li> <li>- WIR0226 (SWLAN MAC Filtering)</li> <li>- WIR0231 (SWLAN Rekeying)</li> <li>- WIR0401 (Bluetooth Policy and Training)</li> <li>- WIR0931 (Home AP PSK passcode)</li> </ul> </li> <li>- Renumbered checks to highlight their independence from other checks:               <ul style="list-style-type: none"> <li>- WIR0115-03 now WIR0114</li> <li>- WIR0115-04 now WIR0116</li> </ul> </li> <li>- WIR-MOS-PDA-030 renumbered to WIR-MOS-PDA-039 to avoid conflict with changes to WIR-MOS-030.</li> <li>- Made several editorial revisions to Wireless Overview.</li> </ul>	
V6R4	Wireless STIG, V6R3	<ul style="list-style-type: none"> <li>- Fixed typos in the Overview document.</li> <li>- Fixed typos in the Bluetooth STIG (Check WIR0405).</li> <li>- Fixed typos in the PDA STIG (Check WIR-MOS-PDA-030).</li> <li>- Fixed typos in the Wireless Keyboard and Mouse STIG (Check WIR0535).</li> <li>- Included the Wireless Remote Access Policy STIG, which was missing in the previous release.</li> </ul>	28 January 2011
V6R3	Wireless STIG, V6R2	<ul style="list-style-type: none"> <li>- Converted to new XCCDF STIG format.</li> <li>- Added four new checks for the new</li> </ul>	29 October 2010

UNCLASSIFIED

Wireless STIG Revision History, V6R9  
24 October 2014

DISA Field Security Operations  
Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<p>Wireless Access Point (Internet-only Gateway connection) to support devices, such as the iPad that require Internet access but cannot connect directly to the network.</p> <ul style="list-style-type: none"><li>– Separated wireless remote access requirements for laptops and smartphones.</li><li>– Downgraded several CAT I requirements to CAT II to be consistent with current severity category definitions.</li><li>– Deleted two CAT I checks that were applicable to classified PDAs. These requirements are covered in the SME PED STIG.</li><li>– Added information on Cellular Boosters.</li></ul>	