

**DoD Bluetooth Headset Security Requirements Matrix**  
**Version 2.0**  
**April 7, 2008**

Requirement Number	Requirement	Source of Requirement
<p>This matrix was developed by the DISA Field Security Operations (FSO) and is an unofficial compilation of DoD security requirements for DoD Bluetooth headsets and earbuds for use with Blackberry and Windows Mobile handheld devices. The purpose of the matrix is to provide a tool for DISA FSO when evaluating Bluetooth headsets/earbuds. The requirements listed in this document are subject to change as new security vulnerabilities are identified or DoD commands or agencies provide comments to DISA.</p> <p>A copy of this matrix will be provided to DoD commands/agencies and vendors upon request (send an email request to <a href="http://fso_spt@disa.mil">http://fso_spt@disa.mil</a>).</p> <p>See Requirement 25.0 in the <b>DoD Wireless Push Email System Security Requirements Matrix</b> for information on handheld device Bluetooth security requirements.</p> <p><b>Changes from previous version (1.01, 1 Oct 2007):</b></p> <p>-Requirements 1.0, 3.3, and 3.4 have been updated.</p> <p>-Requirement 1.1 was deleted.</p>		
1.0	Bluetooth v1.2 or later should be used.	NSA Bluetooth Security Team
2.0	Bluetooth radios must be Class 2 or Class 3.	NSA Bluetooth Security Team
	Bluetooth Pairing requirements	
3.0	A new randomly-generated PIN at least 8 decimal digits in length should be used for each pairing.	NSA Bluetooth Security Team
3.1	<p>Pairing should be done as infrequently as possible, ideally in a secure area where attackers cannot realistically observe the passkey entry and intercept Bluetooth pairing messages.</p> <p>(Note: A "secure area" is defined as a non-public area that is indoors away from windows in locations with physical access controls.)</p>	NSA Bluetooth Security Team
3.2	The Bluetooth headset/audio gateway device must remain undiscoverable to other Bluetooth devices at all times other than the initial pairing process. It should only support the minimal amount of Bluetooth services required for use as a headset for a handheld device.	NSA Bluetooth Security Team
3.3	Bluetooth Security Mode 3 (link level security) must always be used by both the headset and the audio gateway device along with 128 bit Bluetooth encryption.	NSA Bluetooth Security Team
4.0	Devices should support only a single headset connection between a single headset and a single handheld device/audio gateway device.	NSA Bluetooth Security Team
5.0	User must be able to authorize all initial incoming connection requests and there should be an indication of active Bluetooth link on both the handheld device and Bluetooth headset.	NSA Bluetooth Security Team

<b>Requirement Number</b>	<b>Requirement</b>	<b>Source of Requirement</b>
6.0	<p>Bluetooth stack lockdown techniques should be used on the handheld device to disable unauthorized Bluetooth connections (headset profile and serial port profile are authorized). Unnecessary Bluetooth services, user controls, and applications must be either removed from the handheld device or reliably disabled permanently. (User cannot enable unauthorized Bluetooth services.)</p> <p>Note: This feature may already be included with the handheld device security policy manager.</p>	NSA Bluetooth Security Team
7.0	The security implementation of the headset/earbud shall be Independently reviewed prior to DoD use.	DISA FSO
8.0	The microphone on the headset needs to be turned off by the headset software immediately after the completion of a call and remain off until a new call is initiated or received.	NSA Bluetooth Security Team
9.0	DoD Bluetooth headsets should only be used for telephony functions, not for listening to streaming audio from a media player.	NSA Bluetooth Security Team