United States Trustee Program's
Wireless LAN Security Checklist

In support of a standing trustee's proposed implementation of Wireless Access Points (WAP) in § 341 meeting rooms and courtrooms, the following wireless LAN security checklist must be completed and submitted to the United States Trustee for approval prior to implementation. Completion of this checklist will assist the United States Trustee in determining the strength of the security controls the standing trustee has or will have in place prior to implementation. The checklist reflects guidance provided by the National Institute of Standards and Technology (NIST) on implementing secure WAPs (*see* NIST Special Publications 800-48, "Wireless Network Security," which is available, along with other helpful information, at www.csrc.nist.gov/publications/nistpubs).

The checklist consists of two sections. Section one lists the mandatory security requirements, and requires the signature of the standing trustee to attest that they are in place or will be in place immediately upon approval of the WAP by the United States Trustee. Section two lists best practices which, while not required for approval, are strongly recommended.

Wireless access connections should be regarded in the same manner as any physical Internet connection and protected accordingly. WAPs should never be connected directly to any United States Trustee Program network. All business communications over a wireless or other un-trusted network, such as the Internet, must use a Virtual Private Network (VPN) solution to encrypt all communications. WAPs must be connected to a firewall that only allows access to a VPN service.

WIRELESS LAN SECURITY CHECKLIST FOR STANDING TRUSTEES – SECTION ONE (MANDATORY REQUIREMENTS)				
	Mandatory Security Requirements	**Currently in Place**	**Will be Implemented Prior to Activation**	**Remarks**
1	Security policy that addresses the use of wireless technology, including IEEE 802.11x technologies.			
2	Comprehensive security assessments performed at regular and random intervals (including validating that rogue WAPs do not exist in the IEEE 802.11x WLAN) to fully understand the wireless network security posture.			
3	Default shared keys replaced every 90 days.			
4	Administrator WAP password changed every 90 days or post compromise.			
5	Network users trained in the risks associated with wireless technology.			
6	Complete inventory of all WAPs and IEEE 802.11x wireless devices conducted.			
7	WAPs maintained in secured areas to prevent unauthorized physical access and user manipulation.			
8	When disposing of WAPs no longer required, WAP configuration settings cleared to prevent disclosure of network configuration, keys, passwords, etc.			
9	If the WAP supports logging, logging turned on and logs reviewed on a regular basis.			
10	Default SSID* and default IP address changed in the WAPs.			

WIRELESS LAN SECURITY CHECKLIST FOR STANDING TRUSTEES – SECTION ONE (MANDATORY REQUIREMENTS)				
	Mandatory Security Requirements	**Currently in Place**	**Will be Implemented Prior to Activation**	**Remarks**
11	SSID* character string validated to establish that it does not reflect the trustee's name.			
12	All insecure and nonessential management protocols on the WAPs disabled.			
13	All security features of the WLAN product, including the cryptographic authentication and the strongest encryption algorithm available (WPA2 or better), enabled.			
14	Encryption in use and the encryption key size at a minimum of 256 bits.			
15	All WAPs meet requirements of trustee's internal network security.			
16	"Ad hoc mode" for IEEE 802.11 disabled.			
17	User authentication mechanisms enabled for the management interfaces of the WAP.			
18	MAC filtering enabled and in use.			
19	Anti-virus software installed and latest anti-virus definitions maintained on all wireless clients.			
20	SSL/TLS used for Web-based management of WAPs.			
21	If using SNMP agent, SNMPv3 or equivalent cryptographically protected protocol used to enhance the security of WAP management traffic.			

WIRELESS LAN SECURITY CHECKLIST FOR STANDING TRUSTEES – SECTION ONE (MANDATORY REQUIREMENTS)				
	Mandatory Security Requirements	**Currently in Place**	**Will be Implemented Prior to Activation**	**Remarks**
22	Personal firewall software installed on all wireless clients.			
23	Software patches and upgrades fully tested and deployed on a regular basis.			
24	Security impact of deploying a wireless product fully understood.			

* SSID – Short for ***S****ervice* ***S****et* ***Id****entifier*, a 32-character unique identifier attached to the header of packets sent over a Wireless LAN (WLAN) that acts as a password when a mobile device tries to connect to the Wireless LAN. The SSID differentiates one LAN from another, so all access points and all devices attempting to connect to a specific Wireless LAN must use the same SSID. A device will not be permitted to join the WLAN unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. An SSID is also referred to as a *network name* because essentially it is a name that identifies a wireless network.

I declare that the above information is true and correct to the best of my knowledge and belief. Practices are in place or will be immediately upon activation of wireless devices.

_____ _____

Chapter 13 Standing Trustee Date

WIRELESS LAN SECURITY CHECKLIST FOR STANDING TRUSTEES – SECTION TWO (RECOMMENDED BEST PRACTICES)					
	Recommended Best Practices	**Yes**	**No**	**If "no," plans to implement? By when?**	**Remarks**
1	WAPs turned off when not in use (e.g., after hours and on weekends).				
2	Broadcast SSID* feature disabled in WAPs.				
3	WAP channels at least five channels different from any other nearby wireless networks to prevent interference.				
4	Intrusion detection agents deployed on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.				
5	Technology deployed to analyze auditing records and logs for suspicious activity.				

* SSID – Short for ***S****ervice* ***S****et* ***Id****entifier*, a 32-character unique identifier attached to the header of packets sent over a Wireless LAN (WLAN) that acts as a password when a mobile device tries to connect to the Wireless LAN. The SSID differentiates one LAN from another, so all access points and all devices attempting to connect to a specific Wireless LAN must use the same SSID. A device will not be permitted to join the WLAN unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. An SSID is also referred to as a *network name* because essentially it is a name that identifies a wireless network.

Submitted by:

_____ _____

Chapter 13 Standing Trustee Date