Safeguard Computer Security Evaluation Matrix (SCSEM)

Wireless LAN

Release IV

May 30, 2008

Internal
Revenue
Service

Tester: *Insert Tester Name*
Date: *Insert Date(s) Testing Occurred*
Location: *Insert Location testing was conducted*
Agency POC(s): *Insert each Agency interviewee(s) name, address, phone number and email address.*
Hostname(s): *Insert the hostnames of the device(s) and the purpose of each device.*

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
	AT-1; AT-2; AT-3; AT-4; AT-4, AT-5	Checks to ensure users a trained in awareness of wireless computer security risks.	1. Examine wireless computer security awareness training material. 2. Examine training records of selected users. Note: This can be tested with the MOT SCSEM tests for security training records. This may require an interview with an HR representative depending on who within the agency holds the training records.	1. Material provides basic awareness of the risks associated with wireless technology. 2. Records include the type of instruction received and the date completed.			
	CA-1;	Checks to ensure security assessments are conducted on the wireless network.	1. Examine the results of the last security assessment of the wireless network.	The agency uses wireless security assessment tools (e.g., vulnerability assessment) and regularly conducts scheduled security assessments. The assessments include validating that rogue access points do not exist on the wireless network.			
	RA-5	Checks that a site survey has been completed to measure and map wireless access point coverage.	1. Examine the results of the site survey.	The site survey report contains access point locations, determines coverage areas, and assigns radio channels to each access point and that ensures the coverage range does not expose APs to potential malicious activities.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
	CM-8	A complete inventory of all APs and 802.11 wireless devices should be conducted.	1. Examine the inventory of all wireless access points and 802.11 wireless devices.	An inventory is maintained of all wireless access points and 802.11 wireless devices. The inventory includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner).			
	PL-2; PL4	Wireless networks can not be used until they comply with the agency's security policy.	1. Examine the agency's wireless LAN policy and procedures to verify it is policy that wireless networks must be authorized prior to implementation.	1. The policy states that wireless networks must be authorized by agency officials prior to implementation. Wireless devices must be tested as operating in compliance with the agency's wireless security policy prior to being implemented.			
	IA-3	Checks the location of wireless access points.	1. Examine network diagrams and tour the facility to view the physical location of all wireless access points in the facility.	1. Wireless access points are located on the interior of the facility and not located near exterior walls or windows. Wireless access points are located in out of reach, secured areas, such as restricted telecommunications closets, to prevent unauthorized physical access and user manipulation.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
	AC-17	Checks the range boundaries of wireless coverage areas.	1. Review the site survey report and network diagrams to verify the location of each AP and coverage areas. 2. Select a sample of APs and attempt to connect to the wireless network from inside and outside of the documented coverage areas.	A wireless connection is only successful inside the documented coverage area.			
	AC-12	Checks to ensure access points are turned off when not in use.	1. Examine the agency's wireless LAN policy and procedures to verify it is policy to turn off wireless access points when they are not in use (e.g., after hours, weekends). 2. Select an AP that is not in use to verify that access point services are not running. Attempt to connect to the access point.	1. The policy states that wireless access points are to be turned off when not in use. 2. The connection attempt to the access point fails. Access point services are not running.			
	AC-12	The reset function on APs should be used only when needed, and the latest security settings are applied after its use.	1. Examine the agency's wireless LAN policy and procedures to verify it covers use of the access point reset function.	1. The policy states that the reset function is only used when needed, and is restricted to authorized personnel. Appropriate personnel restore the latest security settings after a reset.			
	CM-2; CM-3	The default SSID should be changed in the access point.	1. Examine wireless access point configuration, SSID name setting.	1. The SSID has been changed to a value other than the default value for the access point. 2. The SSID character string does not reflect the agency's name, or any other identifying information of the agency.			
	CM-2; CM-3	The broadcast SSID feature should be disabled.	1. Examine wireless access point configuration, SSID broadcast setting.	The broadcast SSID feature is disabled.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
	SA-2	Checks to ensure access points are protected against radio interference from nearby wireless networks.	1. Examine the agency's site survey report to determine the channels used by each wireless network within the agency. 2. For a selected sample of access points, examine the wireless access point configuration, wireless channel setting.	1. Channel for each wireless network is documented in the site survey report. 2. AP channels are at least five channels different from any other nearby wireless networks to prevent interference. The channel settings match what is documented in the site survey report.			
	CM-6	All insecure and nonessential management protocols on the APs are disabled.	1. Examine the wireless access point configuration to verify that insecure and non essential protocols are disabled.	All insecure and nonessential management protocols, (e.g., telnet, FTP) on the APs are disabled.			
	CM-6	Checks to ensure encryption keys are properly configured and controlled.	1. Examine the wireless access point configuration, encryption key settings. 2. Examine documented records of encryption key changes.	1. The agency has changed the shared key from the default setting because it is easily exploited. 2. The encryption key size is at least 128-bits. 3. Cryptographic keys are replaced periodically, and when there are personnel changes, with more secure unique keys. Key changes are tracked and documented.			
	SC-7	A properly configured firewall must exist between the wired infrastructure and the wireless network (AP or hub to APs).	1. Examine the network architecture diagram.	1. A firewall is present that separates the agency's wired network from the wireless network.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
	SI-3; SI-8	Antivirus software is installed on all wireless clients.	1. Examine selected wireless clients to verify the existence of anti-virus software.	Antivirus software is installed on the wireless clients to ensure that wireless client do not introduce known worms and viruses to the wired network while protecting the wireless client from viruses that originate on the wired network.			
	SC-7	Personal firewall software is installed on all wireless clients.	1. Examine selected wireless clients to verify the existence of personal firewall software.	1. Personal firewall software is installed on wireless network clients.			
	AC-3	File sharing on wireless clients is disabled.	1. Examine selected wireless clients to verify if file sharing is enabled.	File sharing is disabled on the wireless clients.			
	IA-3; CM-8	MAC access control lists must be deployed.	1. Examine the wireless access point configuration, MAC address access control list. 2. Attempt to access the wireless access point with a client that is not on the authorized MAC address access control list.	1. The MAC address access control list is populated with authorized clients only. 2. The attempt to access the access point fails.			
	CM-4	Software patches are deployed and tested regularly.	1. Review the records containing installation, configuration and testing of software patches. 2. Examine the wireless access point configuration, patch level.	1. Records indicate that software patches are deployed and tested regularly. 2. The wireless access point is current with the vendor's patch level.			
	CM-4	Software upgrades are deployed and tested regularly.	1. Review the records containing installation, upgrade and testing information of software upgrades.	The records will show that software upgrades, installations, and testing is performed regularly.			
	AC-3; IA-2	All APs must have strong administrative passwords.	1. Review documentation that provides admin password standards.	The records will explain that strong passwords are to be used. (e.g. min length of 8 characters, use of numeric and special characters)			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
	AC-13	All passwords should be changed regularly.	1. Review documentation the explains the expiration intervals of passwords.	The documentation will explain when passwords automatically expire.			
	CM-2; CM-3	Where possible “ad hoc mode” for 802.11 should be disabled.	1. Review the AP configuration files and verify that ad hoc mode is disabled by default.	Ad hoc mode will only be enabled as needed.			
	CA-3; SC 20	The wireless network should use static IP addressing.	1. Examine the wireless access point configuration to ensure that DHCP is not enabled.	The AP is not configured to use DHCP, static ip addresses are used instead. Using static IP addressing makes it more difficult for a hostile user to connect to the network.			
	IA-2; CM-6	User authentication mechanisms for the management interfaces of the AP should be enabled.	1. Examine the wireless access point configuration to ensure the management interface use some kind of authentication mechanism. (e.g. username and password)	Connection to the AP's management interface requires authentication.			
	CA-3	Management traffic destined for APs should be on a dedicated wired subnet.	1. Review the detailed network diagram.	Management traffic destined for APs will be on a dedicated wired subnet. Passing management traffic over an “out of band’ network or management subnet protects management traffic, interfaces, and passwords from organizational and outside users.			
	SC-14; SC-13	Web-based management session should use SNMPv3 and/or SSL/TLS.	1. Review the session audit logs and verify that SNMPv3 and/or SSL/TLS is enabled.	SNMPv3 and/or SSL/TLS will be enabled.			
	AC-6	SNMP settings on APs are configured for least privilege (i.e., read only).	1. Review AP configurations files and verify that least privilege principle are utilized. For example, users are configured with read only privileges.	SNMP settings on APs are configured for least privilege (i.e., read only).			
	CM-2	SNMP is disabled if not used.	1. Review configuration files and verify that SNMP is disabled by default.	SNMP will be disabled by default.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
	CM-2	SNMPv1 and SNMPv2 are not to be used.	1. Review AP configuration files and verify that SNMPv1 and SNMPv2 are not enabled.	No AP will have SNMPv1 and SNMPv2 enabled. SNMPv1 and SNMPv2 message wrappers support only trivial authentication based on plain-text community strings and so are fundamentally insecure and not recommended. Agencies should use SNMPv3			
	CA-3; SC-13	SNMPv3 or FIPS-140-2 compliant encryption should be used to manage AP traffic.	1. Review the configuration files and check the that SNMPv3 or FIPS-140-2 compliant encryption is enabled.	SNMPv3 or FIPS-140-2 compliant encryption will be enabled.			
	CM-6	A local serial port interface may be used for AP configuration.	1. Connect to an AP using local serial port interface.	A connection to the local serial port interface should be allowed for AP configurations. By using a local serial port interface for AP configuration ensures that sensitive management information do not traverse the network as well as minimizing the risk of unauthorized users gaining access via a network protocol used to manage the AP.			
	IA-7; SC-12	RADIUS and Kerberos are acceptable forms of authentication for the wireless network.	1. Review the local security policies for the possible application of RADIUS or Kerberos.	There will be written documentation stating that RADIUS and Kerberos are acceptable forms of authentication.			
	AU-2	If an authentication mechanism such as RADIUS is utilized, then auditing technology is also used to analyze the records produced by RADIUS.	1. Obtain and review the audit logs that can trace RADIUS connections.	An audit log of RADIUS connections is maintained.			
	CA-3; CA-7; AU-2; AU-6	Intrusion detection is applied to the wireless portion of the network.	1. Review Intrusion Detection logs and verify that traffic is captured for the wireless network.	Wireless traffic will be captured in the audit logs.			
	SC-12	Key-mapping keys (802.1X) rather than default keys should be utilized for sessions.	1. Review the encryption configuration files and/or session logs to verify that 802.1x is enabled.	Key-mapping key (802.11X) are used by during sessions.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
	PL-2; PL-6	The impacts of deploying any security feature or product must be understood prior to deployment.	1. Review the process that takes place prior to deployments.	There will be meetings, procedures and plans that occur before there is a deployment.			
	CM-4; AU-3	There should be a policy and audit record guiding the installation of releases to 802.11 WLAN technologies that incorporate fixes to the security features, or provide enhanced security features.	1. Review the logs that contain any new 802.11 WLAN that has been installed/upgraded.	There will be a log containing 802.11 upgrade information and what feature was enhanced.			
	MP-6	When disposing of access points, access point configuration should be cleared.	1. Review the procedure followed when disposing of access points.	The procedure will clear access point configuration information.			
	AU-6	If the access point supports logging, this feature must be enabled and reviewed regularly.	1. Review the access point configuration files to verify that logging is enabled.	If the access point logging feature is enabled, there will be a record kept that verifies that the logs are reviewed regularly.			

IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence. Please find more details of each below.

Test ID	Identification number of SCSEM test case
NIST ID	NIST 800-53/PUB 1075 Control Identifier
Test Objective	Objective of test procedure.
Test Steps	Detailed test procedures to follow for test execution.
Expected Results	The expected outcome of the test step execution that would result in a Pass.
Actual Results	The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail	Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence	Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the information is provided. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible). Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.

Version	Release Date	Summary of Changes	Name
0.1	5/30/2008	First Release	