

**INDEX TO INTERNAL AUDIT PROGRAM  
INFORMATION SYSTEMS  
WIRELESS LOCAL AREA NETWORK (WLAN) REVIEW**

<b><u>Item</u></b>	<b><u>Description</u></b>	<b><u>Page</u></b>
1.	Network Overview.....	1
2.	Network Communication and Security.....	1

## **WIRELESS LOCAL AREA NETWORK (WLAN) REVIEW**

Objective: Security is about reducing risk not eliminating it. In most cases, elimination is not possible. The purpose of this review is to evaluate the controls and precautions we are implementing to stop the casual to mid-level attacker from accessing or obtaining information from the Association wireless 802.11b network.

### **1. Network Overview**

A. Obtain an understanding for the WLAN being reviewed.

- Identify the wireless network protocols being employed within the Association (i.e., 802.11b).
- Determine the purpose of WLAN and that management's approval was given (i.e., vendor demos requiring internet access, etc. this then could help restrict or focus access (vpn or mac acl)).
- Determine which sites within the Association have been selected to utilize a WLAN.
- Perform a perimeter check to identify any external Basic Service Station (BSS) unit that might overlap the Association's (risk is that our network could become an inadvertent distribution system from nearby networks).
- Obtain a list of the manufacturer, type of all Access Points (AP) in use.
- Determine the peripheral connections, if any (shared disks, printers, etc.).
- Obtain a schema or locational listing of all known/approved wireless networks and their associate IP address ranges.

### **2. Network Communications and Security**

A. Ensure that adequate controls exist over information transmitted to and from the AP. Sensitive data should be protected from being changed or intercepted.

- Determine if APs are secured from unauthorized access.
- Ensure sufficient guidelines, procedures and standards have been developed to assist in the proper implementation of future wireless systems.



## **WIRELESS LOCAL AREA NETWORK (WLAN) REVIEW**

- Obtain a list of users that have admin rights and support the WLAN.
- Determine if your BSS extends beyond the physical walls of the building (note, therefore, BSS should be found at core of building away from public areas also).
- Ascertain if authentication to an AP requires more than a simple handshake (inquire if Cisco LEAP or Radius technologies have been employed to ensure unauthorized user cannot connect to the network).
- Ensure that sufficient policies and guidelines have been established within the information systems user policy manual.
- Determine if, at minimum, Wired Equivalent Privacy (WEP) been enabled.
- Determine if alternative encryption/security schemes such as IPSec and secure socket layer are employed to compensate for WEP weakness.
- Determine if Virtual Private Network (VPN) is used on the wireless networks to further protect and segregate them from the wired network.
- Review the password and connection settings to ensure that these objects are appropriately secure.
  - Has the AP beacon been disabled? (or if not, an explicit option set interval to 0).
  - Disable DHCP?
  - Ensure that default SSIDs or AP passwords have been changed.
  - Ensure that signal strength is not excessive to properly perform function. (Weaker signal small traveling range).
  - Ensure that comments and naming conventions do not identify Astoria Federal Savings nor provide helpful information.
- Ascertain if the wireless network is monitored for unauthorized connections or stations.
  - By whom?
  - How often?
  - What tools are used?
  - What are the procedures followed if an unauthorized site is found?

## **WIRELESS LOCAL AREA NETWORK (WLAN) REVIEW**

- Ascertain if the Association facilities are checked for rogue wireless networks.
  - By whom?
  - How often?
  - What tools are used?
  - What are the procedures followed if an unauthorized site is found?