Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G530 – WIRELESS LOCAL AREA NETWORK (LAN) SECURITY

CONTENTS:

I. DEFINITION

There is no definition for this guideline.

II. RATIONALE

These guidelines are intended to improve the security of wireless networks for the State of Idaho.

III. GUIDELINE

There is no guideline for this guideline.

IV. PROCEDURE REFERENCE

Policies for mobile devices are detailed in ITA Information Technology Enterprise Policies *P4540 – Wireless Security for State Local Area Networks.*

V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876.

VI. INTRODUCTION

1. Wireless networking technologies are revolutionizing business and government operations. Through the use of wireless, organizations are better equipped to provide information access to their customers and employees – anytime, anywhere. Based on many independent studies, wireless technologies increase employee productivity, reduce costs, enhance accuracy, increase flexibility, and boost employee satisfaction.

   A. 63% of end-users report that wireless LAN technology improves the accuracy of every day tasks;

   B. 51% of healthcare organizations find significant improvements in accuracy when using wireless technology;

   C. 87% of wireless users believe wireless LAN's improve their quality of life, taking into account attributes such as increased flexibility, productivity and time savings;

   D. 92% of organizations realized a definite economic and business benefit after installation of wireless LAN's; and

   E. On average, wireless LAN users are connected 1¾ hours more per day, making them as much as 22% more productive than non-wireless LAN users.

   Additionally, wireless LAN technologies are typically very cost-effective to deploy versus traditional wired infrastructures. The obvious savings of wireless networks over hard-wired networks are in the installation of cabling infrastructure (of lack thereof). However, additional savings can be realized by lowering support costs, particularly by simplifying the "add, move, and change" process associated with hard-wired networks.

2. While the benefits of wireless networking are very stimulating, we must be extremely sensitive to the risks associated with this new technology. In particular, **security must be a foremost concern in any organization deploying wireless networks**. The threat to an organization with an improperly secured wireless network is very real and could impact the State's enterprise as a whole if not addressed appropriately. Without proper security precautions, intruders can freely access your wireless network, and potentially inflict damage to systems on your wired network. If your wireless network is not secured, the intruder can easily access your data, monitor your network traffic, inflict down-time to your business operations, or illicitly use your network.

   The purpose of this document is to provide a minimum set of guidelines for agencies to consider when deploying a wireless network. If the wireless network is connected to the State's wired infrastructure, agencies are **highly encouraged** to adopt the appropriate countermeasures to protect their network from being

compromised. As the old cliché states, “We are only as strong as our weakest link.”

We recognize that each agency must conduct its own risk assessment when installing a wireless network; therefore, the recommended countermeasures may apply in some instances and not in others. However, the guidelines provided throughout this document will greatly simplify your effort in completing this risk assessment by providing you with a detailed list of threats, vulnerabilities, and countermeasures to consider. The purpose of your wireless network will greatly influence your risk assessment and the resulting level of security that should be implemented. For instance, if you are deploying a wireless network in your training facility that is *not* connected to your agency’s wired network, then the security countermeasures may be less stringent than if you are deploying a network that *is* connected to your wired infrastructure. To accommodate these different types of wireless network deployments, the *Recommended Security Guidelines* section of this document provides four (4) separate recommendations. Instead of providing a “one-size fits all” solution, these guidelines are designed to provide recommended security controls for the following types of wireless network deployments:

A. Public Wireless LAN – Provides wireless access unrestricted to anyone;

   (1) *Possible example:* Stand-alone, publicly-accessible wireless network for citizen access.

B. Open Wireless LAN – Limits wireless access to pre-authorized users with no attempt to keep communications private;

   (1) *Possible example:* Agency’s stand-alone training network.

C. Private Wireless LAN – Limits wireless access to pre-authorized users with “due diligence” to keep communications private; and

   (1) *Possible example:* Agency wireless network for employees.

D. Trusted Wireless LAN – Limits wireless access to pre-authorized users with assured private communications.

   (1) *Possible example:* Agency wireless network for employees that are handling sensitive information.

We encourage you to look at the benefits of wireless networks and how they can enhance your agency’s operations. However, ***while you are investigating the possibility of wireless, consider security from the start***. It is our hope that these set of security guidelines can be of assistance to you in this process. The security of your wireless network(s) is paramount – both to your agency and to the State’s enterprise network.

"Of 500 firms recently polled by Jupiter Research, less than half have implemented security solutions for their wireless networks."

-- PC Magazine, Fall 2003

VII. WIRELESS NETWORKS – AN OVERVIEW

Wireless technology, and specifically the wireless local area network (LAN), is continually evolving. However, the basic technology and concepts have been around for years. This section provides a general overview of wireless LAN components for those who are not familiar with this technology.

1. Types of Wireless Technology – Many different types of wireless technologies are available, depending upon the need of the individual and organization. The three most common forms of wireless technologies for computers are infrared, Bluetooth, and Wi-Fi (802.11).

   A. *Infrared* is a basic, short-range wireless technology that has a range of 10 feet with a maximum throughput of 4 Mbps. Typically, infrared is used to synchronize data between handheld devices and other computers.

   B. *Bluetooth* operates in the 2.4-GHz spectrum and usually has a range of 30 feet, with a maximum throughput of 720 Kbps. Bluetooth is often used for short-range wireless needs and is popular for wireless connections with a printer, keyboard or mouse.

   C. *Wi-Fi* is the term often used to describe wireless technologies based upon the IEEE 802.11 standards. (In the industry, the term Wi-Fi is more appropriately used to refer to 802.11 products that have been certified by the Wi-Fi Alliance.) The 802.11-based products operate either in the 2.4-GHz or 5-GHz spectrum with data rates ranging from 11 to 54 Mbps. A full explanation of the 802.11 wireless standards can be found in Appendix A (*Guide to 802.11 Wireless Standards*).

   For the purposes of this document, the guidelines are focused on the implementation of 802.11-based wireless technologies.

2. Wi-Fi (802.11) Wireless Networks Explained – A wireless network essentially sends radio-frequency signals between computers to share information. In wireless networking, a point-to-point architecture would enable a computer to communicate directly with another computer. This is often referred to as *ad hoc mode*, in which a direct peer-to-peer connection between the end-user wireless devices (e.g., laptops, computers, PDA's) is permitted.

   For the purposes of this document, a wireless network would be more similar to a client/server architecture (often referred to as *infrastructure mode*), in which a

key component of the architecture includes a wireless *access point (AP).* The end-user wireless devices would communicate with the access point. The access point then essentially acts like a wireless switchboard, connecting wireless devices (e.g., laptops, PDA's, etc) to each other. In some cases, the AP interconnects the wireless network with the organization's existing wired network, enabling the wireless users to access resources on the wired network or Internet.

To communicate with the wireless network, each end-user's device (e.g., laptop, computer, PDA, etc.) requires a *wireless network interface adapter* (often referred to as a *PC Card*). Today, many portable computers are now equipped with a wireless network interface built into the system. The wireless network adapter enables the end-user device to communicate with the AP or other wireless devices.

In more advanced architectures, a *wireless switch* may be preferred to allow centralized management of security, quality of service, and the ability to easily control the wireless environment. A switch-based wireless LAN architecture reduces the access point to a "dumb radio frequency terminal" and transfers the security and management features to the switch.

With this basic understanding of wireless technologies, we are ready to begin the discussion of why we need to be very concerned about security when deploying wireless networks.

VIII. WHY DO YOU NEED TO SECURE YOUR WIRELESS NETWORK?

Although wireless technologies offer significant benefits, the risks related to these technologies are significant. Prior to deploying wireless LAN's, agencies should address the unique security challenges associated with this new technology. Many of the current wireless protocols and products do not provide adequate protection, thereby requiring agencies to understand wireless security issues and the available methods to enhance the protection of their wireless networks. To a large extent, the risks associated with wireless LAN's can be minimized; however, the appropriate risk mitigating controls may require a tradeoff between ease of use, costs, and available technology. Like any maturing technology, the industry is aggressively working to develop new protocols and technologies to ensure wireless is more secure. With that in mind, some agencies may want to consider waiting for these more mature and secure solutions. However, for those who desire to move forward in the near term, a firm understanding of the security issues and risk mitigation options should be understood.

The wireless LAN environment is riddled with vulnerabilities. Without security enhancements or configuration changes, wireless devices and their transmissions may be wide open to compromise. A complete list of threats and vulnerabilities to the wireless LAN is described in a later section (see *Threats and Vulnerabilities*). However, to provide a general understanding of the vast security issues associated

with wireless, the following list[1] provides a high-level summary of the threats and vulnerabilities that you should be aware of:

1. Malicious persons may gain unauthorized access to an agency's computer network through wireless connections, bypassing any existing security perimeter protections (e.g., firewalls);

2. Sensitive information that is not encrypted and that is transmitted between two wireless devices may be intercepted and disclosed;

3. Weak encryption within existing wireless technologies may be bypassed and/or cracked, leading to disclosure of sensitive information;

4. Denial of Service (DoS) attacks may be directed at wireless connections or devices, rendering the systems and/or network unusable;

5. Malicious entities may deploy unauthorized equipment (e.g., end-user wireless devices or access points) to surreptitiously gain access to sensitive information;

6. Data may be extracted without detection from improperly configured devices;

7. Viruses or other malicious code may corrupt data on a wireless device and be subsequently introduced to an agency's wired network;

8. Intruders may, through wireless connections, connect to other agencies or organizations for the purposes of launching attacks and concealing their activities;

9. Malicious entities may use third-party, untrusted wireless network services to gain access to an agency's or other organization's network resources; and

10. Internal attacks may be possible via ad hoc transmissions.

As you can see from the list above, wireless threats and vulnerabilities are evident. Without taking appropriate action, an agency can expose themselves to unnecessary risks. An agency would never think of installing an unsecured, wired network "drop" outside the front door of the building – available for anyone to use with no questions asked; however, unsecured wireless access is virtually the same result – except with wireless, the intruder can have complete access to your information and be essentially undetected.

For a complete review of wireless networks and associated security issues, please reference Appendix B, *Wireless Security Resources*.

IX. THE NEED FOR A RISK ASSESSMENT

[1] Tom Karygiannis, Les Owens, *NIST Special Publication 800-48: Wireless Network Security*, November 2002 < http://csrc.nist.gov >, pp 2-5, 2-6

Prior to implementing a wireless network, the agency should complete a full risk assessment. The risk assessment will enable the agency to define their risks with deploying a wireless network and determine what actions they should take. Furthermore, the risk assessment is a process that allows the agency to balance operational and economic costs of implementing certain security measures with the resulting gain in mission effectiveness by deploying wireless technologies. The goal of the risk assessment is to investigate the threats, vulnerabilities, and risk mitigating controls (or countermeasures) and determine the appropriate balance to protect the agency's information, systems, and network. By going through this risk assessment process, the agency will be able to:

1. Determine the risk of deploying a wireless LAN;

2. Determine whether this is an acceptable risk; and

3. Identify the security controls that should be implemented to reduce the risk.

In order to assist agencies in the completion of a wireless LAN risk assessment, the subcommittee has completed a comprehensive template of a risk assessment for wireless networks (see Appendix C, *802.11 Wireless Network Risk Assessment Form*). The risks of deploying a wireless network will be different agency to agency, depending upon the sensitivity of the information to be protected and the purpose of the network to be deployed. The Committee has completed a majority of the "homework" for you by identifying the potential threats, vulnerabilities, and risk mitigating controls for wireless networks. Therefore, agencies are encouraged to use this template as a starting point for their wireless network risk assessment process.

To fully understand the risk assessment process used by the Committee, please reference Appendix D, *Risk Assessment Guidelines*. These guidelines outline the risk assessment methodology used by the Committee. We would like to thank the Idaho State Tax Commission for allowing us to use their risk assessment methodology.

> **A risk assessment is a "fundamental activity that allows an organization to manage its information security risks in a cost-effective manner rather than reacting to individual problems in an ad-hoc manner only after a problem has been detected."**
>
> - U.S. General Accounting Office

X. THREATS AND VULNERABILITIES

1. Wireless threats and vulnerabilities are very real. Intruders are actively exploiting weaknesses within wireless networks for malicious purposes. This section

provides a detailed description of the most common wireless threats and vulnerabilities. These threats and vulnerabilities can essentially be classified into four (4) separate categories:

A. Passive Wireless Attacks – Non-intrusive attack which gives an intruder access to information transmitted on the wireless network or ability to use the network without authorization;

B. Active Wireless Attacks – Intrusive attack in which the intruder intends to alter, destroy, intercept, or disrupt wireless communications;

C. Negligence or Unintentional Threats – Unintentional situations or misconfigurations which expose the wireless network to unnecessary security risks; and

D. Specific Wireless Vulnerabilities – Existing wireless technology problems that can be compromised to enact a passive and/or active attack.

2. Passive Wireless Attacks

A. Eavesdropping – In a wireless network, eavesdropping is easy because wireless communications are not easily confined to a physical area. A nearby attacker can receive the radio waves from the wireless network without any substantial effort or equipment. All frames sent across the wireless medium can be examined in real time or stored for later examination.

To connect with wireless LAN's from distances greater than a few hundred feet, sophisticated hackers use long-range antennas (that are either commercially available or home built) and can pick up 802.11 signals from up to 2,000 feet away. The complete kit costs about $160.

B. Illicit Use – Any individual associated to a wireless access point can connect to the networks that live behind the access point. Illicit use may not cause any operational problems, but it still may be unwanted and unlawful use. The individual may simply be someone who drove up near the access point, associated to it to check his mail. Alternatively, they may be sending spam to thousands of e-mail addresses. In a malicious scenario, the individual may even be attempting to exploit a server that lives on the accessible networks or use the access point as a mask to hide the source of illegal actions, such as hacking other networks.

3. Active Wireless Attacks

A. Wireless Jamming Denial-of-Service Attack – The 802.11 specifications define a limited range of frequencies for communication. An attacker can create a device that will saturate the 802.11 frequency bands with noise. If the attacker can create enough RF noise to reduce the signal-to-noise ratio (SNR) to an unusable level, then the devices within range of the noise will be

effectively taken offline. The devices will not be able to pick out the valid network signal from all of the random noise being generated and, therefore, will be unable to communicate.

Creating a device that produces a lot of noise at 2.4 GHz is relatively easy and inexpensive to construct. However, there are several common commercial devices available today that can easily take down a wireless network. Unfortunately, many 2.4 GHz cordless phones that can be purchased in electronics stores have the capability to take an 802.11b wireless network offline. While not a refined electronic weapon, these phones can interfere or completely disable a WLAN. Cordless phones use several different modulation techniques and can overlap on the frequencies used by 802.11b. This overlapping is simply noise to an 802.11b wireless network device. The cordless-phone-induced noise can drop the SNR enough to bring down any WLAN network nearby.

B. Data-Link Layer Denial-of-Service (DoS) Attack – A data-link DoS can target either a host or a network. Data-link attacks disable the ability of hosts to access the local network. An example of this would be flooding a non-switched Ethernet network with invalid frames. An attacker (or sometimes a malfunctioning network interface card) can send repeated frame headers with no payload. These headers are rebroadcast to all hosts on the network and effectively tie up the medium. Data-link DoS attacks are not common on wired networks because most networking gear has the intelligence to prevent data-link attacks from propagating to hosts on the network.

   However, unobstructed access to the wireless medium again creates new opportunities for these types of DoS attacks. Even with Wired Equivalent Privacy (WEP) algorithm turned on (which provides encryption for transmitted information), an individual has access to the link layer information and can perform some DoS attacks. Without WEP, the individual has full access to manipulate associations between end-user devices and access points and can terminate access to the network.

C. Network Layer Denial-of-Service Attack – A network-layer DoS is accomplished by sending a large amount of data to a network. This type of attack targets the network infrastructure. For example, an attacker may send 100 Mb/s of data to a network that can only transmit 10 Mbps. The network obviously cannot retransmit all the data being sent to it, so the network equipment is forced to drop packets. This excessive traffic may also cause high loads on the CPU's within the network equipment itself, causing further network problems.

   A typical network-based DoS attack is a ping flood. An attacker generates massive amounts of Internet Control Message Protocol (ICMP) traffic destined for the victim network. (ICMP packets are used for management functions such as querying the availability and services of a host.) This

usually saturates the victim's network links. By cutting off the victim's LAN from the rest of the Internet, the attacker has denied access to any services that reside on the victim's network.

When a wireless access point allows any client to associate, it is vulnerable to a network-level DoS attack. Since an 802.11 network is a shared medium, a malicious user can flood the network with traffic, denying access to other devices associated with the affected access point. As an example, an attacker can associate to an 802.11 network and send an ICMP flood to the gateway. While the gateway may be able to withstand the amount of traffic, the shared bandwidth of the 802.11 infrastructure is easily saturated. Other clients associated to the same AP as the attacker will have a very difficult time sending packets.

D. Manipulation – Address Resolution Protocol (ARP) is the mechanism that IP-enabled Ethernet devices use to determine which device on a network has a particular IP address. An attacker can force packets to go through a malicious host by poisoning the ARP mechanism. This “man in the middle” can watch, drop, forward, and manipulate data moving between the client and the server.

   A wireless attacker can intercept traffic between any hosts on the same broadcast domain, regardless if they are wired or wireless by using ARP poisoning.

E. Access Point Hi-Jacking – Simple Network Management Protocol (SNMP) agents are often used on wireless access points for configuration and monitoring. If not configured correctly, individuals with wireless access can easily reconfigure the wireless access point (AP) using SNMP to operate the AP as desired.

F. Theft or Re-configuration – Manufacturers always provide methods for those in physical possession of access points to reset and reconfigure the access points. This makes them a popular item to steal or replace with an access point configured to the intruder’s preferences.

G. Media Access Control (MAC) Spoofing – One suggested method to improve wireless security is to use MAC access lists. Host identification based on an authorized list of MAC addresses provides a low level of security, but MAC addresses were never intended to be used in this manner. Any attacker can easily change the MAC address on their host to impersonate a valid station or access point.

H. Hostile, Rogue Access Points – Using widely available tools, such as HostAP, hackers can force end-user wireless network adapters to connect to an undesired 802.11 network or alter the configuration of the end-user device to operate in ad-hoc networking mode.

A hacker begins this attack by using freeware software (HostAP) to convert the attacking end-user device to operate as a functioning access point. As the victim's system broadcasts a probe to associate with an access point, the hacker's new malicious access point responds to the victim's request for association and begins a connection between the two. After providing an IP address to the victim's workstation (if needed), the malicious access point can begin its attacks. The hacker - acting as an access point - can use a wealth of available hacking tools available that have been tested and proven in a wireless environment. At this point, the hacker can exploit all vulnerabilities on the victim's system, which can include installing the HostAP firmware or any other laptop configuration.

4. Negligence or Unintentional Threats

   A. Non-Hostile, Rogue Access Points – The consumer market for wireless access points makes wireless access points and wireless LAN cards very inexpensive. In an attempt to foster the consumer market, these devices have been made “plug and play.” In an effort to improve productivity or flexibility, an employee may install an unauthorized access point. If this access point is plugged into an office Ethernet jack, it will provide access to the trusted network without safeguards for anyone within range of the access point.

      Additionally, a wireless LAN card in “ad hoc” mode will provide access to any network that the host is connected to without providing safeguards for the network.

   B. Interference from Other Networking Protocols – In particular, Bluetooth uses the same Industrial, Scientific and Medical (ISM) band as 802.11b and 802.11g. The direct-sequence spread spectrum (DSSS) modulation in 802.11b is susceptible to interference from the modulation used in Bluetooth networks. While there are potential solutions to prevent Bluetooth from stepping on 802.11b transmissions, large-scale Bluetooth deployments may still interfere to the point of inoperability with 802.11b networks. As time passes, the 2.4 GHz ISM band will become more crowded, making unintended DoS attacks against 802.11b networks commonplace. For instance, Sirius and XM satellite radio, who have spectrum bordering the ISM band, have complained that ISM-band devices may cause interference with their ground based repeaters and satellites.

   C. Routing Between Trusted and Untrusted Networks – A host can be connected to other networks at the same time it is connected to the wireless network. Since both Windows and Linux provide routing features, this may expose the hosts on the trusted network to all of the hosts on the other “unknown” networks.

D. Misconfigured Virtual Private Network (VPN) – A possible layer of security with a wireless network is to use a VPN solution. By design, VPN connections are designed to provide a trusted connection over an untrusted network to a private network. However, improper configuration of the connecting host can inadvertently expose the trusted network to hosts on the untrusted network.

E. Lack of Education – Most systems/network administrators are not anywhere near up to speed on 802.11 security protocols. Security procedures are still being developed and changing as new technology and protocols are introduced, giving quick-learning hackers the edge. New wireless LAN hacking tools are introduced every week and are widely available on the Internet for anyone to download.

F. Misconfigured End-User Devices – Misconfigured host wireless devices can inadvertently expose the host system and the WLAN to eavesdropping and/or hijacking.

G. Unintentional Network Layer Denial-of-Service Attack – Given the relatively slow speed of 802.11b networks, a network DoS may happen inadvertently due to large file transfers or bandwidth-intense applications. A few bandwidth-hungry applications on a WLAN can hamper access for all associated stations. With the deployment of higher-speed WLAN technologies, these unintentional attacks will become less frequent.

5. Specific Wireless Vulnerabilities

A. Wired Equivalent Privacy (WEP) Weaknesses – WEP has been proven ineffective as a means to encrypt data. WEP was quickly broken by published tools (such as WEPCrack and AirSnort), which exploit vulnerabilities in the WEP encryption algorithm. WEPCrack or AirSnort passively observe WLAN traffic until it collects enough data by which it recognizes repetitions and can then break the encryption key. Once the encryption key is broken, the tool can then assist the intruder to monitor all transmissions.

B. Weak Authentication – The designs of both open and shared-key 802.11 client authentication is weak. Open authentication simply involves providing the correct Service Set Identifier (SSID). Shared-key authentication (which uses a shared WEP key) is vulnerable since a malicious user can decipher the shared WEP key (by intercepting the clear-text challenge and the same challenge encrypted with the WEP key).

C. Evolving 802.11 Standards – The 802.11 standards are not complete (See http://grouper.ieee.org/groups/802/11/). Known vulnerabilities with the finalized standards have led numerous vendors to develop enhancements that are not in the 802.11 standards. The resulting products may not

interoperate with each other or, in the worst case, may interoperate at a lower feature set that requires incomplete deployment of the desired security features.

These threats and vulnerabilities may seem overwhelming; however, the next section provides specific, practical solutions to minimize these security risks. With a firm understanding of your vulnerabilities, you can make logical decisions on which risk mitigating controls are appropriate for your environment.

XI. RISK MITIGATING CONTROLS (COUNTERMEASURES)

Risk mitigating controls (or countermeasures) are those policies, procedures, or technologies that can be employed to minimize the risks of the threats and vulnerabilities associated with a wireless network. The types of controls that an agency should employ will be largely dependent upon the purpose of the wireless network. For instance, if you are deploying a stand-alone wireless network for a training room, the security controls may be minimal. However, if you are deploying a wireless network in your conference room for personnel to be able to access files from your agency's file servers on your wired network, the controls would be much more stringent.

The following list of risk mitigating controls is provided as a "menu" for an agency to consider when architecting their wireless network. While implementing all of the following controls may help an agency achieve maximum protection, the agency should weigh the benefits and costs before implementing each option. In the next section, "Recommended Security Guidelines", we have recommended specific controls for common wireless network deployments. Additionally, in Appendix C (*802.11 Wireless Network Risk Assessment Form*), these risk mitigating controls have been correlated to the specific threat and/or vulnerability that they address. This correlation should greatly assist you during your risk assessment process to ensure that you are considering the appropriate risk mitigating controls for each threat and/or vulnerability that may apply to your environment.

1. Possible Risk Mitigating Controls to Minimize Wireless Network Security Risk

   A. Use Encryption – Implement several layers of encryption to obscure transmitted data in an effort to prevent attackers from gleaning useful information from the network traffic. At a minimum, enable the highest level of WEP (Wireless Encryption Protocol) that ships with the access point. At a minimum, use 128 bit encryption. (**NOTE**: WEP has several weaknesses and has been proven to be "broken" easily; however, simply having it enabled may turn away an intruder or curious person.)

   B. Separate the Wireless Network from Your Trusted Wired Network – Place access points on separate subnets and put a stateful packet inspection firewall between that subnet and the trusted network.

C. Change Default Service Set ID (SSID) Settings – Change the default SSID that ships with your access point. Do not use information in the SSID that would associate your agency or location with the access point.

D. Change the Default Administrator Password – Change the default administrator's password on the access point

E. Do Not Broadcast the Access Points Identification – Disable the "broadcast" mode in which access points periodically transmit their SSID's.

F. Use Strong Authentication

(1) Never use open and/or shared authentication; use 802.1X exclusively.

(a) Implement with the appropriate Extensible Authentication Protocol (EAP): EAP-Cisco Wireless (LEAP), EAP-TLS, Protected EAP (PEAP), etc.

(i) PEAP is recommended for most implementations as it supports various EAP-encapsulated methods for user authentication.

(ii) Consider implementing 802.1x TLS (Transport Layer Security) mutual authentication between host and access point with dynamic WEP. In EAP-TLS, certificates are used to authenticate the authentication server to the supplicant, and to authenticate the supplicant to the authentication server.

G. Require Strong Password Usage – Secure all host user accounts with strong passwords. (A strong password should not be a dictionary word, a name, a date, or any other distinguishable phrase. It should be a mixture of alpha, numeric, and symbol characters and be at least 8 characters in length.)

H. Limit Access to the Wireless Network by MAC Address – Configure your access points so they allow only clients with specific MAC addresses to access the network.

I. Limit Access to the Wireless Network by Using Static IP Addresses – When feasible, provide static IP addresses to authorized wireless clients; disable DHCP on the wireless network.

J. Control Access Point Coverage

(1) Carefully place each access point to limit its signal radiation to only those areas required;

(2) If possible, turn down the power on your access point to the lowest level needed to reach all legitimate users; and

(3) Use a directional antenna to limit access to required serviceable areas.

K. Use “Infrastructure Mode” Versus “Ad Hoc Mode” and Limit Peer-to-Peer Connections

(1) Disable the "ad hoc" mode on the wireless LAN card that allows them to connect with other wireless LAN cards;

(2) Identify peer-to-peer ad hoc networks between devices and take appropriate action, as needed; and

(3) Identify AP’s created by wireless laptops in “ad hoc” mode.

L. Use SNMP Securely – If you are running SNMP (Simple Network Management Protocol) agents on your access points, assign a non-obvious name to the "community" that identifies which management applications can communicate with the SNMP agents.

M. Identify Rogue Access Points – Identify rogue access points; specifically, investigate any rogue AP that broadcasts a connection to the trusted enterprise network.

(1) **NOTE:** See www.netstumbler.com and www.kismetwireless.net for open source tools to help identify rogue AP’s; and

(2) Enable rogue access point discovery on AP’s (or wireless switches), if available.

N. Monitor the Wireless Network for Suspicious Events

(1) Incorporate wireless intrusion detection to monitor network activity; and

(2) Identify intruders and attacks when they happen; establish an incident response plan to address such incidents.

O. Physically Secure your Wireless Equipment – Physically secure the access point and other wireless devices.

P. Minimize Interference with Other Wireless Technologies

(1) Conduct an initial and periodic site survey for other 2.4 GHz devices and obstructions;

(2) Set a policy to minimize 2.4 GHz interference issues; do not allow 2.4 GHz cordless phone purchases. Specify 900 megahertz or 5.8GHz in all cordless phone purchases (**NOTE:** Cell phones range from 824 to 848 megahertz.); and

(3) Test all Bluetooth devices for interference prior to purchase.

Q. Implement a Wireless Security Awareness & Education Program

(1) Educate the users of wireless LAN's to the risks and their responsibility in maintaining security;

(2) Conduct an on-going wireless network security awareness campaign for end-users, technology professionals, and executives

(3) Educate and certify wireless network administrators to ensure they have the necessary skills to properly implement and maintain wireless LAN's (see http://www.cwne.com/index.html).

R. Establish a Wireless Security Policy – Identify and publish a "minimum acceptable secure configuration" for wireless access points. Set a policy especially for AP's that may provide access to the trusted network.

S. Implement Multi-Layered Security – Use a multi-layer "defense-in-depth" approach implementing several prevention security features backed by detection and response. While each alone maybe deemed insufficient, the combination further mitigates the risks involved in wireless communications.

T. Periodically Test to Ensure Correctly Functioning Systems – Use a wireless LAN testing device/sniffer to detect interference, invalid frames, and/or malfunctioning hardware.

U. Require a VPN for Wireless Network Connections – Use an IPSec VPN solution between the wireless client and a VPN termination device (located between the trusted wireless LAN and the wired network). An IPSec VPN provides secure, industry-standard Layer 3 encryption with strong authentication.

V. Permit Access Based on Specific Times of Day – Restrict access to proper times; establish a remote access policy to limit wireless connections based upon time of day and/or limit the length of time a device can be associated with the WLAN.

W. Upgrade Wireless Devices to Support New Security Features – Periodically check with the wireless manufacturer for firmware upgrades. Many manufacturers are providing updates to improve security through the addition of Wi-Fi Protected Access (WPA) support.

X. Use Wi-Fi Protected Access (WPA) in Enterprise Mode (if available) – When possible, use WPA in enterprise mode (using a RADIUS-based authentication server) with an EAP (Extensible Authentication Protocol), to improve authentication and encryption key distribution. (**NOTE:** WPA is a subset of the impending 802.11i standard.)

Y. Minimize Accidental Association to Other Networks – Identify accidental associations with neighboring WLAN's and take action to minimize and/or eliminate such connections.

Z. Attempt to Use Industry Standard Security Features versus Proprietary Solutions – Focus on the use of "open" industry standard protocols for wireless networking and wireless security.

XII. RECOMMENDED SECURITY GUIDELINES

The recommended security guidelines within this section provide a template for an agency to consider when deploying a wireless network. As discussed earlier, the security controls that should be implemented will be largely influenced on the intended use of the wireless network, the sensitivity of the information being transmitted, and the integration of the wireless network with other networks and/or systems. The matrix below identifies the recommend security controls for four (4) specific types of wireless network deployments:

1. Public Wireless LAN – Provides wireless access unrestricted to anyone (e.g., stand-alone public wireless network for citizen access);

2. Open Wireless LAN – Limits wireless access to pre-authorized users with no attempt to keep communications private (e.g., agency's stand-alone training network);

3. Private Wireless LAN – Limits wireless access to pre-authorized users with "due diligence" to keep communications private (e.g., agency wireless network for employees, interconnected to the agency's wired network); and

4. Trusted Wireless LAN – Limits wireless access to pre-authorized users with assured private communications (e.g., agency wireless network for employees that are handling sensitive information).

As discussed throughout this document, each agency needs to conduct a risk assessment prior to deploying a wireless network. These recommended security controls should be considered during that risk assessment process, in the context of the type of wireless network to be deployed.

Wireless Network Deployment				Recommended Security Control
Public	**Open**	**Private**	**Trusted**	
✓	✓	✓	✓	Physically secure the access point (AP) and other wireless devices

Wireless Network Deployment				Recommended Security Control
Public	**Open**	**Private**	**Trusted**	
✓	✓	✓	✓	Periodically check with the wireless manufacturer for firmware upgrades. Many manufacturers provide updates to improve security and other features (specifically, many manufacturers are adding Wi-Fi Protected Access [WPA] support)
✓	✓	✓	✓	Change the default administrator's password on the wireless access point
✓	✓	✓	✓	Focus on the use of "open" industry standard protocols for wireless networking and wireless security (versus using proprietary solutions)
✓	✓	✓	✓	Identify AP's created by wireless laptops in "ad hoc" mode
✓	✓	✓	✓	Disable the "ad hoc" mode on the wireless LAN card that allows the card to connect with other wireless LAN cards
✓	✓	✓	✓	Identify peer-to-peer ad hoc networks between devices and take appropriate action, as needed
✓	✓	✓	✓	Identify accidental associations with neighboring WLAN's and take action to minimize and/or eliminate such connections
✓	✓	✓	✓	Identify and publish a "minimum acceptable secure configuration" for wireless access points providing access to the network. Set a policy especially for AP's that may provide access to the trusted network
✓	✓	✓	✓	Educate the users of wireless LAN's to the risks and their responsibility in maintaining security
✓	✓	✓	✓	If you are running SNMP (Simple Network Management Protocol) agents on your access points, assign a non-obvious name to the "community" that identifies which management applications can communicate with those agents
✓	✓	✓	✓	Identify intruders and attacks when they happen; establish an incident response plan to address such attacks

Wireless Network Deployment				Recommended Security Control
Public	**Open**	**Private**	**Trusted**	
	✓	✓	✓	Identify rogue access points, specifically looking for AP's that broadcast a connection to a trusted network (**NOTE:** See www.netstumbler.com and www.kismetwireless.net for open source tools to assist in this process.)
	✓	✓	✓	Enable rogue access point discovery on AP's (or wireless switches), if available
	✓	✓	✓	Place AP's on separate subnets and put a stateful packet inspection firewall between that subnet and the trusted network (if there is an interconnection with a trusted network)
	✓	✓	✓	Implement several layers of encryption to obscure transmitted data in an effort to prevent attackers from gleaning useful information from the network traffic. Enable the highest level of WEP (Wireless Encryption Protocol) that ships with the access point. At a minimum, use 128 bit. (**NOTE:** WEP has several weaknesses and has been proven to be "broken" easily; however, simply having it enabled may turn away an intruder or curious person.)
	✓	✓	✓	Change the default SSID (Service Set ID) that ships with your access points. Do not use information in the SSID that would associate your Agency or location with the access point
	✓	✓	✓	Carefully place each access point to limit its signal radiation to only those areas required
	✓	✓	✓	Secure all host user accounts with strong passwords (A strong password should not be a dictionary word, a name, a date, or any other distinguishable phrase. It should be a mixture of alpha, numeric, and symbol characters and be at least 8 characters in length.)

Wireless Network Deployment				Recommended Security Control
Public	**Open**	**Private**	**Trusted**	
	✓	✓	✓	Set a policy to minimize 2.4 GHz interference issues; do not allow 2.4 GHz cordless phone purchases. Specify 900 megahertz or 5.8GHz in all cordless phone purchases (**NOTE:** Cell phones range from 824 to 848 megahertz.)
	✓	✓	✓	Test all Bluetooth devices for interference prior to purchase
		✓	✓	Never use open and/or shared authentication; use 802.1X exclusively
		✓	✓	When possible, use WPA (Wi-Fi Protected Access) in enterprise mode (using a RADIUS-based authentication server) with the appropriate EAP (Extensible Authentication Protocol) to improve authentication and encryption key distribution. (**NOTE:** WPA is a subset of the impending 802.11i standard)
		✓	✓	Implement the appropriate Extensible Authentication Protocol (EAP): EAP-Cisco Wireless (LEAP), EAP-TLS, Protected EAP (PEAP), etc. - PEAP is recommended for many implementations as it supports various EAP-encapsulated methods for user authentication. - Consider implementing 802.1x TLS (Transport Layer Security) mutual authentication between host and access points with dynamic WEP. (In EAP-TLS, certificates are used to authenticate the authentication server to the supplicant, and to authenticate the supplicant to the authentication server.)
		✓	✓	If possible, turn down the power on your access point to the lowest level needed to reach all required areas
		✓	✓	Conduct an on-going wireless network security awareness campaign for end-users, technology professionals, and executives

Wireless Network Deployment				Recommended Security Control
Public	**Open**	**Private**	**Trusted**	
		✓	✓	Educate and certify wireless network administrators to ensure they have the necessary skills to properly implement and maintain wireless LANs (see http://www.cwne.com/index.html)
		✓	✓	Disable the "broadcast" mode in which access points periodically transmit their SSID's
		✓	✓	Use a multi-layer "defense-in-depth" approach implementing several prevention security features backed by detection and response. While each alone maybe deemed insufficient, the combination further mitigates the risks involved in wireless communications.
		✓	✓	Conduct an initial and periodic site survey for other 2.4 GHz devices and obstructions, to minimize undesirable interference
		✓	✓	Periodically use a wireless LAN testing device/sniffer to detect interference, invalid frames, and/or malfunctioning hardware
		✓	✓	Provide static IP addresses to wireless clients (if practical); disable DHCP on the wireless network.
			✓	Use an IPSec VPN solution between the wireless client and a VPN termination device (located between the wireless LAN and the trusted wired network). An IPSec VPN provides secure, industry-standard Layer 3 encryption with strong authentication.
			✓	Use a directional antenna to limit access to required serviceable areas
			✓	Incorporate wireless intrusion detection to monitor network activity
			✓	Configure your access points so they allow only clients with specific MAC addresses to access the network.

Wireless Network Deployment				Recommended Security Control
Public	**Open**	**Private**	**Trusted**	
			✓	Restrict access to proper times; establish a remote access policy to limit wireless connections based upon time of day and/or limit the length of time a device can be associated with the WLAN

REVISION HISTORY

07/01/13 – Changed “ITRMC” to “ITA”.

6/16/09 – Added Procedure Reference, Contact Information and Revision History to this guideline; changed the layout and deleted Timeline.

7/20/05 – Moved Guideline from Category 400, Architecture and Design, to Category 500, Security Procedures. Changed the Guideline number from G430 to G530.

Effective Date: December 17, 2003

Appendix A: Guide to 802.11 Wireless Standards

This appendix provides a full explanation of the 802.11 standards and is divided into four sections: the **802.11 Quick Reference Table,** an **Overview of the IEEE 802.11 Standards,** the **Pros and Cons of Existing 802.11 Standards,** and the **Additional Information on Existing and Future 802.11 Standards.**

802.11 Quick Reference Table

The following table provides a quick look at the currently available 802.11 wireless network standards and provides a high-level comparison of the key features for each. This table is adapted from *PC Magazine, Fall 2003, Special Wireless Issue, "Deconstructing 802.11 Wireless."*

	802.11b	**802.11a**	**802.11g**	**802.11a/g**
Products began shipping	Late 1999	Late 2001	Mid-2003	Mid-2003
Frequency	2.4GHz	5GHz	2.4GHz	2.4GHz, 5Ghz
Max Theoretical Throughput	11 Mbps	54 Mbps	54 Mbps	54 Mbps
Maximum usable indoor range	150 feet	75 feet	150 feet	75 feet (a); 150 feet (g)
Signal Modulation Technique	DSSS	OFDM	OFDM	OFDM
Compatibility	Compatible with "g" products if "g" products are configured to run in mixed mode	Incompatible with "b" and "g" products but can coexist in the same device	Backward-compatible with "b" products but only at "b" throughput	"a" is incompatible with "b" and "g" but can coexist in the same device. "g" is compatible with "b"
Approx Max Number of Users per AP	32	64	64	128
Number of Overlapping Channels	32	64	64	128
Most popular environments and why	Widely adopted in offices and homes; products are mature and inexpensive	Adopted by offices and enterprises; higher throughput and larger number of channels can serve more concurrent users	Sill new but will be popular in offices, enterprises, and homes because of its greater throughput	Still new but will be popular in offices and enterprises; combination of standards allows greater throughput and user density

Appendix A: Guide to 802.11 Wireless Standards

Overview of the IEEE 802.11 Standards

The IEEE (Institute of Electrical and Electronics Engineers) is a non-profit professional association of over 380,000 individuals in 150 countries (see www.ieee.org). Roughly 30% of the world's published literature in electrical engineering, computers and control technology has originated from IEEE. The IEEE focuses on development of open standards that will allow compatibility between products manufactured by different vendors.

- *IEEE Project 802 LAN/MAN Standards Committee*

The IEEE develops standards through committees. Since there are so many committees, the IEEE resorts to numbers to organize committee lists. The IEEE 802 LAN/MAN Standards Committee develops Local and Metropolitan Area Network standards. The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs.

- *IEEE Project 802.11 Wireless LAN/MAN Standards Committee*

In 1990, the IEEE 802 LAN/MAN Standards Committee formed the 802.11 Working Group to develop and recommend a wireless LAN standard. The emerging knowledge base has resulted in numerous Task Groups with the resulting standards reflecting the Task Groups' number.

- **IEEE Project 802.11** - Developed a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable and moving stations within a local area.

- **IEEE Project 802.11a** - Developed a Higher Speed PHY in the 5 GHz band for use in fixed, moving or portable Wireless Local Area Networks using the existing 802.11 Medium Access Control (MAC).

- **IEEE Project 802.11b** – Increased the data rate and range of 802.11 compatible networks in the 2.4 GHz band. The aim of this project differed from 802.11a by staying within the 2.4 GHz band.

- **IEEE Project 802.11c** – In cooperation with the 802.1 Working Group, added a sub clause to IS 10038 (802.1D) to cover "bridge" operation with IEEE 802.11. This standard is of more interest to companies developing 802.11 products.

- **IEEE Project 802.11d** - Added requirements and definitions necessary for 802.11 equipment to operate in markets not served by the current standard. This standard is of more interest to companies developing 802.11 products.

- **IEEE Project 802.11e** - Enhance the Quality of Service requirements to make 802.11 wireless networks suitable for voice (VoIP), video conferencing, and media stream distribution.

- **IEEE Project 802.11f** – Develop recommended practices to achieve multi-vendor Access Point interoperability across a distribution system supporting IEEE 802.11 Wireless LAN Links.

- **IEEE Project 802.11g** – Increased the data rate of 802.11b compatible networks in the 2.4 GHz band.

- **IEEE Project 802.11h** – Enhance the existing 802.11 MAC and 802.11a PHY with network management and control extensions for spectrum and transmit power management in 5GHz license exempt bands to ensure regulatory acceptance of 802.11 5GHz products. This standard is of more interest to companies developing 802.11 products.

- **IEEE Project 802.11i** - Enhance the current 802.11 MAC to provide improvements in security.

- **IEEE Project 802.11j** – Enhance 802.11 standard to allow channel selection for 4.9 GHz and 5 GHz to conform to newly available frequencies made available in Japan for radio operation.

- **IEEE Project 802.11k** – Define Radio Resource Measurement enhancements required to provide services; such as roaming, coexistence, and others; to external devices on the network. It is necessary to provide these measurements and other information in order to manage these services from an external source.

- **IEEE Project 802.11ma** - Incorporate accumulated maintenance changes (editorial and technical corrections) into 802.11-1999, 2003 edition (incorporating 802.11a-1999, 802.11b-1999, 802.11b-1999 corrigendum 1-2001, and 802.11d-2001).

- **IEEE Project 802.15.2-2003** – Developed recommended practices for IEEE 802.15 Wireless Personal Area network to allow coexistence with other wireless devices. This includes recommended practices for IEEE 802.11 devices to facilitate coexistence with IEEE 802.15 devices operating in the same location.

- **IEEE Project 802.15.4-2003** – Intended to provide a standard for ultra low complexity, ultra low cost, ultra low power consumption and low data rate wireless connectivity among inexpensive devices. The raw data rate will be high enough (maximum of 250kbs) to satisfy a set of simple needs such as interactive toys, but scaleable down to the needs of sensor and automation needs (20kbps or below) for wireless communications.

Pros and Cons of Existing 802.11 Standards

Before we explain the pros and cons amongst the various 802.11 standards, it is important to understand 802.11. 802.11 is the standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. The standard provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) modulation or direct sequence spread spectrum (DSSS) modulation. Currently, there are three standards widely available on the market: 802.11a, 802.11b, and 802.11g.

- **802.11a:** Extends 802.11 to 54 Mbps in the 5GHz band. Uses an orthogonal frequency division multiplexing modulation scheme rather than FHSS or DSSS.

802.11a	
Pros	**Cons**
▪ Products following 802.11a can be "Wi-Fi Certified"	▪ Shorter range than 802.11b
▪ Eight available channels	▪ Not interoperable with 802.11b
▪ Less potential for RF interference than 802.11b and 802.11g	▪ Speed declines with distance
▪ Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments	▪ Actual throughput is about half of the link speed divided by the number of clients associated with the access point
▪ Uses Orthogonal Frequency Division Multiplexing (ODFM) modulation to produce maximum theoretical data rate of 54 Mbps	
▪ Realistically achieves throughput somewhere between 20 Mbps to 25 Mbps in normal traffic conditions	
▪ Range about 25 meters (75 feet) at high speed in office environment	
▪ Maximum range 50 meters (150 feet) at the lowest speed in office environment	
▪ High density hot spots can achieve greater aggregate capacity with A due to the number of overlapping channels in the 5 GHz band	

- **802.11b:** Extends 802.11 to 11 Mbps with fallback to 5.5Mbps, 2Mbps, and 1Mbps within the 2.4 GHz band. 802.11b uses only DSSS.

802.11b	
Pros	**Cons**
▪ Products following 802.11b can be "Wi-Fi Certified"	▪ Not interoperable with 802.11a
▪ Requires fewer access points than 802.11a for coverage of large areas	▪ Only three non-overlapping channels in the U.S.
▪ Offers high-speed access to data at up to 300 feet from base station	▪ 802.11b hardware must be replaced to migrate to 802.11g
▪ 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations)	▪ Throughput gains provided by optional Packet Binary Convolutional Coding (PBCC) modulation may not materialize in a multi-vendor environment
▪ Maximum theoretical data rate of 11 Mbps	▪ Speed declines with distance
▪ Average throughput falling in the 4 Mbps to 6 Mbps range	▪ Actual throughput is about half of the link speed divided by the number of clients associated with the access point
▪ Maximum range is 75 meters (250 feet) at the lowest speed	▪ Bluetooth devices, 2.4 GHz cordless phones and even microwave ovens are sources of interference and thus reduce performance
▪ Higher speed range is about 30 meters (100 feet)	
▪ Use of “Barker Code” modulation at 1-2 Mbps data rates maintains compatibility with 802.11	
▪ Use of the optional Packet Binary Convolutional Coding (PBCC) modulation allows vendors to extended throughput. Results vary by vendor	

- **802.11g:** Extends 802.11b to 20+ Mbps in the 2.4 GHz band.

802.11g	
Pros	**Cons**
▪ Products following 802.11g can be “Wi-Fi Certified"	▪ Not interoperable with 802.11a
▪ Improved security enhancements over 802.11	▪ Only three non-overlapping channels in the U.S.
▪ Backward compatible with 802.11b	▪ “Backward compatibility" with 802.11b means that when a mobile 802.11b device associates to an 802.11g access point, all connections on that access point slow down to 802.11b speeds
▪ 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations)	▪ 802.11g hardware required
▪ Use of “Barker Code” modulation at 1-2 Mbps data rates maintains compatibility with 802.11	▪ Speed declines with distance
▪ Use of Complementary Code Keying (CCK) modulation at 5.5-11 Mbps data rates maintains compatibility with 802.11b	▪ Actual throughput is about half of the link speed divided by the number of clients associated with the access point
▪ Uses Orthogonal Frequency Division Multiplexing (ODFM) modulation to produce 54 Mbps bandwidth	
▪ 802.11g “ready” hardware can be firmware upgraded to 802.11g	
▪ In the exact same conditions, theory suggests 802.11g should have greater throughput than 802.11a on equal distant stations	

Additional Information on Existing and Future 802.11 Standards

- *IEEE Project 802.11c -- Bridge Operation Procedures*
  802.11c provides information needed to ensure proper bridge operations. Product developers utilize this standard when developing access points. There's really not much in this standard relevant to wireless LAN installers.

The Global Evolution of 802.11 Standards

- *IEEE Project 802.11d -- Global Harmonization*
  When 802.11 first became available, only a handful of regulatory domains (e.g., U.S., Europe, and Japan) had rules in place for the operation of 802.11 wireless LANs. In order to support a widespread adoption of 802.11, the 802.11d task group has an ongoing charter to define PHY requirements that satisfy regulations within additional countries. This is especially important for operation in the 5GHz bands because the use of these frequencies differ widely from one country to another. As with 802.11c, the 802.11d standard mostly applies to companies developing 802.11 products.

- *IEEE Project 902.11h - Dynamic Channel Selection/Transmission Power Control*
  This standard is supplementary to the MAC layer to comply with European regulations for 5GHz WLANs. European radio regulations for the 5GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the furthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.

The Quality Side of 802.11 Standards

- *IEEE Project 802.11e - MAC Enhancements for QoS*
  802.11e provides Quality of Service (QoS) support for LAN applications, which will be critical for delay-sensitive applications such as Voice over Wireless IP (VoWIP). The standard will provide classes of service with managed levels of QoS for data, voice, and video applications.

  Without strong quality of service (QoS), the existing version of the 802.11 standard doesn't optimize the transmission of voice and video. There's currently no effective mechanism to prioritize traffic within 802.11. As a result, the 802.11e task group is currently refining the 802.11 MAC (Medium Access Layer) to improve QoS for better support of audio and video (such as MPEG-2) applications. The 802.11e group should finalize the standard by the end of 2002, with products probably available by mid-2003.

  Because 802.11e falls within the MAC Layer, it will be common to all 802.11 PHYs and be backward compatible with existing 802.11 wireless LANs. As a result, the lack of 802.11e being in place today doesn't impact your decision on which PHY to use. In addition, you should be able to upgrade your existing 802.11 access points to comply with 802.11e through relatively simple firmware upgrades once they are available.

The Roaming Side of 802.11 Standards

- *IEEE Project 802.11f - Inter Access Point Protocol*
  The existing 802.11 standard doesn't specify the communications between access points in order to support users roaming from one access point to another. The 802.11 Working Group purposely didn't define this element in order to provide flexibility in working with different distribution systems (i.e., wired backbones that interconnect access points).

  The problem, however, is that access points from different vendors may not interoperate when supporting roaming. 802.11f is currently working on specifying an inter access point protocol that provides the necessary information that access points need to exchange to support the 802.11 distribution system functions (e.g., roaming). The 802.11f group expects to complete the standard by the end of 2002, with products supporting the standard by mid-2003.

  In the absence of 802.11f, you should utilize the same vendor for access points to ensure interoperability for roaming users. In some cases a mix of access point vendors will still work, especially if the access points are Wi-Fi-certified. The inclusion of 802.11f in access point design will eventually open up your options and add some interoperability assurance when selecting access point vendors.

The Security Side of 802.11 Standards

- *IEEE Project 802.11i - MAC Enhancements for Enhanced Security*
  The IEEE 802.11 Working Group instituted Task Group i to produce a security upgrade for the 802.11 standard.

  This supplemental draft standard is intended to improve WLAN security. It describes the encrypted transmission of data between systems of 802.11a and 802.11b WLANs. It defines new encryption key protocols including the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES). AES will require new hardware when it is completed in 2003.

  802.11i is building the standard around 802.1X port-based authentication for user and device authentication. The 802.11i standard, which isn't expected to be complete until late 2003, includes two main developments: Wi-Fi Protected Access (WPA) and Robust Security Network (RSN).

  - Wi-Fi Protected Access (WPA)
    The Wi-Fi Alliance has taken a subset of the draft 802.11i standard, calling it WPA, and now certifies devices that meet the requirements.

    Pros:
    - WPA addresses the shortcomings of WEP
    - WPA improves security of legacy devices to a minimally acceptable level

    Cons:
    - Not all users will be able to take advantage of it because WPA might not be backward-compatible with some legacy devices and operating systems.
    - Not all users will have the processing resources needed for WPA. (e.g., a PDA)
    - TKIP/WPA degrades performance unless a WLAN system has hardware that will run and accelerate the WPA protocol.

  - Robust Security Network

Pros:

- Significantly stronger than either WEP or WPA.

Cons:

- Will run very poorly on legacy devices that lack hardware required to accelerate the algorithms in clients and access points.
- Infrastructure requirements increase costs to deploy wireless.

Other IEEE Standards with 802.11 Implications

- *IEEE Project 802.15 Wireless PAN Standards Committee*

  The IEEE 802.15 working group addresses WPAN standards.

  There are four active task groups:

  - 802.15.1: Delivered a standard for low-speed, low-cost WPANs based on the Bluetooth spec.
  - 802.15.2: Currently developing recommended practices on how 802.11 WLANs and 802.15 WPANs can co-exist in the 2.4 GHz band. It is mainly working on the interference problem between Bluetooth and 802.11.
  - 802.15.3: Currently working on a standard for higher speed WPANs from 10 Mbps to 55 Mbps at distances less than 10 meters.
  - 802.15.4: Currently working on a standard for simple, low-cost, low-speed WPANs with data ranges from 2 Kbps to 200 Kbps and uses DSSS modulation in the 2.4 GHz and 915 MHz ranges.

- *IEEE Project 802.16 Wireless MAN Standard Committee*

  Global standard ratified in 2001 for 10 to 66 GHz wireless metropolitan area networks as an economical method of high-speed "last-mile" connection to public networks.

- *IEEE Project 802.1x - Port Based Network Access Control*

  The 802.1x standard was designed to provide a mechanism to associate end-user identity with the port of access on a wired LAN. 802.1x extends the commonly installed AAA infrastructure used to authenticate network access (e.g. dial-up, VPN) to ports on a wired LAN.

  Since 802.1x was initially conceived for a wired LAN, preventing a compromise of 802.1x in a wireless environment requires a modified implementation outlined in the 802.11i Standard for Robust Security Network (RSN).

For the latest information on standards and drafts in the 802 series go to www.ieee802.org/802info.html

Appendix B: Wireless Security Resources

For those interested in a more detailed investigation of wireless technologies and associated security issues, readers are recommended to refer to the following resources:

- Arunesh Mishra & William A. Arbaugh, An Initial Security Analysis of the IEEE 802.1X Standard (University of Maryland, 6 Feb 2002)
- Ben King, "Beyond Wi-Fi: the future of wireless networks" ZDNet Australia, 07 May 2003 <http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20274285,00.htm>
- Bob Fleck and Jordan Dimov, Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network, 06 June 2003 <http://www.cigitallabs.com/resources/papers/download/arppoison.pdf>
- Brian Clark, "WLAN security checklist" Wireless LAN Info Center, 11 Feb 2003 <http://searchnetworking.techtarget.com/infoCenter/tip/0,294276,sid7_gci879905_tax293385,00.html?Offer=wlancross5.27>
- Bruce Potter and Bob Fleck, "802.11 Security: Attacks and risks" Wireless LAN Info Center, 01 Dec 2002, 21 May 2003 <http://searchnetworking.techtarget.com/infoCenter/tip/0,294276,sid7_gci877526_tax293470,00.html>
- Cisco Aironet Response to University of Maryland's Paper, "An Initial Security Analysis of the IEEE 802.1x Standard" (Cisco Systems, 1992-2002)
- Configuring the Cisco Wireless Security Suite – Revision 2.0 (Cisco Systems, 2002)
- Dan Jones, "Cisco's Path to Switchdom" Unstrung, 02 June 2003 <http://www.unstrung.com/document.asp?doc_id=34593>
- Dan Jones, "Vivato's Switch Bitch" Unstrung, 29 January 2003, 04 June 2003 <http://www.unstrung.com/document.asp?doc_id=27661>
- Derek Krein, "Why distributed wireless IDS is needed" Federal Computer Week, 28 April 2003 <http://www.fcw.com/fcw/articles/2003/0428/tec-wire-04-28-03.asp>
- Dr. Paul Goransson, 802.11… A Standard for the Present and Future (Meetinghouse Data Communications, 1 Feb 2003)
- Jim Burns, Selecting an Appropriate EAP Method for Your Wireless LAN (Meetinghouse Data Communications, 1 Feb 2003)
- Jim Geier, "Defining Access Point Range Boundaries" 802.11 Planet, 27 May 2003, 05 June 2003 <http://www.80211-planet.com/tutorials/article.php/2212591>
- Jon A. LaRosa, WPA: A Key Step Forward in Enterprise-class Wireless LAN (WLAN) Security, (Meetinghouse Data Communications, 26 May 2003)
- John Cox, "Cisco touts plan to tame WLANs" Network World, 02 June 2003 <http://www.nwfusion.com/news/2003/0602ciscowlan.html?page=1>

Appendix B: Wireless Security Resources

- John Cox, "Wireless LAN switch feast" Network World, 12 May 2003 <http://www.nwfusion.com/news/2003/0512wifidinner.html?page=1>
- Lisa Phifer, "Air Safety" Information Security, April 2003: 48-54
- Merritt Maxim & David Pollino, Wireless Security (Berkeley, California: RSA Press, 2002)
- Mike van Opstal, "Implementing 802.1x on Wireless Networks with Cisco and Microsoft" University of Maryland Information Systems Security Lab, 30 January 2002, 22 May 2003 <http://www.cs.umd.edu/~mvanopst/8021x/howto/>
- Robert Scheier, "Ten steps to low-cost wireless LAN security" Wireless LAN Info Center, 21 Aug 2002 <http://searchnetworking.techtarget.com/infoCenter/tip/0,294276,sid7_gci846101_tax293385,00.html?Offer=wlancross5.27>
- Steven J. Vaughan-Nichols, "Making the WPA Upgrade" 802.11 Planet, 12 May 2003 <http://www.80211-planet.com/tutorials/article.php/2201281>
- SyDisTyKMoFo (Marc), "Wireless LAN Attacks Explained" Security Protocols, 20 May 2003, 06 June 2003 < http://security-protocols.com/article.php?sid=1504&foo=Wireless%20LAN%20Attacks%20Explained>
- The Next Generation of LAN Access: Addressing the Requirements of Mobile Networking, (Extreme Networks, 2003)
- Tom Karygiannis, Les Owens, "NIST Special Publication 800-48: Wireless Network Security", November 2002 < http://csrc.nist.gov >

Appendix C

802.11 Wireless Networks
Risk Assessment Form

Date:	Contact Name:	Manager/Supervisor's Name:	Date sent to ITA:
October 2003	ISEC Wireless Networking Subcommittee	ISEC	December 17, 2003

This form should be used in conjunction with the attached information and the Risk Assessment Guidelines.

***Step 1* – Scope of this Risk Assessment?** Wireless LAN (802.11) Data Communications within Trusted Networks

Step 2 **Threat Agent**	**Description of Threat and/or Vulnerability** (Is there a Security Guideline in operation ? if so give reference code in final column)	***Step 3*** **Risk Level** (Table 1)				***Step 4*** **Control Reference**
		TR	**MR**	**SR**	**IR**	
2.4 GHz Devices	**Wireless Jamming Denial-of-Service Attack** - The 802.11 PHY specifications define a limited range of frequencies for communication. The 802.11 devices that use a specific PHY are constrained to these frequency ranges. An attacker can create a device that will saturate the 802.11 frequency bands with noise. If the attacker can create enough RF noise to reduce the signal-to-noise ratio to an unusable level, then the devices within range of the noise will be effectively taken offline. The devices will not be able to pick out the valid network signal from all of the random noise being generated and therefore will be unable to communicate. Creating a device that produces a lot of noise at 2.4 GHz is relatively easy and inexpensive to construct. However, there are several common commercial devices available today that can easily take down a wireless network. Unfortunately, many 2.4 GHz cordless phones that can be purchased in electronics stores have the capability to take an 802.11b network offline. While not a refined electronic weapon, these phones can interfere or completely disable a WLAN. Cordless phones use several different modulation techniques and can overlap on the frequencies used by 802.11b. This overlapping is simply noise to an 802.11b radio. The cordless-phone-induced noise can drop the SNR enough to bring down any WLAN network nearby. There are also interference problems with other networking protocols. In particular, Bluetooth uses the same ISM band as 802.11b and 802.11g. The DSSS modulation in 802.11b is susceptible to interference from the modulation used in Bluetooth networks. While there are potential solutions to prevent Bluetooth from stepping on 802.11b transmissions, large-scale Bluetooth deployments may still interfere to the point of inoperability with 802.11b networks. As time passes, the 2.4 GHz ISM band will become more crowded, making unintended DoS attacks against 802.11b networks commonplace. Sirius and XM satellite radio, who have spectrum bordering the ISM band, have complained that ISM-band devices may cause interference with their ground based repeaters and satellites.					t) u) v) w) xb) ac)

Appendix C

802.11 Wireless Networks
Risk Assessment Form

Date:	**Contact Name**:	**Manager/Supervisor's Name:**	**Date sent to ITA:**
October 2003	ISEC Wireless Networking Subcommittee	ISEC	December 17, 2003

Step 2 **Threat Agent**	**Description of Threat and/or Vulnerability** (Is there a Security Guideline in operation ? if so give reference code in final column)	***Step 3*** **Risk Level** (Table 1)				***Step 4*** **Control Reference**
Any individual with Wireless LAN gear	**Data-link Layer Denial-of-Service Attack** - A data-link DoS can target either a host or a network. Data-link attacks disable the ability of hosts to access the local network. An example of this would be flooding a non-switched Ethernet network with invalid frames. An attacker (or sometimes a malfunctioning NIC) can send repeated frame headers with no payload. These headers are rebroadcast to all hosts on the network and effectively tie up the medium. Data-link DoS attacks are not common on wired networks because most networking gear has the intelligence to prevent data-link attacks from propagating to hosts on the network. Unobstructed access to the wireless medium again creates new opportunities for DoS attacks. Even with WEP turned on, an individual has access to the link layer information and can perform some DoS attacks. Without WEP, the individual has full access to manipulate associations between stations and access points to terminate access to the network.					a) b) f) g) h) i) j) k) l) m) p) r)

Appendix C

802.11 Wireless Networks
Risk Assessment Form

Date:	**Contact Name**:	**Manager/Supervisor's Name:**	**Date sent to ITA:**
October 2003	ISEC Wireless Networking Subcommittee	ISEC	December 17, 2003

Step 2 **Threat Agent**	**Description of Threat and/or Vulnerability** (Is there a Security Guideline in operation ? if so give reference code in final column)	***Step 3*** **Risk Level** (Table 1)				***Step 4*** **Control Reference**
Any individual with Wireless LAN gear	**Network Layer Denial-of-Service Attack** – A network-layer DoS is accomplished by sending a large amount of data to a network. This type of attack targets the network infrastructure. For example, an attacker may send 100 Mb/s of data to a network that can only transmit 10 Mb/s. The network obviously cannot retransmit all the data being sent to it, so the network equipment is forced to drop packets. This excessive traffic may also cause high loads on the CPUs within the network equipment itself, causing further network problems. A typical network-based DoS attack is a ping flood. An attacker generates massive amounts of ICMP traffic destined for the victim network. (ICMP packets are used for management functions such as querying the availability and services of a host.) This usually saturates the victim's WAN links. By cutting off the victim's LAN from the rest of the Internet, the attacker has denied access to any services that reside on the victim's LAN. When a wireless access point allows any client to associate, it is vulnerable to a network-level DoS attack. Since an 802.11 network is a shared medium, a malicious user can flood the network with traffic, denying access to other devices associated to the affected access point. As an example, an attacker can associate to an 802.11 network and send an ICMP flood to the gateway. While the gateway may be able to withstand the amount of traffic, the shared bandwidth of the 802.11 infrastructure is easily saturated. Other clients associated to the same AP as the attacker will have a very difficult time sending packets. Given the relatively slow speed of 802.11b networks, a network DoS may happen inadvertently due to large file transfers or bandwidth-intense applications. A few bandwidth-hungry applications on a WLAN can hamper access for all associated stations. With the deployment of higher-speed WLAN technologies, these unintentional attacks will become less frequent.					a) b) f) g) h) i) j) k) l) m) n) p) q) r)
Any individual with Wireless LAN gear	**Eavesdropping** - In a wireless network, eavesdropping is easy because wireless communications are not easily confined to a physical area. A nearby attacker can receive the radio waves on the wireless network without any substantial effort or equipment. All frames sent across the wireless medium can be examined in real time or stored for later examination. *To connect with wireless LANs from distances greater than a few hundred feet, sophisticated hackers use long-range antennas that are either commercially available or home built and can pick up 802.11 signals from up to 2,000 feet away. The complete kit costs about $160.*					a) b) f) g) h) i) j) k) l) m) n) o) p) q) r)

Appendix C

802.11 Wireless Networks
Risk Assessment Form

Date:	**Contact Name**:	**Manager/Supervisor's Name:**	**Date sent to ITA:**
October 2003	ISEC Wireless Networking Subcommittee	ISEC	December 17, 2003

Step 2 **Threat Agent**	**Description of Threat and/or Vulnerability** (Is there a Security Guideline in operation ? if so give reference code in final column)	***Step 3*** **Risk Level** (Table 1)				***Step 4*** **Control Reference**
Any individual with Wireless LAN gear	**Manipulation** - ARP (Address Resolution Protocol) is the mechanism that IP-enabled Ethernet devices use to determine which device on a network has a particular IP address. An attacker can force packets to go through a malicious host by poisoning the ARP mechanism. This "man in the middle" can watch, drop, forward, and manipulate data moving between the client and the server. *A wireless attacker can intercept traffic between any hosts on the same broadcast domain, regardless if they are wired or wireless by using ARP poisoning.*					a) b) f) g) h) i) j) k) l) m) n) o) p) q) r)
Any individual with Wireless LAN gear	**Illicit Use –** Any individual associated to a wireless access point can connect to the networks that live behind the access point. Illicit use may not cause any operational problems, but it still may be unwanted and unlawful use. The individual may simply be someone who drove up near the access point, associated to it to check his mail. Alternatively, they may be sending spam to thousands of email addresses. The individual may even be attempting to exploit a server that lives on the accessible networks or use the access point as a mask to hide the source of illegal actions, such as hacking other networks.					a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) r) o) ag)
Any individual with Wireless LAN gear	**Rogue access points** – The consumer market for wireless access points makes wireless access points and wireless LAN cards very inexpensive. In an attempt to foster the consumer market, these devices have been made "plug and play." An access point plugged into an office Ethernet jack will provide access to the trusted network without safeguards for anyone within range of the access point. A wireless LAN card in "ad hoc" mode will provide access to any network the host is connected to without providing safeguards for the network.					n) o) p) ac)
Any individual with Wireless LAN gear	**Access Point Hi-Jacking** - SNMP (Simple Network Management Protocol) agents are often used on wireless access points for configuration and monitoring. Individuals with wireless access can easily reconfigure the wireless access point to operate as they desire.					a) b) g) h) i) j) k) l) m) n)

Appendix C

802.11 Wireless Networks
Risk Assessment Form

Date:	**Contact Name**:	**Manager/Supervisor's Name:**	**Date sent to ITA:**
October 2003	ISEC Wireless Networking Subcommittee	ISEC	December 17, 2003

Step 2 **Threat Agent**	**Description of Threat and/or Vulnerability** (Is there a Security Guideline in operation ? if so give reference code in final column)	***Step 3*** **Risk Level** (Table 1)				***Step 4*** **Control Reference**
Any individual with physical access to wireless LAN access points	**Theft or Re-configuration –** Manufacturers always provide methods for those in physical possession of access points to reset and reconfigure the access points. This makes them a popular item to steal or replace with an access point configured to the intruder's preferences.					l) r) s)
Vulnerable data encryption	**Wired Equivalent Privacy (WEP)** has been proven ineffective as a means to encrypt data. WEP, was quickly broken by published tools WEPCrack and AirSnort, which exploit vulnerabilities in the WEP encryption algorithm. WEPCrack and AirSnort passively observe WLAN traffic until it collects enough data by which it recognizes repetitions and breaks the encryption key.					aa)
Vulnerable authentication	Papers have been published to demonstrate how certain versions of the newly proposed 802.1x standard can be defeated. Cisco has published a response that states the attack can be mitigated by the use of EAP-TLS with WEP based encryption. Where concerns demand higher levels of mitigation, Cisco has implemented a non-standard TLS Cisco protocol with additional mitigating elements.					aa)
Host Identity Theft	**MAC Spoofing** – Host identification based on an authorized list of MAC addresses provides a low level of security, but MAC addresses were never intended to be used in this manner. Any attacker can easily change the MAC address on their host to impersonate a valid station or access point.					h)
Inadvertent association with rogue access points	Using widely available tools such as HostAP, hackers can force wireless network adapter to connect to an undesired 802.11 network or alter the configuration of the station to operate in ad-hoc networking mode. A hacker begins this attack by using freeware HostAP to convert the attacking station to operate as a functioning access point. As the victim's station broadcasts a probe to associate with an access point, the hacker's new malicious access point responds to the victim's request for association and begins a connection between the two. After providing an IP address to the victim's workstation (if needed), the malicious access point can begin its attacks. The hacker - acting as an access point - can use a wealth of available hacking tools available that have been tested and proven in a wireless environment. *At this point, the hacker can exploit all vulnerabilities on the victim's laptop, which can include installing the HostAP firmware or any other laptop configuration or programmatic changes.*					q) x) y)

Appendix C

802.11 Wireless Networks
Risk Assessment Form

Date:	**Contact Name**:	**Manager/Supervisor's Name:**	**Date sent to ITA:**
October 2003	ISEC Wireless Networking Subcommittee	ISEC	December 17, 2003

Step 2 **Threat Agent**	**Description of Threat and/or Vulnerability** (Is there a Security Guideline in operation ? if so give reference code in final column)	***Step 3*** **Risk Level** (Table 1)				***Step 4*** **Control Reference**
Vendor Interoperability	**802.11 Standards** are not complete (See http://grouper.ieee.org/groups/802/11/). Known vulnerabilities with the finalized standards have led numerous vendors to develop enhancements that are not in the 802.11 standards. The resulting products may not interoperate with each other, or in the worst case may interoperate at a lower feature set that requires incomplete deployment of the desired security features.					z)
Wireless Host Routing	A host can be connected to other networks at the same time it is connected to the wireless network. Since both Windows and Linux provide routing features, this may expose the hosts on the trusted network to all of the hosts on the other "unknown" networks.					x) y)
Wireless "Build Out" on Trusted Network Connections	Any connection to the trusted network can be used as a connection point for a wireless access point. An employee with a Lap Top containing a wireless adapter would be able to very easily acquire a SOHO wireless access point that would quickly connect to their office DSL connection.					x) y)
Improper VPN Host Configuration	By design, VPN connections are designed to provide a trusted connection over an untrusted network to a private network. Improper configuration of the connecting host can inadvertently expose the trusted network to hosts on the untrusted network.					x) y)
Administrative Inexperience	Most administrators are not anywhere near up to speed on 802.11 security protocols and procedures are still being developed; giving quick-learning hackers the edge. New wireless LAN hacking tools are introduced every week and are widely available on the Internet for anyone to download.					y) ah)
802.11 Authentication, Open & Shared-Key	The designs of both open and shared-key 802.11 client authentication is weak. Open authentication simply involves providing the correct SSID. Shared-key authentication (which uses a shared WEP key) is vulnerable since a malicious user can decipher the shared WEP key (by intercepting the clear-text challenge and the same challenge encrypted with the WEP key).					ab)
Improper Host Wireless Configuration	Misconfigured host wireless devices can inadvertently expose the host system and the WLAN to eavesdropping and/or hijacking.					a) h) k) l) p) s) x) xb) ad)

	Risk Mitigating Controls	***Step 5*** **Further Action Needed**	**By Whom**	**Date**
a)	Several layers of encryption can and should be implemented to obscure transmitted data in an effort to prevent attackers from gleaning useful information from the network traffic. (a) Enable the highest level of WEP (Wireless Encryption Protocol) that ships with the access point. At a minimum, use 128 bit.			
b)	Place APs on separate subnets and put a stateful packet inspection firewall between that subnet and the trusted network.			

Appendix C

802.11 Wireless Networks
Risk Assessment Form

Date:	Contact Name:	Manager/Supervisor's Name:	Date sent to ITA:
October 2003	ISEC Wireless Networking Subcommittee	ISEC	December 17, 2003

	Risk Mitigating Controls	*Step 5* Further Action Needed	By Whom	Date
c)	DO NOT allow SMTP relay.			
d)	DO use SMTP authentication.			
e)	Use http authorization to get to the Internet.			
f)	Change the default SSID (Service Set ID) that ships with your access points.			
g)	Disable the "broadcast" mode in which access points periodically transmit their SSIDs.			
h)	Implement 802.1x TLS (Transport Layer Security) mutual authentication between host and access point with dynamic WEP. (Implement with the appropriate Extensible Authentication Protocol (EAP): EAP-Cisco Wireless (LEAP), EAP-TLS, Protected EAP (PEAP), etc. PEAP is recommended for most implementations as it supports various EAP-encapsulated methods for user authentication.)			
i)	Configure your access points so they allow only clients with specific MAC addresses to access the network.			
j)	If possible, turn down the power on your access point to the lowest level needed to reach all legitimate users.			
k)	Disable the "ad hoc" mode on the wireless LAN card that allows them to connect with other wireless LAN cards.			
l)	Secure all host user accounts with strong passwords (A strong password should not be a dictionary word, a name, a date, or any other distinguishable phrase. It should be a mixture of alpha, numeric, and symbol characters and be at least 8 characters in length.)			
m)	If you're running SNMP (Simple Network Management Protocol) agents on your access points, assign a non-obvious name to the "community" that identifies which management applications can communicate with those agents.			
n)	Identify Rogue access points that broadcast a connection to the trusted enterprise network. (NOTE: See www.netstumbler.com, www.kismetwireless.net, and www.thehackerschoice.com for open source tools; also enable rogue access point discovery on APs, if available)			
o)	Identify Peer-to-peer ad hoc networks between devices			
p)	Identify APs created by wireless laptops in "ad hoc" mode (See n) NOTE above.)			
q)	Identify accidental associations with neighboring WLANs.			
r)	Identify intruders & attacks when they happen			
s)	Physically secure the device			
t)	Conduct a site survey for 2.4 GHz devices and obstructions			

Appendix C

802.11 Wireless Networks
Risk Assessment Form

Date:	Contact Name:	Manager/Supervisor's Name:	Date sent to ITA:
October 2003	ISEC Wireless Networking Subcommittee	ISEC	December 17, 2003

	Risk Mitigating Controls	*Step 5* Further Action Needed	By Whom	Date
u)	Do not allow 2.4 GHz cordless phone purchases. Specify 900 megahertz or 5.8GHz in all cordless phone purchases (NOTE: Cell phones range from 824 to 848 megahertz.)			
v)	Test all Bluetooth devices for interference prior to purchase			
w)	Have a contingency plan for alternate communication methods. (Wired?)			
x)	Educate the user of wireless LANs to the risks and their responsibility in maintaining security.			
xb)	Conduct a wireless network security awareness campaign for end-users, technology professionals, and executives			
y)	Identify and publish a "minimum acceptable secure configuration" for wireless access points providing access to the trusted network.			
z)	Focus on the use of "open" industry standard protocols for wireless networking and wireless security.			
aa)	Use a multi-layer "defense in depth" approach implementing several prevention security features backed by detection and response. While each alone maybe deemed insufficient, the combination further mitigates the risks involved in wireless communications.			
ab)	Never use open and/or shared authentication; use 802.1X exclusively.			
ac)	Use a wireless LAN testing device/sniffer to detect interference, invalid frames, and/or malfunctioning hardware			
ad)	Use an IPSec VPN solution between the wireless client and a VPN termination device (located between the trusted w ireless LAN and the wired network)			
ae)	Incorporate wireless intrusion detection to monitor network activity			
af)	Use directional antenna to limit access to required serviceable areas			
ag)	Restrict access to proper times; establish a remote access policy to limit wireless connections based upon time of day and/or limit the length of time a device can be associated with the WLAN			
ah)	Educate and certify wireless network administrators to ensure they have the necessary skills to properly implement and maintain wireless LANs (see http://www.cwne.com/index.html)			

Appendix C

802.11 Wireless Networks
Risk Assessment Form

Date:	Contact Name:	Manager/Supervisor's Name:	Date sent to ITA:
October 2003	ISEC Wireless Networking Subcommittee	ISEC	December 17, 2003

STEP 6

Date of review by Security Planning Team:

Date of review by Executive Management Team:

Table 1

Possible Outcome			
	Slightly Harmful	***Harmful***	***Extremely Harmful***
Highly Unlikely	**Trivial Risk**	**Tolerable Risk**	**Moderate risk**
Unlikely	**Tolerable Risk**	**Moderate risk**	**Substantial Risk**
Likely	**Moderate risk**	**Substantial Risk**	Intolerable Risk

Note: Tolerable here means that risk has been reduced to the lowest level reasonably practicable.

Table 2

Risk Level	Action and Timescale
Trivial	No action is required and no documentary records need to be kept.
Tolerable	No additional controls are required. Consideration may be given to a more cost-effective solution or improvement that imposes no additional cost burden. Monitoring is required to ensure that the controls are maintained.
Moderate	Efforts should be made to reduce the risk but costs of prevention should be carefully measured and limited. Risk reduction measures should be implemented within a defined time period. Where the moderate risk is associated with extremely harmful consequences, further assessment may be necessary to establish more precisely the likelihood of harm as a basis for determining the need for improved control measures.
Substantial	Work should not be started until the risk has been reduced. Considerable resources may have to be allocated to reduce the risk. Where the risk involves work in progress urgent action should be taken.
Intolerable	Work should not be started or continued until the risk has been reduced. If it is not possible to reduce risk even with unlimited resources, the activity has to prohibited by policy.

Risk Assessment Guidelines

Effective: December 17, 2003

Objective

Provide a consistent method and presentation of risk assessment information useful to management decisions that will provide background information to support future budget requests.

Scope

The risk assessment process outlined can be applied to the security of employees & visitors, information, and physical assets.

Ownership

The agency's Security Officer/Coordinator shall maintain the currency of these guidelines.

Responsibility

1. Security Officer/Coordinator
    a. Provide initial training and guidelines.
    b. Facilitate risk assessment when requested.
    c. Mentor risk assessment process.
    d. Review risk assessments for completeness
    e. Submit risk assessments to Security Planning Team
2. Managers/Supervisors
    a. Identify areas in need of risk assessment.
    b. Identify Risk Assessment Team Leader.
3. Risk Assessment Team Leader
    a. Identify Risk Assessment Team Members.
    b. Complete Risk Assessment
    c. Submit Risk Assessment to agency Security Officer/Coordinator.
4. Security Planning Team
    a. Review risk assessments recommended actions
    b. Endorse or reject as deemed appropriate

Guidelines

Introduction

Risk assessments identify areas of potential & actual loss and the appropriate development of cost effective countermeasures to nullify the risks/losses identified.

The fundamental aim of any risk assessment is the protection of people, facilities, equipment and other assets against reasonably anticipated threats. Protection is accomplished through unobtrusive cost effective management controls that will either prevent or detect the treat.

The attached form has been designed to assist you in undertaking a risk assessment. This form should be used for a specific activity or to perform a generic risk assessment of a common activity or task.

Step 1 – Identify the scope of your risk assessment.

The scope outlines what is at risk. This "asset" may be a "state of being" such as "confidentiality" or "integrity".

Some examples are:

- Physical security of the Boise Office
- Confidentiality during communications with constituents
- Integrity of Constiuent Accounts
- Safety of Boise Office

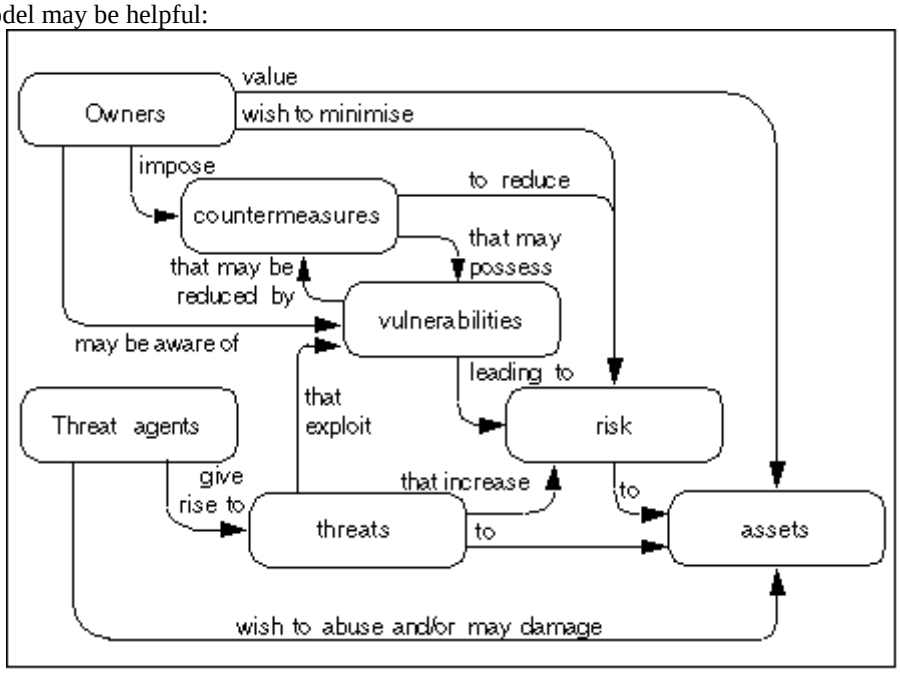
Limiting scope to a manageable size will produce a better risk assessment.

***Step 2* - Identify the threat**

All threats associated with the activity should be listed. Do not expect to find every type of threat for every activity. Threats may be identified by:

- observing the activity being undertaken
- speaking with persons carrying out the activity
- using a threat or audit checklist appropriate to the activity

The following model may be helpful:



Keep in mind the following definitions:

- Threat agents are things or people that give rise to threats.
- Threats are events or activities generally outside your control which will negatively impact the organization.
- Vulnerabilities are weaknesses within the process or activity under consideration.

Use as many pages as necessary to identify all threats. Completing the page information will help ensure no pages get lost.

***Step 3* - Estimate the risk**

The risk may be assessed by referring to Table 1 on the form. Mark the corresponding risk level column e.g. TR = Tolerable Risk, MR= Moderate Risk, SR = Substantial Risk, IR = Intolerable Risk.

- Loss of more valuable assets is more harmful to the agency
- Loss of a valuable asset that cannot be replaced is extremely harmful to the agency
- Reputation and taxpayer trust are valuable assets to the agency

***Step 4* - Identify risk mitigating controls**

Document existing controls and enter the Control Reference in the Threat Table started in Step 2. An existing control will often mitigate the risk of several of the identified threats.

Where appropriate, brain storm methods to reduce the possibility the events outlined will occur. These methods may include:

- A process (or device) to prevent the occurrence of the event
- A process to detect the occurrence of the event
- A process to transfer the risk

The methods identified are potential management controls that will mitigate the occurrence of these undesired events. "Controls" include policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected.

***Step 5* – Identify Further Action Needed**

Based on the data presented by the risk assessment, what further actions are needed?

- Existing controls may need no action or require documentation.
- Newly identified controls may require guidelines for implementation or research to establish a budget.

More then anything, the next action will be determined by circumstance.

The risk levels documented in Step 3 provide a means of prioritizing your efforts.

- Address the higher risk issues first
- Implement the cheapest solutions first

No one will endorse a million dollar mouse trap for the occasional mouse.

***Step 6* - Review the assessment**

Forward the completed Risk Assessment to the agency Security Officer/Coordinator, who will schedule a Security Planning Team review.

The emphasis of this review is to establish a consensus. Debate is anticipated and encouraged to improve the risk assessment. Participants in the risk assessment are invited to attend and answer questions.

Only risk assessment accepted by the Security Planning Team will be provided to the Executive Management Team.

Risk Assessments endorsed by the Executive Management Team are approved for submission in the budget process.

Conclusion

Assessments should be regularly reviewed to ensure their continued validity. Do not amend the assessment for every trivial change, but if a new task or procedure is introduced into the work area consider the effects it may have on existing assessments. Each time the assessment is reviewed; the appropriate section of the form should be completed and re-submitted to the agency Security Officer/Coordinator.

Enforcement

Management shall require the information in these guidelines prior to endorsing security decisions.

Audit Model

Audit will consist of:

1. Periodic reviews of formal security decisions to ensure risk assessment information is present.

Exemptions

Exemption requests should be forwarded to the agency Security Officer/Coordinator who will present them to the Security Planning Team for consideration.

_____ (agency name)

Risk Assessment Form

Date:	**Contact Name**:	**Manager/Supervisor's Name:**	**Date sent to Security Officer/Coordinator**

This form should be used in conjunction with the attached information and the Risk Assessment Guidelines.

***Step 1* – Scope of this Risk Assessment?**

Step 2 **Threat Agent**	**Description of Threat and/or Vulnerability** (Is there a Security Guideline in operation ? if so give reference code in final column)	***Step 3*** **Risk Level** (Table 1)				***Step 4*** **Control Reference**
		TR	**MR**	**SR**	**IR**	

	Risk Mitigating Controls	***Step 5*** **Further Action Needed**	**By Whom**	**Date**
a)				
b)				
c)				
d)				
e)				
f)				
g)				
h)				

_____ (agency name)

Risk Assessment Form

Page _____ of _____

Date:	**Contact Name**:	**Manager/Supervisor's Name:**	**Date sent to Security Officer/Coordinator**

Additional notes:

STEP 6

Date of review by Security Planning Team:

Date of review by Executive Management Team:

Table 1

Possible Outcome			
	Slightly Harmful	***Harmful***	***Extremely Harmful***
Highly Unlikely	**Trivial Risk**	**Tolerable Risk**	**Moderate risk**
Unlikely	**Tolerable Risk**	**Moderate risk**	**Substantial Risk**
Likely	**Moderate risk**	**Substantial Risk**	Intolerable Risk

Note: Tolerable here means that risk has been reduced to the lowest level reasonably practicable.

Table 2

Risk Level	**Action and Timescale**
Trivial	No action is required and no documentary records need to be kept.
Tolerable	No additional controls are required. Consideration may be given to a more cost-effective solution or improvement that imposes no additional cost burden. Monitoring is required to ensure that the controls are maintained.
Moderate	Efforts should be made to reduce the risk but costs of prevention should be carefully measured and limited. Risk reduction measures should be implemented within a defined time period. Where the moderate risk is associated with extremely harmful consequences, further assessment may be necessary to establish more precisely the likelihood of harm as a basis for determining the need for improved control measures.
Substantial	Work should not be started until the risk has been reduced. Considerable resources may have to be allocated to reduce the risk. Where the risk involves work in progress urgent action should be taken.
Intolerable	Work should not be started or continued until the risk has been reduced. If it is not possible to reduce risk even with unlimited resources, the activity has to prohibited by policy.