2008/2009 : Report 15

OFFICE OF THE
Auditor General
of British Columbia

Wireless Networking Security in Victoria Government Offices:

Gaps in the Defensive Line

February 2009

Library and Archives Canada Cataloguing in Publication Data

British Columbia. Office of the Auditor General.

Wireless networking security in Victoria government offices : gaps in the defensive line / Auditor General of British Columbia.

(Report ; 2008/2009: 15)

ISBN 978-0-7726-6101-2

1. Computer networks--Security measures--British Columbia. 2. Wireless communication systems--British Columbia. 3. Government communication systems--British Columbia. I. Title. II. Series: Report (British Columbia. Office of the Auditor General ; 2008/2009: 15)

QA76.9.A25B76 2008 658.4'78 C2009-900396-1

OFFICE OF THE
Auditor General
of British Columbia

LOCATION:
8 Bastion Square
Victoria, British Columbia
V8V 1X4

OFFICE HOURS:
Monday to Friday
8:30 a.m. — 4:30 p.m.

TELEPHONE:
250 387-6803
Toll free through Enquiry BC at: 1 800 663-7867
In Vancouver dial: 604 660-2421

FAX: 250 387-1230

E-MAIL: bcauditor@bcauditor.com

WEBSITE:
This report and others are available at our website, which also contains further information about the Office: www.bcauditor.com

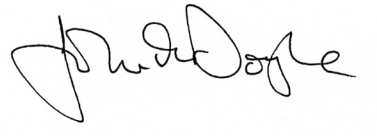
OFFICE OF THE
Auditor General
of British Columbia

8 Bastion Square
Victoria, British Columbia
Canada V8V 1X4
Telephone: 250 387-6803
Facsimile: 250 387-1230
Website: www.bcauditor.com

The Honourable Bill Barisoff
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Sir:

I have the honour to transmit herewith to the Legislative Assembly of British Columbia my 2008/2009 Report 15: Wireless Networking Security in Victoria Government Offices: Gaps in the Defensive Line.



John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
February 2009

copy: Mr. E. George MacMinn, Q.C.
Clerk of the Legislative Assembly

Table of Contents

Auditor General's Comments

John Doyle
Auditor General

Wireless technologies are ubiquitous in our society, from cell phones and other personal devices we use everyday to laptops and personal digital assistants in business environments. The many benefits of these make it difficult for most of us to imagine life "without wireless."

However, in the realm of computing, these technologies also introduce new risks to the integrity and security of networks and information. Data transmitted over the air waves can, if not properly secured, be captured, copied and possibly altered. It is especially troubling that organizations using wireless computing without appropriate security may not even know if their business data is being secretly monitored, intercepted or captured by an outside party. Governments are among these vulnerable organizations.

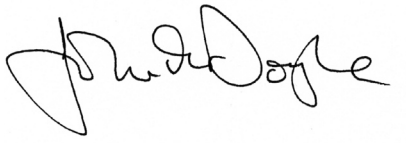
This was my initial review of this area. We took a high-level focus, confining the review to just provincial government offices in metropolitan Victoria. Nevertheless, even at this broad level, we found a number of gaps in the defensive line. We concluded that many likely government wireless access points have no, or only modest levels of protection; and that government's wireless computing policies are not up-to-date, creating an insufficient framework for a strong defence. After presenting government with these findings, we provided a reasonable period of time to address these issues before making them public.

Although our objective with this work was to advise government, we believe that the findings and recommendations we present in this report serve as sound advice for any organization that has implemented, or is thinking of implementing, wireless computing. Some general guidance and security tips are also included in the back of the report.

Given the pervasiveness of wireless computing in government and the related risks, I plan to build on this work and expand my coverage into other areas of government over time, such as Crown agencies and the SUCH sector (schools, universities, colleges and health authorities). I may also look in more detail at other aspects of wireless computing security, such as unauthorized wireless access points, as well as at the security of other types of wireless computing devices, such as personal digital assistants.

Auditor General's Comments

I would like to thank the staff in the Ministry of Labour and Citizens' Services, especially the Office of the Chief Information Officer, for the cooperation and assistance they provided my staff during their work on this audit.



John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
February 2009

Audit Team

Bill Gilhooly, Assistant Auditor General

David Lau, IT Audit Specialist

Government's Response

The Ministry of Labour and Citizens' Services is supportive of the Office of the Auditor General undertaking an audit of wireless networking security in Victoria government offices. The protection of information is a responsibility and an obligation that the Government of British Columbia takes very seriously. This audit has provided valuable information that will inform our ongoing efforts to strengthen information technology security as well as to provide important information security policies, standards and awareness opportunities.

In July 2008, responding to the identified vulnerability of wireless access points, the Government Chief Information Officer advised all Ministry Chief Information Officers to ensure any wireless access points within government are secured to industry best practices. The Office of the Chief Information Officer documented and distributed an interim standard for wireless networking based on the wireless networking standards for PharmaNet.

Ministries reviewed their wireless access points and reconfigured or replaced those that did not meet the interim standard.

Since July 2008, the Office of the Chief Information Officer has developed government wireless security standards and the cryptographic standards for information protection. Both standards will be approved and published by the end of February 2009.

The Ministry of Labour and Citizens' Services supports and appreciates the recommendations provided by the Auditor General of British Columbia, and will utilize the recommendations to assist in a continuous improvement of the government's wireless network security.

Lori Wanamaker, CA
Deputy Minister, Ministry of Labour and Citizens' Services

Detailed Report

The Advantages and Risks of Wireless Computing

Wireless technologies enable one or more hardware devices to communicate without being physically connected. They use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.

The suite of wireless technologies ranges from complex systems such as Wireless Local Area Networks (WLANs), cell phones and personal digital assistants (for example, BlackBerrys) to simple devices such as wireless headphones, microphones and other devices that do not process or store information. Wireless technologies also include infrared devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link.

In the last decade, significant technological advances have increased the speed and reliability of wireless technologies, resulting in wide mainstream acceptance and use across society.

What is wireless computing?

Wireless computing is a class of wireless technologies that has become very popular in recent years. Wireless networks are increasingly popular among personal, academic, business and government users. Extending the range of traditional wired networks, these new networks use radio waves to transmit data to wireless-enabled devices such as laptops and personal digital assistants.

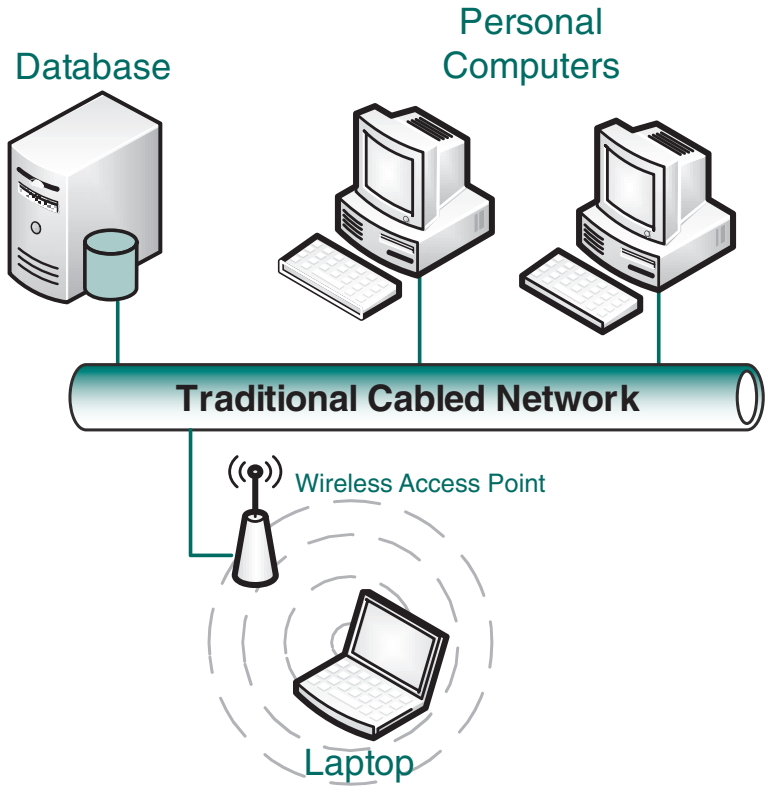
Wireless computing connection points are widely available in many public places. A user can sit in any "hotspot"—such as a hotel, shopping centre, coffee shop, library, school, airport or a business—and connect "untethered" to a host computer, network or online service provider. This ease of access is due in part to new wireless communication standards and methods that significantly increase wireless bandwidth (the data transmission rates), and to decreasing costs of equipment such as laptops and connectivity devices. Wireless connections are also relatively easy to install and use. Being able to connect this way is convenient and useful for many reasons.

There are two common ways that wireless network environments are enabled:

- The most common is where one or more wireless access points are connected in an infrastructure mode network (Exhibit 1).
- The second way is an ad hoc wireless network, where two or more computers, such as laptops, are connected wirelessly and transfer information back and forth (Exhibit 2).

Exhibit 1:

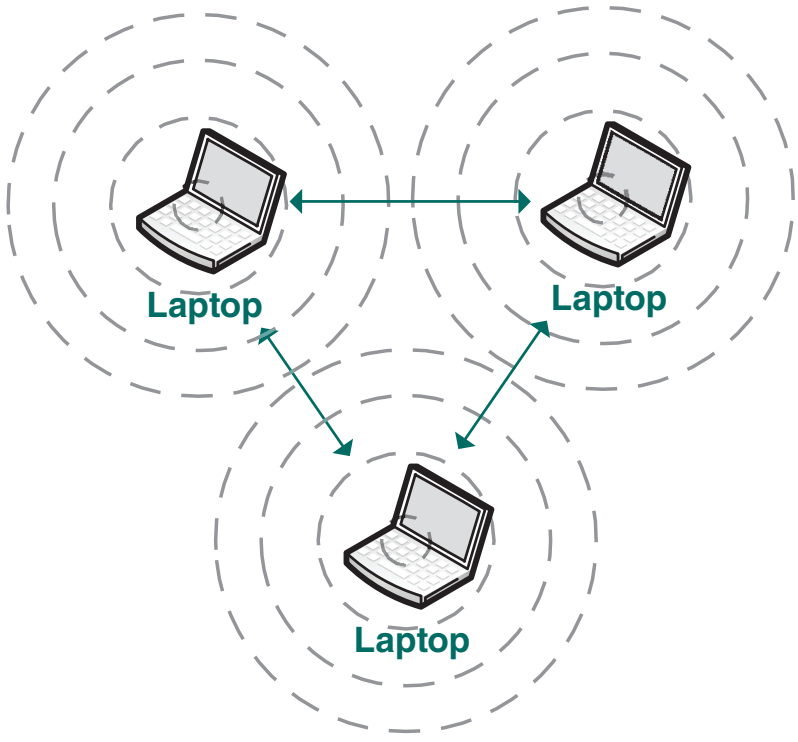
Example of a Wireless Infrastructure Mode Network



Source: Compiled by the Office of the Auditor General.

Exhibit 2:

Example of Wireless Ad Hoc Networking



Source: Compiled by the Office of the Auditor General.

The risks with wireless computing

Although wireless computing has several significant benefits, it can also be vulnerable to attack or compromise. As a result, it poses significant information security risks to any individual or organization using it.

Many government offices use wireless networks as an extension of their offices' existing wired networks. If the networks are not properly designed and secured with strong data encryption[1] during transmission through the air waves, even relatively small wireless network segments put the entire network at serious security risk.

[1] Encryption refers to the process of transforming words and numbers so that they cannot be read by anyone but those having the knowledge (or "key") to decode the information

While it is true that regular cable-based network environments also face the same security challenges as wireless networks do, wireless computing involves additional risks. The three chief ones to maintaining the confidentiality, integrity and availability of information are:

- protecting against attacks that exploit wireless data transmissions;
- establishing physical control of wireless-enabled hardware devices; and
- preventing unauthorized wireless deployments.

One of the biggest inherent problems is that radio waves transmitting data can be intercepted by anyone with malicious intent, or even just curiosity. In either case, the results can be damaging.

For example, as Exhibit 3 shows, if wireless network access points are not properly installed, signal leakage[2] outside of government premises can propagate and be picked up by those with wireless scanning equipment in lobbies, cars or nearby parking lots. There is also extra risk in multi-tenant buildings, where only a single wall, ceiling or floor may be between a wireless access point and scanning equipment.

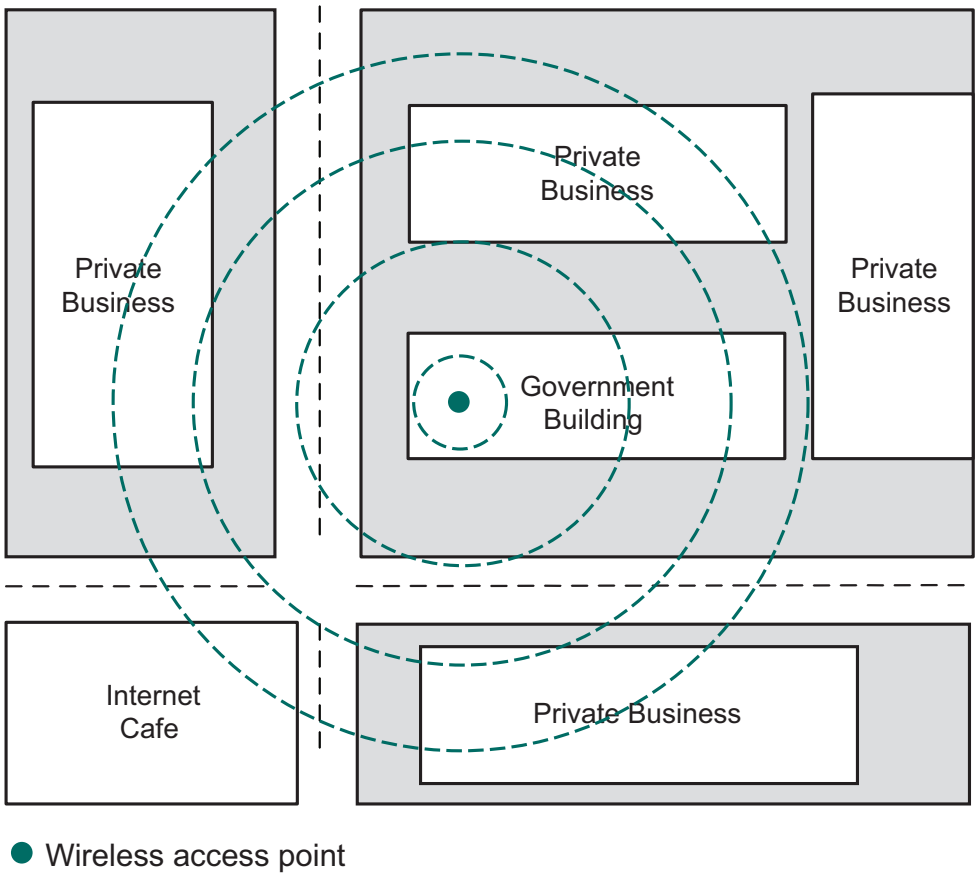
In situations where access points are broadcasting data with weak or no encryption, all the data received and transmitted through them could be intercepted and copied. Of greatest concern are "keys to the kingdom" data—sensitive information such as userids and passwords which, if picked up, could put the entire network under significant security threats.

In many cases, an organization may be under surveillance in this way yet never be aware of what is happening until a breach is realized.

[2] Signal leakage occurs when wireless signals are broadcast beyond the perimeter of an entity's building, which increases the susceptibility to attack.

Exhibit 3:

Example of signal leakage that can occur from a wireless access point



Source: Compiled by the Office of the Auditor General

How attacks can be carried out

The most common way that wireless installations are attacked is by individuals who, equipped with a specially enabled laptop computer fitted with an external antenna, drives or walks around buildings to find where signal leakage is occurring from wireless access points. The transmission information captured lets an attacker know whether or not the wireless access point is using encryption.

After finding out which wireless access points have no or weak encryption, the way is open for the individual—if he or she is so inclined—to carry out any type of a variety of attacks (see below). Unfortunately, the Internet makes available free software that can assist hackers in receiving and processing wireless signal scans, as well as deciphering some types of encryption. Strong encryption is therefore a very important element in protecting any wireless network environment.

Some Common Methods of Attacking Wireless Networks

Type	Method	Examples
Passive attacks	Eavesdropping	Attacker reads and captures message contents from the air waves from particular sites.
	Traffic analysis	Attacker monitors data transmissions are monitored to look for patterns.
Active attacks	Masquerade	Attacker impersonates an authorized user and his or her privileges to gain access to systems and data.
	Replay (also known as "man-in-the-middle")	Attacker actively eavesdrops after independently connecting with two victims and then relays messages between them, making them believe they are talking directly to each other over a private connection. In fact, the attacker controls the entire conversation.
	Message modification	Attacker alters a legitimate message by deleting or modifying it.
	Denial-of-service	Attacker floods a wireless network with excess radio signals to prevent authorized users from accessing it.

Attacks on wireless computing networks from outsiders are not the only problem. Sometimes users will secretly attach their own wireless access points to a network without the knowledge of those that administer the security of the network. These unauthorized, or rogue wireless access points, pose a significant risk, since they may be installed inside the firewall, which is set up to protect an organization's information assets from other types of external attacks.

Network monitoring software is available that may detect rogue wireless access points, however, using it is often less effective than just doing onsite wireless scans to find the physical locations of wireless access points to see if they should be connected to the regular wired network.

Detailed Report

Purpose and Scope of the Audit

What we looked at

In conducting this audit, we had two aims:

- to conduct a high-level security assessment of government wireless access points in the metropolitan Victoria area; and
- to identify and report on probable government wireless access points (WAPs) that are not complying with applicable government wireless security guidelines or leading industry practices.

This audit is the first of several we have planned on this topic and that will cover other geographic locations and other types of assessments.

Our approach

We set the stage for carrying out this audit by first reviewing government's existing security policies for wireless computing. We then acquired the physical addresses we needed through the Accommodation and Real Estate Services of the Ministry of Labour and Citizens' Services database, as well as a list of all known government Internet addresses from the Office of the Chief Information Officer. We also obtained a legal opinion to confirm that the method we were proposing to use to detect WAPs—conducting external scans—did not violate provincial privacy laws.

Over two days in February 2008, our audit team performed external scans of 285 offices at 109 Victoria government sites (with civic addresses). This involved driving past the identified government sites and scanning for particular radio frequency signals. For this purpose we used a laptop running wireless scanning tools, and employed vehicle-mounted wireless and GPS antennas. We stationed ourselves as close as possible to the site locations on roads and parking lots and then at a one-block radius around each site. Without scanning within government building sites (something that could be done as a potential follow-up assessment), actual locations of WAPs are only approximate because of the nature of wireless radio reception and the tools used.

Detailed Report

We prepared a detailed management report and provided it to the Office of the Chief Information Officer on May 30, 2008. We offered not to publish our public report until the significant deficiencies we found were remedied. We also briefed a number of the ministries' Chief Information Officers on August 8, 2008. The Office of the Chief Information Officer prepared an action plan to deal with the findings of our assessment, and provided our Office with status updates on several occasions.

Note that to avoid introducing additional security risks, we have not named specific locations and government entities in this report.

We conducted the audit in accordance with the assurance standards recommended by the Canadian Institute of Chartered Accountants. Accordingly, it included tests and other procedures we considered necessary to obtain sufficient and appropriate evidence to support our conclusions.

What we did not look at

This was a high-level assessment of wireless computing within just one geographic area. It did not include entering government buildings where there were suspected unsecured or possible unauthorized wireless access points. This audit also did not assess compliance with security policies in any other areas where government uses wireless technologies (such as BlackBerrys and cell phones).

What We Found and Recommended

Two-thirds of scanned wireless access points near government buildings used only modest encryption or none at all

The external scans we conducted identified a total of 5,573 wireless access points (WAPs). Of these, 1,445 were within approximately half a block of a government office building site. Although we could not be certain that all of these WAPs lie within government buildings (and not, say, commercial businesses), there is a high probability that many are, given the clustering of government buildings in some areas. The Office of the Chief Information Officer agreed with our assumption.

Exhibit 4 below shows an example of a scan result for several government office buildings, with the street names and internet addresses removed.

Of the WAPs we found close to government buildings, 442 (about a third) did not use any form of encryption, 542 used a modest form of encryption, and the remaining 461 used strong encryption.

Some of the 442 unencrypted WAPs are likely connected to internal provincial government networks at numerous sites across Victoria. This, in our view, broadened the risk of confidential information at these unprotected access points being exposed to unauthorized parties.

The 542 modestly encrypted WAPs also pose known security weaknesses. Without good encryption, attackers can sometimes find the encryption key in minutes, using tools found on the Internet.

In both cases above, we recommended that government conduct detailed assessments at the sites we identified in our management report, to determine which particular wireless access devices were broadcasting data with either modest or no encryption, and implement appropriate security.

Exhibit 4

Sample scan results for several government office buildings in downtown Victoria, showing wireless access points and level of encryption

Source: Compiled by the Office of the Auditor General.

Several government sites were receiving or broadcasting information with no encryption

Weaknesses in wireless networking at two ministries concerned us. One ministry, we found, was broadcasting unencrypted information over a point-to-point link between two of its buildings. Because the signal was bouncing off taller buildings in the area, it was possible for traffic from this link to be received over a wide area (more than 700 metres across).

Another ministry we found had three WAPs broadcasting unencrypted information within one building that could be picked up from outside the premises. Information transmitted over these insecure links could be accessed from residences, offices, streets and parking lots across a large reception zone. We recommended that government either encrypt the information going through these links or, if that was not feasible, move the data traffic to a secure land-based link (that is, using cables).

One-third of access points near a health authority site had no encryption

At one health authority site, 64 of the 182 WAPs on or near the site had no encryption.

We presented these findings to the health authority's security group, who followed up on our findings and provided a written response. We were told that the access points with no encryption were related to guest access points, called PartnerConnect, where visiting partners and vendors can access the Internet. According to the health authority, clinical use is prohibited, and this service, although unencrypted, still requires a username and password to access it.

As well, the health authority told us that an additional 75 WAPs related to prototype wireless services, which were subsequently deactivated. The security group also indicated that they investigated the remaining WAPs we picked up in our scans and reported no further security-related issues.

We did not follow up on the status of the health authority's actions in this audit.

Government's wireless security policies are not up-to-date

Wireless technologies and standards are changing so rapidly that the importance of keeping security policies up-to-date is paramount. A wireless security defensive zone based on out-dated standards is a completely inadequate way to protect the rest of the network from intrusion. Although no security measures can be deemed 100% foolproof, a sound security policy based on the latest standards is the foundation on which to build the rest of the network defenses.

We found that the wireless security policy and guidelines issued by government in 2003 do not reflect either current wireless security standards or even the current requirements of the Office of the Chief Information Officer for wireless connectivity to internal provincial government networks. This, we feel, creates the risk that the standards used by government organizations to protect their networks are not robust enough to meet the risks in the current environment. And even if policies and guidelines were compliant with the existing standard, the levels of encryption prescribed are not strong enough to effectively deter potential attacks.

The Office of the Chief Information Officer agreed that government's polices need to be updated, and included this issue for resolution in its action plan.

Recommendations

1. ***Government should reconfigure, upgrade or replace any of its wireless access points found to be transmitting without encryption.***
2. ***Ministries should review their wireless access points and reconfigure those suspected of using little or no encryption, to ensure they are set up with stronger security encryption.***
3. ***Government should review its wireless computing security policies and guidelines and update them to reflect the latest standards.***
4. ***Government should regularly monitor its wireless computing practices to ensure they are in compliance with its wireless security policies.***

Appendices

Appendix A: Security Guidelines for Wireless Area Networks

Policies	Controls
■ Understand and adhere to all applicable policies, standards and guidelines for wireless infrastructure security. ■ In the absence of applicable or outdated policy and standards, create an appropriate security policy with supporting standards for wireless LAN infrastructure. ■ The policy should address aspects such as purpose, responsibilities, enforcement, exceptions, and terms and definitions. ■ Maintain policies, standards and guidelines to ensure they are current and relevant with wireless LAN technology developments and new threats.	Utilize the following minimum controls when attaching a wireless LAN infrastructure to the government network: ■ Utilize all the controls as stipulated in the appropriate government information security policy. ■ Control physical access to wireless LAN devices to prevent malicious activities such as resetting device to default factory setting. ■ Check regularly for vendor security patches and upgrades and apply as needed. ■ Have regular, independent security assessments performed to measure compliance and check for rogue or unauthorized wireless devices. ■ Maintain a complete inventory of all wireless LAN devices. ■ If the business requirement exists, provide for wireless LAN guest access to avoid rogue access points connecting to internal networks.
Awareness and Training	**Monitoring and Audit**
Users and administrators of the wireless LAN need to be educated in wireless network security: ■ Ensure that users on the wireless LAN are trained in information security awareness and the risks associated with wireless technology. ■ Administrators must track progress of the latest wireless LAN standards and security features. ■ Administrators must vigilantly monitor for new wireless LAN threats and vulnerabilities. ■ Ensure staff clears wireless LAN device configurations before disposing of equipment to prevent disclosure of network configuration, keys, passwords, etc.	■ Enable logging on wireless LAN devices and review logs on a regular basis for security-related events. ■ Establish programs to detect rogue access points (unapproved internal network connections and attempts to mimic official networks to capture confidential information). ■ If your wireless LAN does not provide for automated rogue detection, establish a manual audit program. ■ Establish procedures for reporting and responding to wireless LAN security incidents.

Source: PriceWaterhouseCoopers, LLP

Appendix B: Useful Tips for Accessing and Using Government Networks

All users accessing government networks

Regardless of the method used to connect to a government network, these minimum security measures should be followed:

- Ensure that a personal firewall is enabled on your computer (i.e., McAfee);
- Install proven anti-virus software;
- Ensure your anti-virus software is up-to-date with the latest virus definition files;
- Keep your Windows (or other Operating Systems) up to date with the latest security patches;
- Do not open email attachments from unknown senders;
- Avoid file sharing by disabling this feature on your computer; and
- Make regular backups of critical data.

In addition to these basic security measures, other specific ones must also be followed, depending on your access method.

Wired Networks (ADSL, Cable, Dial-up)

To connect securely, use the Workplace Technology Services (WTS) security infrastructure such as:

- Virtual Private Network (VPN) to connect securely over the internet;
- Desktop Terminal Services (DTS); and
- HTTPS security enabled websites, which you can recognize by the https in the URL address.

Wireless Computing

- Change the default admin password on the wireless router;
- Enable strong encryption, ideally using Wi-Fi Protected Access (WPA);
- Turn the wireless network off when you will not use it for prolonged periods; and
- Do not put personally identifiable information, such as your name, in wireless device identifiers (known as SSIDs).

Appendix B

HOTSPOTS (Airports, Cyber Cafés)

- Avoid using hotspots if transmitting any confidential or sensitive information unless you are using VPN or HTTPS;
- If you do not know what VPN or HTTPS is, you should not be using hotspots to transmit sensitive data;
- Watch out for shoulder surfing (people may be watching over your shoulders to obtain sensitive information such as userids and passwords); and
- Avoid using adhoc (peer to peer) wireless.

If in doubt, contact your system administrator for advice or instructions.

Source: PriceWaterhouseCoopers, LLP