OFFICE OF THE
Auditor General
of British Columbia

REPORT HIGHLIGHTS **February 18, 2009**

Wireless Networking Security in Victoria Government Offices

Introduction

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. 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.

Although wireless computing has several significant benefits, it can also be vulnerable to attack or compromise. Many government offices use wireless networks as an extension of their offices' existing wired networks. If the networks are not properly secured with strong data encryption during transmission through the air waves, even relatively small wireless network segments could put the entire network at risk.

Purpose of the Audit

The goal of the audit was to conduct a high-level security assessment of government wireless access points (WAPs) in the Victoria area and identify potential access points that may not be sufficiently encrypted and comply with leading industry security practices.

Conclusion

As wireless computing and the use of wireless technologies becomes increasingly prevalent throughout government, it is paramount that the transmission of information through these wireless networks be protected. As of July 2008, current wireless security practices amongst government offices in Victoria showed that the majority of scanned wireless access points near government buildings only used modest encryption or none at all.

Similarly, government's wireless security policies were not up-to-date. We found that the wireless security policy and guidelines issued by government in 2003 no longer reflected 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.

Key Findings and Recommendations

1. Two-thirds of scanned wireless access points near government buildings used only modest encryption or none at all. We recommended that government conduct detailed assessments at the sites 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. If encrypting the information going through these links is not possible, we recommended that government move the data traffic to secure land-based links using cables.

Detailed results of our work were provided to the Chief Information Officer of the Province of British Columbia (CIO) in July 2008 to allow time for government to address security vulnerabilities prior to the public release of our general findings. The CIO reports that he has advised all ministry chief information officers to ensure any wireless access points within Government are secured to industry best practices.

2. One-third of access points near a health authority site had no encryption. We presented these findings to the health authority's security group, who followed up and provided a written response. Their response explained that many of their WAPs were for "guest access" and required a username and password to access, that they have since deactivated 75 other WAPs and examined their remaining points to ensure no further security-related issues. We did not follow up on the status of the health authority's actions in this audit.

3. Government's wireless security policies are not up-to-date. We recommended that government review its wireless computing security policies and guidelines and update them to reflect the latest standards, as well as ensure that they are in compliance with its wireless security policies. When presented with the findings of this report, the Office of the Chief Information Officer agreed that government's polices need to be updated. They report that they are developing new government wireless security standards to be published by the end of February 2009.

For more information, please contact:
Office of the Auditor General, 8 Bastion Square, Victoria, B.C. V8V 1X4
Tel: 250 387-6803
A copy of the full report is available on our website at: **www.bcauditor.com**