Section 9

Update on the implementation of recommendations from:

Wireless Networking Security in Victoria Government Offices: Gaps in the Defensive Line

February 2009

October 2009

RECOMMENDATION STATUS SUMMARY

Wireless Networking Security in Victoria Government Offices: Gaps in the Defensive Line

As at July 31, 2009

(*Please tick implementation status for each recommendation.*)

Auditor General's Recommendations	Implementation Status				
	Fully	**Substantially**	**Partially**	**Alternative Action**	**No Action**
1. Government should reconfigure, upgrade or replace any of its wireless access points found to be transmitting without encryption.	X				
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.	X				
3. Government should review its wireless computing security policies and guidelines, and update them to reflect the latest standards.	X				
4. Government should regularly monitor its wireless computing practices to ensure they are in compliance with its wireless security policies.			X		

PROGRESS IN IMPLEMENTING RECOMMENDATIONS FORM

Wireless Networking Security in Victoria Government Offices: Gaps in the Defensive Line

As at July 31, 2009

General comments

*Please provide an introductory statement summarizing progress [since the Public Accounts Committee last discussed the report - **if applicable**].*

Progress by recommendation

For each recommendation, provide your assessment of implementation status as per the legend at the bottom of the page, and information on actions taken and results to support the status reported. Also include a work plan schedule for any recommendations not yet implemented.

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation, including dates)
Recommendation 1: Government should reconfigure, upgrade or replace any of its wireless access points found to be transmitting without encryption.		
F	Ministries and Workplace Technology Services have reviewed the Auditor General's report and identified three non-compliant wireless WAN bridged circuits.	Workplace Technology Services has shutdown the three point-to-point wireless WAN bridged circuits found on the previous Auditor General's report. All WiFi / WLAN wireless access points currently supported by Workplace Technology Services have WPA/AES 256 encryption enabled at each location.

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation, including dates)
Recommendation 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.		
F	The Government Chief Information Officer sent a memorandum to the ministry chief information officers on February 26, 2009, requesting confirmation of all existing wireless access points, a detailed security plan for the wireless access points, and commitment to ensure all future wireless installation are in compliance with existing security policy. Ministries reviewed their wireless access points and reported their findings and commitment to the Government Chief Information Officer.	Ministries have reviewed all their wireless access points and confirmed that they meet encryption standards. The ministry review demonstrated that there is a level of commitment from ministries that all new wireless network installations will comply with the relevant corporate policy and standards.
Recommendation 3: Government should review its wireless computing security policies and guidelines and update them to reflect the latest standards.		
F	The Office of the Chief Information Officer reviewed existing policy and standards on wireless computing. The Office of the Chief Information Officer documented and distributed an interim standard for wireless networking based on the wireless networking standards for PharmaNet. The audit report became a strong driver to accelerate the completion of the standard development on wireless networking and cryptographic controls, which were under development within the Office of the Chief Information Officer.	The Office of the Chief Information Officer developed and published (a) the *Technical Security Standard for Wireless Local Area Networks* and (b) the *Cryptographic Standards for Information Protection* in February 2009. The newly created standards were communicated to the ministry chief information officers.

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation, including dates)
Recommendation 4: Government should regularly monitor its wireless computing practices to ensure they are in compliance with its wireless security policies.		
P	In April 2009, the Government Chief Information Officer issued a memorandum requesting Workplace Technology Services to undertake an evaluation of the deployment of a corporate-wide network access control mechanism.	Workplace Technology Services has initiated a pilot project to evaluate network access control software. Network access control software provides a constant network monitoring capability that can prevent unauthorized devices (including unauthorized wireless access points) from connecting to the network.

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation