Wireless Networking Security in Government: Phase 2
Ministry of Labour, Citizens' Services and Open Government

As at: July 20, 2012
Released: 8 December 2010
1st Follow-up: April 2011 2nd Follow-up: October 2011 3rd Follow-up: March 2012
Discussed by the Public Accounts Committee: 26 May 2010

Self-assessment conducted by Ministry of Labour, Citizens' Services and Open Government

Comments:

Currently three recommendations are fully or substantially implemented and two are partially implemented.

Recommendations

RECOMMENDATIONS ADDRESSED IN PREVIOUS FOLLOW-UP REPORT(S):	SELF-ASSESSED STATUS
Recommendation 1: To support the government's IM/IT (information technology and management) policies relating to wireless network security, government establish adequate procedures to ensure ministry compliance with the policies as established by the Office of the Chief Information Officer.	**Fully or substantially implemented**
Recommendation 2: Shared Services BC regularly update the job descriptions of all key IT personnel to ensure the roles and responsibilities are clearly delineated.	**Fully or substantially implemented**
Recommendation 5: For monitoring purposes, Shared Services BC develop a process for establishing and updating an inventory list of authorized wireless access devices and that the list be verified periodically.	**Fully or substantially implemented**

Outstanding Recommendations:

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 3: Government develop a network access control solution for monitoring and detecting, on a real time basis, unauthorized computing devices — particularly wireless — connected to the government network, including devices that are not configured properly.	**Partially implemented**

Actions taken, results and/or actions planned

To provide rogue device detection and guest network capability, a pilot for one of the major government IT facilities is starting in August 2012. Another extended proof of concept is also planned, which will provide capability to apply policy controls for enabling both user and device authentication for access control.

Implementation and service delivery of the Network Access Control infrastructure is in scope for the large network outsourcing contract planned this year.

Recommendations (Cont.)

Recommendation 4: Shared Services BC implement mechanisms and procedures to scan and confirm that only properly configured and authorized wireless access devices are installed when connecting to the government network infrastructure.	**No action taken**

Actions taken, results and/or actions planned

No action since previous report, fully addressing this recommendation is dependent on the implementation of Recommendation 3. Network Access Control will fulfill this requirement.

Wireless Networking Security in Government: Phase 2
Simon Fraser University

As at: August 10, 2012
Released: 8 December 2010
1st Follow-up: April 2011 2nd Follow-up: October 2011 3rd Follow-up: March 2012
Discussed by the Public Accounts Committee: 26 May 2010

Self-assessment conducted by Simon Fraser University

Comments:

Recommendations

RECOMMENDATIONS ADDRESSED IN PREVIOUS FOLLOW-UP REPORT(S):	SELF-ASSESSED STATUS
Recommendation 1: Establish a formal IT committee with a strong mandate to oversee IT strategic direction, IT needs of the university community and, most importantly, the protection of the university's IT network.	**Fully or substantially implemented**
Recommendation 2: Establish an IT Security Officer position that has exclusive duties and responsibilities relating to IT security and is accountable to independent senior management.	**Fully or substantially implemented**
Recommendation 4: Establish policy and procedures to ensure that users are formally and regularly asked online to accept the policy for appropriate use of communication technology (including wireless) provided by the university.	**Alternative action taken**
Recommendation 5: Enforce periodic change of password.	**Alternative action taken**
Recommendation 6: Require staff with high-level access rights to systems, applications and data to access system resources using secured wireless methods only.	**Alternative action taken**
Recommendation 7: Conduct review to limit the use of ad hoc and peer-to-peer networking.	**Alternative action taken**
Recommendation 8: While monitoring wireless networking activities, ensure that log reviews are fully documented and include such information as the type of reports reviewed, the date of the review, and what action has taken place.	**Alternative action taken**

Recommendations (Cont.)

Outstanding Recommendations:

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 3: Ensure that the Information Security Policy is supported with detailed wireless security standards and procedures to guide the implementation and maintenance of a robust wireless security network.	**Fully or substantially implemented**

Actions taken, results and/or actions planned

The committee described in Recommendation 1, called "IT Strategies" meets bi-monthly, and has made deliberate progress towards articulating and establishing an over-arching policy & practice framework for Information Security, IT Security, and Wireless Security (among a number of other agenda items). An initial draft is being revised by a subcommittee, expected to report during the Fall 2012 term. When this activity concludes, we anticipate some small number of formal policies to be proposed under SFU's policy on policies, and other parts of the framework to be put into effect directly. We currently expect the wireless standards and procedures to fall into the latter category, implying more timely formal approval.