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

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

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

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

Recommendations addressed in previous follow-up(s):

RECOMMENDATION	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

Shared Services BC completed an initial Proof of Concept for basic Network Access Control during the summer of 2010.

The current government environment has components from multiple vendors that may be used for our Network Access Control solution. During Fiscal Year 2012, an extended Proof of Concept will evaluate different scenarios including, but not limited to, government-owned devices vs. non-government-owned devices, wired and wireless network access, standard authentication vs. non-standard authentication. As a result of this Proof of Concept, a solution will be recommended.

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.	**Partially implemented**

Actions taken, results and/or actions planned

Fully addressing this recommendation is dependent on the implementation of Recommendation 3. Network Access Control will fulfill this requirement.

Audit of Wireless Networking Security in Government, Phase 2
Simon Fraser University

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

Self-assessment conducted by Simon Fraser University

Rather than considering wireless security in isolation, we have begun a review of our overall information security framework. Initial discussion at the senior IT Strategies committee is scheduled for February 9, 2012. Some technical progress has also been made on stronger wireless security, as described below.

Recommendations addressed in previous follow-up(s):

RECOMMENDATION	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.)

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.	**Partially implemented**

Actions taken, results and/or actions planned

On the technical front, we have provided software to simplify the wireless configuration of client devices dramatically. This gives us leverage to put pressure on our entire user community (students, faculty, staff) to use our secure wireless SSIDs (SFUNET-SECURE, eduroam), rather than the insecure SFUNET. Even though all wireless access points are outside the network security perimeter of our enterprise applications, we will move gradually to tighten wireless security. As our revised information security framework is articulated, it will incorporate wireless security standards as recommended.