APPENDIX 1

GOVERNANCE AND MANAGEMENT OF CITY WIRELESS TECHNOLOGY NEEDS IMPROVEMENT

MARCH 12, 2010

TORONTO Auditor General's Office

Jeffrey Griffiths, C.A., C.F.E.
Auditor General
City of Toronto

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Wireless technology is a fast growing alternative to wired networking

The use of wireless technology is a fast growing alternative to wired networking which relies on cabling between computer network devices. Wireless local area networks or "Wi-Fi" (WLANs) use radio waves to communicate over short distances instead of traditional networking cables.

The City uses WLANs to extend its existing wired network by attaching a number of wireless access points to the City's wired network. Wireless access points are hardware devices that transmit and receive information. Each access point can serve multiple users within a defined area. As users move beyond the range of one access point they are automatically handed over to another.

Wireless technology is generally used in locations where it is difficult, costly, or not possible to install wire cabling. Wireless technology is also used to connect portable or temporary computer devices or workstations when the network is only required for a short time period.

Demand in the use of wireless technology will increase

Future developments for wireless technology have great potential to improve City efficiency and effectiveness. Expansion of wireless technology is expected to provide employees with tools to streamline daily work activities and reduce cumbersome manual processes.

As useful as it is, wireless technology comes with some degree of risk. Risk management protocols are necessary to ensure data is secure and maintained properly.

Audit addresses City action in addressing wireless related risks

The objective of this audit was to determine what steps the City has taken to address risks related to the emerging use of wireless technology. Specific areas reviewed include an analysis of existing wireless related policies, general management and operational practices in effect, and safeguards used to secure city wireless infrastructure and data.

Five year expansion costs expected to be $520,000 with annual maintenance costs of $200,000

The City plans to install approximately 300 additional access points over the next five years. The projected five year cost to install necessary wireless hardware is $520,000 and annual costs are expected to be approximately $200,000.

Auditor General previously reported on management of cellular phones and wireless hand-held devices

In January 2005, the Auditor General made a number of recommendations resulting from a review of management and administrative controls related to the use of cellular phones, wireless hand-held devices and wireless services received by the City from providers such as Telus and Rogers. As a result, this area was not included in the scope of our current review.

In 2005, the Auditor General also carried out a review of management controls exercised over City information technology assets. Through this most current audit, we determined that issues identified in that review have not been completely addressed. The process to account for and monitor wireless assets from acquisition to deployment, and subsequent monitoring needs to be strengthened.

Currently 25 City divisions, the Toronto Police Service and the TTC either use or plan to use wireless applications in the near future

Currently, 25 City divisions, the Toronto Police Service and the Toronto Transit Commission are either using wireless technology or are planning to implement wireless technology in the near future.

Toronto Fire Services, Toronto Emergency Medical Services, Toronto Transit Commission and the Toront o Police Service use their own in-house expertise to independently manage existing wireless technology.

AUDIT RESULTS IN BRIEF

Centralize Oversight of Wireless Technology

Need more centralized management and oversight of City Divisions and ABC wireless technology

From a governance perspective, the City needs to take a more centralized approach to managing and overseeing the development and implementation of wireless technology.

Before proceeding with further development and implementation of wireless technology systems, steps should be taken to ensure wireless projects undertaken by all City divisions are administered under the City's new information technology governance framework.

Toronto Police Service and the TTC independently develop and implement wireless applications and networks

The Toronto Police Service and Toronto Transit Commission independently develop and implement wireless applications.

The Auditor General, in a number of previous IT related reviews, has commented on the need for a close working relationship between the City and its Agencies, Boards and Commissions.

In this context, it is also noteworthy that the Mayor's Fiscal Review Panel report entitled "Blueprint for Fiscal Stability and Economic Prosperity – a Call to Action" includes a recommendation related to improving the alignment, co-operation and increased oversight of the City's Agencies, Boards and Commissions. In their report, the Review Panel states the need for a plan for more alignment, co-operation and increased oversight of City Agencies, Boards, Commissions and Corporations. The Review Panel report further states that such a plan would create more opportunity for savings and joint initiatives.

The development and implementation of wireless technology at the City is, in our view, an area where this recommendation requires consideration.

Develop a Comprehensive Plan for Wireless Technology

A comprehensive IT wireless plan should be developed

A comprehensive plan for wireless technology does not exist. Such a plan serves as the Information and Technology Division's overall program for designing, developing, implementing, supporting and evaluating City efforts in acquiring and using wireless technology.

Although some policies exist, they are not part of a comprehensive City-wide plan which would provide for coordinated development of wireless technology.

Review City-Wide Information Technology Policies

Existing policies are fragmented, obsolete or not formally adopted

The limited wireless technology policies that exist provide some guidance, however, we noted a number of areas where policies are missing, obsolete or have not been formalized.

Management should review existing information technology policies and address gaps identified. Management should also implement a process for periodic review of information technology policies and procedures and modify them as needed.

Implement City-Wide Wireless Technology Standards

Formal wireless standards are required

Formal standards for the acquisition, development and implementation of wireless technology do not exist. Standards ensure information technology devices connected to the City's network are compatible while maintaining a secure environment. Compliance with appropriate standards is generally known to result in greater efficiencies, cost savings and consistent application of security features.

Develop a Comprehensive IT Security Manual

A comprehensive IT security manual should be developed

Knowledge of and compliance with security policies, standards and related procedures by City staff is critical to ensure availability, integrity and confidentiality of data.

While some security policies exist, they are limited, fragmented and not easily accessible. Security policies and standards should be readily available to staff. Generally accepted best practice consolidates all security related policies, standards and procedures into a single comprehensive manual.

Improve Controls to Detect Unauthorized Access Devices

Additional measures to reduce the risk of unauthorized wireless access points are needed

Wireless access points installed without the knowledge, approval or involvement of the City Information and Technology Division presents a risk to the City.

Although current controls in use protect data and reduce overall risk, steps can be taken to further reduce the risk of unauthorized access.

Strengthen Inventory Controls for Wireless Assets

Wireless asset inventory records in the IT Asset Management System are incomplete and periodic inventory counts are not conducted

In 2005, the Auditor General conducted a review of management controls exercised over City's information technology assets. The audit included recommendations in relation to the implementation of the City's Enterprise Information Technology Asset Management System and strengthening inventory controls over information technology assets.

In this most current review, we noted that controls over wireless assets can be improved. Wireless asset inventory records in the Information Technology Asset Management System are incomplete and periodic inventory counts are not conducted. While the scope of this review did not include a review of other information technology assets, the same situation may exist for other IT assets.

Recommendations identified may be applicable to other City organizations

While our review focused on City operations, the eight recommendations included in this report may be applicable to the major City Agencies, Boards and Commissions and as such this report should be forwarded to them for their review and consideration.

BACKGROUND

The wireless network provides user access to many City facilities

Wireless networks enable users to send and receive information within and between City buildings without wires or cables. The City wireless system is an extension of the City's existing wired network providing user access to systems at City Hall, Metro Hall, City civic centres and 15 other locations.

2000 City staff will work in positions where wireless technology provides portability

In recent years wireless applications have been implemented to support a variety of City services including field inspections performed by Municipal Licenses and Standards, Toronto Building, Toronto Water, and Transportation Services. Current projections indicate that over 2,000 City staff will provide services requiring wireless technology in the near future.

25 City Divisions, the Toronto Police Service and the TTC use or are contemplating the use of wireless technology

Currently 25 City business divisions, the Toronto Police Service and the Toronto Transit Commission use wireless applications.

Examples include:

- A City-owned wireless network for nursing home staff
- An Electronic Patient Care Report (ePCR) system which collects patient information and sends information using wireless technology to a central database
- A City-owned wireless network for automated meter reading at Toronto Water
- Toronto Police use of eCOPS, a wireless records management system as well as use of wireless hand-held devices for parking tag enforcement
- TTC use of a wireless arrival notification system.

Information and Technology Division responsible for wireless infrastructure

City-wide responsibility for maintaining wireless technology involves several areas within the Information and Technology Division including Network Services, the Voice and Wireless Network Group, and the Internet/Network Security Group.

As the need for wireless applications arise, City user divisions develop a business case for their respective wireless projects. The user division is also responsible for funding and implementing the proposed wireless application.

The Information and Technology Division's Risk Management Information Security Unit provides overall direction for security, policy and standard setting, and serves a quality assurance role.

New oversight process in effect

The recently implemented Information Technology Governance Framework manages and monitors changes to the wireless network. This framework provides for centralized governance and oversight over all proposed and existing information technology projects including wireless applications.

AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

Why we conducted this audit

Wireless systems are exposed to many of the same risks as wired systems, however, because wireless technology transmits data through air waves, additional vulnerabilities exist. Without adequate protection, wireless communications are exposed to interference by individuals known as "hackers". Hackers have exploited weaknesses in wireless systems to access data and information, launch viruses and deny service to authorized users.

In view of these risks and the expected increase in the City's use of wireless technology, the Auditor General's work plan included a review of the general oversight, management and operational practices, and technical safeguards in place to mitigate such risk.

Audit Objective

The objective of this audit was to determine steps the City has taken to address risks related to the emerging use of wireless technology. Specific areas reviewed include an analysis of existing wireless related policies, management and operational practices in effect, and safeguards used to secure city wireless infrastructure and data.

Audit Scope and Methodology

The scope of the audit included a review of:

- Policies and standards governing City wireless technology
- Wireless security procedures and standards
- Wireless system features used to protect data
- User training and awareness programs

In 2005, the Auditor General made a number of recommendations resulting from a review of management and administrative controls related to the use of cellular phones, hand-held wireless devices, wireless services received by the City from providers such as Telus and Rogers. As a result, this area was not included in the scope of this current review.

Audit Methodology

Our audit methodology included the following:

- review of Council and Standing Committee minutes
- review of documents, management reports, policies, procedures and related records
- interviews with Information and Technology Division staff
- review of external City of Toronto Wireless Strategy reports
- analysis of wireless inventory records and financial records
- review of wireless security standards and practices documented by professional organizations including Information Systems and Controls Association (ISACA), Institute of Internal Auditors (IIA) and SANS a leading organization in security certifications and training
- review of related audit reports conducted by other municipalities.

Compliance with generally accepted government auditing standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

AUDIT RESULTS

1. Centralize Oversight of Wireless Technology

More centralized management and oversight of wireless development and implementation by City Divisions

From a governance perspective, the City needs to take a more centralized approach to managing and overseeing the development and implementation of wireless technology.

The City recently established two new groups to provide governance for information technology projects designed, developed and implemented across the City. The two groups are known as the Business Advisory Panel and the Enterprise Architecture Review Panel.

The Business Advisory Panel provides strategic direction, establishes business priorities and guides City investment in information and technology.

The Enterprise Architecture Review Panel is a sub-committee of the Business Advisory Panel. The Panel guides the development of City-wide computer development and ensures appropriate standards are in place and followed.

Before proceeding with further development and implementation of wireless technology systems, steps should be taken to ensure wireless projects undertaken by all City divisions and the major City Agencies, Boards and Commissions are administered under the City's new information technology governance framework.

Recommendation:

1. **The Chief Information Officer ensure current and future wireless projects undertaken by City divisions are administered under the Information Technology Governance Framework.**

City ABCs independently develop and implement wireless applications

The Toronto Police Service and Toronto Transit Commission independently develop and implement wireless applications. The Auditor General, in a number of previous IT related reviews, has commented on the need for a closer working relationship between the City and its Agencies, Boards and Commissions.

Mayor's Fiscal Review Panel recommended improvements in coordination and cooperation with City ABCCs

In this context, it is noteworthy that comments made by the Mayor's Fiscal Review Panel include recommendations related to improving the alignment, co-operation and increased oversight of the City's Agencies, Boards and Commission. In their "Blueprint for Fiscal Stability and Economic Prosperity – a Call to Action," the Mayor's Fiscal Review Panel states the need for:

"A plan for much more alignment, cooperation and increased oversight of the 119 Agencies, Boards and Commissions and Corporations creating more opportunities for savings and joint initiatives."

In that same report, Panel members further state that the:

"*City should develop a program to require much more coordination, cooperation with shared best practices, and cost sharing between the City and the ABCCs."*

The development and implementation of wireless technology at the City is an area where this recommendation requires consideration.

Recommendation:

2. The Chief Information Officer ensure measures to provide a consultative and collaborative role on wireless projects undertaken by City Agencies, Boards and Commissions are implemented.

2. Develop a Comprehensive Plan for Wireless Technology

The Information and Technology Division supports technology including use of wireless technology

The overall mission of the Information and Technology Division is to support City computer, data and information needs. The Information and Technology Division collaborates with user divisions to develop improvements in City service delivery through technology. Wireless technology used to support City divisions includes wireless access points connected to the City's wired network, as well as wireless devices such as cell phones and hand-held devices using external cellular service networks.

Comprehensive IT wireless plan does not exist

A comprehensive wireless plan represents the Information and Technology Division's overall plan to define what must be achieved in the future to support the City's future wireless activities. Such a plan does not exist.

The Information and Technology Division has implemented a number of policies including:

- Wireless Communication Devices Policy

  This policy governs the purchase, use, maintenance and billing of wireless communication devices such as cell phones and hand-held devices connected to external service providers.

- Remote Access Policy

  This policy governs employee remote access to the City network.

- Acceptable Use Policy

  This policy outlines proper use of information technology resources.

A number of policies exist which add value but are not a substitute for an overall IT wireless plan

These policies are necessary and useful, but they are fragmented and address specific topics. They are not a substitute for a comprehensive wireless plan. These individual policies should fit within a broader plan. A comprehensive wireless plan provides for a common understanding and commitment by management as to the City's overall IT wireless direction and how this direction conforms with City service objectives.

The plan should consider future demand, projected costs, required user support, compatibility and training

Such a plan should consider future demand for wireless technology as well as cost projections, required user support, compatibility and training. Security and confidentiality issues are also key considerations.

The plan should encompass all types of wireless technology used by the City.

Recommendation:

3. The Chief Information Officer prepare a comprehensive City-wide Information Technology Wireless Plan and periodically review the plan to ensure that it is current and relevant.

3. Review City-Wide Information Technology Policies

IT policies provide guidance to City staff

Information technology policies provide guidance to user divisions on acceptable computer practices. Policies also provide senior level employees with a basis for consistent management, decision-making and resource allocation.

IT policies reviewed were incomplete, outdated and not always formally approved

Our review highlighted areas where policies are needed but do not exist or have not been formalized. For example, there is no policy outlining requirements in areas such as:

- IT Security Incident Reporting
- IT Security Risk Management
- Network Access For Third Parties

The City-wide Corporate Information Security Policy issued in 2005 should include references to policies and standards related to wireless technology. The policy has not been reviewed or revised since it was issued.

Need for management to review and address gaps in IT policies

Management should review existing information technology policies and address identified gaps. Policies should also be reviewed on a regular basis.

Recommendation:

4. **The Chief Information Officer complete a review of City-wide information technology policies to ensure policies are prepared, approved and reviewed on a regular basis.**

4. Implement City-Wide Wireless Technology Standards

Wireless hardware and software standards ensure information technology assets connected to the City's network are compatible and work together to maintain a secure environment.

Standards can lead to efficiencies and cost savings

Standards are also useful in minimizing the number of different types of hardware and software used by the City. Compliance with hardware and software standards is known to result in lower purchase and maintenance costs.

Standards provide for consistent application of security features

Security standards define minimum security requirements and provide for consistent application of security features to reduce risk.

City-wide wireless standards have not been fully developed, approved or widely distributed.

Recommendation:

5. **The Chief Information Officer implement City-wide wireless standards and develop procedures to provide for periodic review to ensure the accuracy and relevancy of wireless standards.**

5. Develop a Comprehensive Information Technology Security Manual

IT policies, procedures, standards and guidelines are electronically available

Some information technology policies, procedures, standards and guidelines are electronically available to City staff on the Information and Technology Division's intranet Web site. Documents are listed alphabetically and cover many information technology topics.

Security policies and standards are not always easy to find

The Information and Technology Division's Web site includes useful information, however, there are sections that are cumbersome and time consuming to search. Although documents are alphabetically ordered the entire listing has to be scanned to find certain documents. As an example, the policy entitled "Corporate Information Security Policy" is located in the 'P' section of the alphabetical listing under a sub-section entitled "Approved Policies".

A comprehensive IT security manual is needed

Knowledge of and compliance with security policies and standards by City staff helps ensure availability, integrity and confidentiality of data. A comprehensive Information Technology Security Manual promotes knowledge and awareness of current information technology security policies, practices, standards and procedures.

A comprehensive Information Technology Security Manual should include a master index for ready access to contents and assist in identifying topics that have not been addressed.

Such a manual serves as a ready reference for users which will improve the ability of City staff to quickly access, review and act on, in relation to the City's overall information technology security requirements.

All security related policies and standards should be incorporated into an approved comprehensive IT Security Manual. The Manual should be readily available to City staff.

Recommendation:

6. The Chief Information Officer develop a comprehensive Information Technology Security Manual as a ready reference for City staff.

6. Improve Controls to Detect Unauthorized Access to Wireless Devices

Additional measures are required to reduce the risk of unauthorized wireless access

Wireless access points installed without the knowledge, input and approval of the Information and Technology Division are a risk to the City. Controls currently in place reduce the risk of unauthorized access to City data.

Currently, controls used to reduce the risk of unauthorized access to City data include the use of an electronic barrier known as a firewall which regulates data received and sent, anti-virus software to protect against viruses, and the requirement for user identification and password protection to access the City's network.

Although current controls protect data and reduce the risk of unauthorized access, further steps can be taken to reduce the risk. For example, implementation of a policy clearly stating the consequences of unauthorized access to City wireless devices.

As part of the Information and Technology Division's program to secure City data, further steps should be taken to ensure cost-effective measures are in effect to reduce the risk of unauthorized wireless access to City data.

Recommendation:

7. The Chief Information Officer implement additional measures to further reduce the risk of unauthorized access to City wireless technology.

7. Strengthen Inventory Controls for Wireless Assets

The Auditor General previously recommended improvements in controlling IT assets

In 2005, the Auditor General conducted a review of management controls exercised over City information technology assets. As a result recommendations were made to give priority to the implementation of the City's Enterprise Information Technology Asset Management System, conduct periodic asset inventory counts and resolve discrepancies identified at the time of the count.

Wireless asset inventory records in the IT Asset Management System are incomplete and periodic inventory counts are not conducted

Although the Unit responsible for deploying wireless assets maintains a record of wireless assets purchased and deployed, wireless inventory records in the City-wide Information Technology Asset Management System are incomplete.

Our review of controls over wireless assets indicated:

- inventory records for these assets do not contain required data
- the location of wireless assets in use is not identified in the asset management system
- periodic inventory counts of wireless assets are not conducted.

Inventory controls over other IT assets may also require strengthening

Although we did not review inventory controls over other information technology assets, the same condition may exist for other IT assets.

Recommendation:

8. The Chief Information Officer ensure information technology inventory records are complete and controls are working as intended.

CONCLUSION

Eight recommendations related to improving and managing City wireless technology

This report contains eight recommendations related to improvement in the management and administration of City wireless technology.

As report recommendations may have relevance to City Agencies, Boards and Commissions, the report should be forwarded to the City's Agencies, Boards and Commissions for review and consideration.

Implementation of the recommendations in this report will provide an effective framework for overall direction and guidance related to City wireless technology. Implementation will also ensure more cost effective deployment and use of wireless technology.