APPENDIX 1

REMOTE ACCESS TO THE CITY'S COMPUTER NETWORK – THE MANAGEMENT OF THE PROCESS REQUIRES IMPROVEMENT

May 27, 2011

TORONTO Auditor General's Office

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Why we did this review

Many City staff need to access the City's computer network from other than their normal work locations. To enhance the security of such access, authorized staff are issued a device known as a remote secure access token. The management of the secure access tokens is the responsibility of the Information and Technology Division. The licence agreement for individual tokens is for a four-year period.

During a general review within the Auditor General's Office of the use of remote access tokens it was noted that the renewal of a recently expired token had only 75 per cent of its useful life remaining. In this context, it was apparent that of the total cost of the token, 25 per cent had already been expended even though the token had not been in use. As a result of this issue we reviewed the process in place to ensure that the City was receiving full value for the funds expended on the tokens.

By our calculations, approximately $40,000, or 20 per cent of the token supply contract costs, could have been avoided over the four-year contract had tokens been ordered only when needed by staff. In addition, maintaining a supply of tokens for emergencies costs the City $17,000 per year. Alternatives for emergency access could reduce this cost.

Review identified three areas where improvements could be made

The review identified the need for:

1. Improvements to token requirement estimates provided to Information and Technology by operating divisions.

2. A review of the process for charging the cost of the token program back to operating divisions.

3. Completion of an assessment and decision on alternatives for remote access service delivery prior to the December 31, 2011 expiration of the current agreement with the supplier of remote access tokens. Such a review to include remote access requirements in an emergency.

This report contains three recommendations which, in our view, will further improve the cost-effectiveness of the remote secure access token process.

BACKGROUND AND OBJECTIVES

At each employee's work location, the City's computer network is accessible by entering the correct combination of user identification and password.

Network access from non-connected computers is a security risk

Remote access to the City's computer network presents a particular security challenge since the access is from a computer not directly linked to the network, and therefore not "trusted". In order to access information and systems stored on the City's network it is necessary to implement additional security to verify that the attempted access is by an authorized individual.

City uses "tokens" to add security to remote access

A common solution to remote access security concerns is to issue staff a remote secure access token. In the City's case, this token displays a six digit number that changes every 60 seconds. This changing number is recognized by software on the network. Staff retain the same token for its full four-year lifespan.

Enhancing remote access security comes at a cost

Remote secure access tokens and related licences are priced on a per user basis and the costs charged back to City divisions as tokens are issued. The tokens themselves have a four-year lifespan after which they expire and must be replaced with a new token. The tokens are managed by the Information and Technology Division.

As users of these tokens, staff of the Auditor General's Office noted that tokens were issued to the Auditor General's Office with only three years remaining in their useful life.

The objective of this review was to assess the procedures and controls over the acquisition and distribution of remote secure access tokens to ensure the process is being effectively managed.

This audit covered the period from January 2009 to April 2011.

Our audit methodology included the following:

- interviews with City staff;
- review of documents, management reports, policies, procedures and related records;
- examination of documents and records;
- evaluation of management controls and practices; and
- other procedures deemed appropriate.

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 to provide 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

ESTIMATING TOKENS FOR FUTURE USE

Tokens are shipped to the City in bulk so need to anticipate token requirements

To ensure tokens are available as required, current procedures require the City to estimate the need for tokens and keep a sufficient inventory to be issued to staff when requested. Based on divisional estimates of tokens required, a competitive process was undertaken and a contract signed with a token provider. Token providers generally ship tokens in bulk which, in the City’s case, means shipments in the range of 800 tokens per shipment.

Token’s four-year lifespan begins immediately on receipt by the City

The tokens become active as soon as they are shipped to the City. This means that the four-year lifespan of the token begins immediately. Related software licences are also payable, even though the token may not be issued to staff.

The need for tokens was significantly over estimate.

Estimations of token requirements provided to the Information and Technology Division by other City divisions were significantly in excess of subsequent actual usage. For example, in October 2010, there were approximately 1,500 tokens in inventory while only 3,000 were being used by staff. We understand that the high level of inventory was generally attributable to estimates provided by Toronto Public Health in anticipation of the implementation of a new computer system. Delays in implementing the system led to actual issuance of tokens being significantly below the estimate.

Specifically, in April 2009 Toronto Public Health indicated they would require 750 tokens between then and December 31, 2010. As at April 2011, Toronto Public Health had only requested 225 tokens.

Tokens expire while held in inventory representing unnecessary costs for the City

Since the City has contractual obligations for specific shipments of tokens, the shortfall in tokens required resulted in excess tokens in inventory and an unnecessary cost to the City. Although staff were able to arrange with the vendor to delay certain shipments, the City still had an excess supply of tokens resulting in unnecessary costs.

The contract with the token supplier specifies that a total of 3,600 tokens were to be delivered on four different dates. To maximize the useful life of tokens they should be delivered to the City as close as possible to the date required by staff.

Cost of excess tokens estimated at $31,000

The City's supply of tokens exceeds current demand and tokens are issued to City staff up to a year after having been received. We estimate the cost associated with the reduced lifespan for tokens purchased as part of this four-year contract to be approximately $31,000 or 20 per cent of the purchase cost of the tokens.

The contract also includes the purchase of new licences and the cost to renew existing licences. At the time of our review there were 1,202 licences available and not in use, (excluding 400 licences held as an emergency preparedness measure). According to management's projection these licences are not expected to be fully used until February 2013.

Additional $9,000 in licence maintenance costs for unused tokens

The initial cost for these licences was in the range of $43,600 and the City pays approximately $6,800 annually in licence maintenance fees for these unused licences. Assuming the historical pattern of token issuance, the excess costs for unused licences is in the range of $9,000 in total.

We appreciate that it may be difficult to arrange for delivery of tokens in a fashion that exactly matches the need. However, it is our view that the extent of the tokens in inventory is excessive. Since divisions are only charged for tokens once they are issued, one solution may be to alter procedures such that charges to divisions take into account costs incurred as a result of inaccurate estimates provided to Information and Technology Division.

Recommendations:

1. **City Council request the Chief Information Officer to advise divisions of the impacts of inaccurate estimates for the supply of remote secure access tokens and stress the importance of providing accurate projected estimates.**

2. **City Council request the Chief Information Officer to revise the procedures for charging back the cost of remote secure access tokens such that divisions are charged for costs incurred where estimates are significantly in excess of actual requirement.**

ALTERNATIVES TO CURRENT REMOTE SECURE ACCESS MODEL

Current practice results in tokens expiring even though they are not being used

Remote secure access tokens are held in inventory until issued to staff. Consistent with industry practice, the City receives bulk shipments of tokens. This results in the City having a supply of unused tokens in inventory. The four-year life of the token begins as soon as the token is delivered to the City. Any time a token spends in inventory represents an unnecessary cost to the City.

The issue with the current process is not only a matter of estimations used to order tokens, but also industry practice that dictates the life of a token begins on delivery rather than when the token is put into use.

There are alternatives to tokens for secure remote access

We are aware that there are alternatives other than remote access tokens to verifying the identity of users accessing networks from remote locations.

Contract with token vendor expires December 31, 2011

The current contract for the supply of remote access tokens expires in December 2011. Staff should ensure that other alternatives to remote secure access to the City's network are fully explored in a time frame that ensures cost-effective continuity of this service for City staff.

400 tokens kept for emergency situations

The Information and Technology Division keeps a minimum supply of 400 tokens for distribution in the event of an emergency. The cost, including licence fees, of keeping these tokens available for an emergency is $17,000 per year.

We understand that a thorough analysis was undertaken in April 2008 to determine the number of tokens that should be kept in the event of an emergency. Given the annual cost of maintaining these tokens it may be prudent to request divisions to review their future requirements.

Alternatives for emergency preparedness are being investigated

Further, Information and Technology staff indicate that they are currently investigating alternative methods of accommodating emergency remote access to the City's network. These alternatives may eliminate the need for an inventory of tokens for an emergency.

Recommendation:

3. City Council request the Chief Information Officer to explore the options available for staff to remotely access the City's network to ensure the most cost-effective solution is implemented prior to December 31, 2011.

CONCLUSION

This report presents the results of our review of the City’s program for providing secure remote access to the City’s computer network. We have three recommendations aimed at improving the cost-effectiveness of the program.

While the cost savings identified in the report are not significant any circumstances which identifies any level of savings should be explored.