TORONTO

STAFF REPORT
INFORMATION ONLY

Response to the 2006 City of Toronto Audit Results and Letter of Recommendations

Date:	January 30, 2008
To:	Audit Committee, City of Toronto
From:	Alok Mukherjee, Chair, Toronto Police Services Board
Reference Number	07-AU3.3

SUMMARY

The purpose of this report is to provide the Audit Committee with the response to the 2006 City of Toronto audit results and letter of recommendations.

Financial Impact

There are no financial implications with regard to the receipt of this report.

ISSUE BACKGROUND

At its meeting held on December 19, 2007, the Toronto Police Services Board was in receipt of a report, dated November 26, 2007, from Chief of Police William Blair regarding the response to the 2006 City of Toronto audit results and letter of recommendations.

COMMENTS

The Board received the Chief's report and agreed to forward a copy to the City of Toronto – Audit Committee for information.

A copy of Board Minute No. P397/07, in the form attached as Appendix "A", regarding this matter is provided for information.

CONTACT

Chief of Police William Blair
Toronto Police Service
Telephone No. 406-808-8000
Fax No. 416-808-8002

SIGNATURE

____

Alok Mukherjee
Chair, Toronto Police Services Board

ATTACHMENT

Appendix A – Board Minute No. P397/07

A: city report audit.doc

APPENDIX A

THIS IS AN EXTRACT FROM THE MINUTES OF THE PUBLIC MEETING OF THE TORONTO POLICE SERVICES BOARD HELD ON DECEMBER 19, 2007

#P397. RESPONSE TO THE 2006 CITY OF TORONTO AUDIT RESULTS AND LETTER OF RECOMMENDATIONS

The Board was in receipt of the following report November 26, 2007 from William Blair, Chief of Police:

Subject: RESPONSE TO 2006 CITY OF TORONTO, AUDIT RESULTS, LETTER OF RECOMMENDATIONS

Recommendation:

It is recommended that the Board receive this report.

Financial Implications:

There are no financial implications relating to the recommendation contained within this report.

Background/Purpose:

The Board requested a status update on the recommendations made in the letter from Ernst & Young supplied to Dr. Alok Mukherjee, Chair of the Toronto Police Services Board dated August 20, 2007.

As part of the examination of the consolidated financial statements of the City of Toronto, Ernst & Young considered the City's internal control structure to determine auditing procedures for the purpose of expressing an opinion on the financial statements. Certain matters came to their attention where they felt management could either strengthen or improve efficiencies within the current processes. Their study and evaluation disclosed no condition that they believed to be a material weakness, but did disclose certain areas that they felt should be reviewed by management. As part of the 2006 audit, there were two recommendations by Ernst & Young that pertain to the Toronto Police Service (TPS). In addition, two recommendations were carried forward from the 2001 Ernst & Young Letter of Recommendations.

Discussion:

Updates on the four on-going recommendations within the report that relate to the Toronto Police Service are as follows:

2006 - Toronto Police Service ("TPS") - Information Technology – Employee Terminations

Monthly termination listings should be provided to the ERMS user administration group on a timely basis and documentation of the review should be retained to provide evidence of the timeliness of user termination processes for all user accounts removed from the system.

In addition, management should review the feasibility of logging user account changes in the Peoplesoft application to provide an audit trail of activities performed and to provide evidence of timely user administration processing.

2006 Management Comments:

The ERMS unit has made a request of the Unit Commander of the Professional Standards Unit to receive notification of terminations on a timely basis. Once the information is received, the proper action is promptly initiated by the ERMS unit and records are kept within the unit that pertains to security changes. The ERMS unit does manually log the security changes and has noted the recommendation to change the PeopleSoft application to maintain a log of those changes. That request for a change to the application will be reviewed and assessed for possible implementation in the future.

2007 Management Comments:

The Enterprise Resource Management Systems (ERMS) unit now receives a report detailing status changes for Service employees. This listing is produced by Communications and System Operations Services on a daily basis. ERMS unit application specialists review the listing and make changes to user accounts, in particular account deletions when appropriate. The Service considers this recommendation to be fully addressed.

2006 – TPS - Information Technology – Privileged Access to Time Recording Management System Application

We recommend that this level of access be revoked from this user. In addition, we recommend that privileged access to the TRMS application be reviewed on a periodic basis to ensure that access of a privileged nature is restricted to authorized individuals in line with their job function.

2006 Management Comments:

The Information Systems Services Project Leader did not realize the level of access that was in place. The level of access has been reduced to the appropriate and required level, Admin Level, and process will be put in place so this doesn't happen again.

2007 Management Comments:

Requests for access to the Time and Resource Management System (TRMS) application must be submitted by the member's unit commander with a description of the need for the level being requested. These requests are reviewed by ERMS unit application specialists before being actioned. As well, the Service is in the process of upgrading the TRMS system. The security module is being reviewed as part of this process. This application will be upgraded in second quarter of 2008, at which time, the recommendation will be considered fully addressed.

2001 – TPS - Information Technology – Disaster Recovery Planning

TPS should consider developing continuity and recovery plans for business support systems. This process should begin with a "business impact analysis" as a basis for determining the timeframe within which critical business processes need to be restored. Disaster recovery plans should then be developed to allow TPS to restore its information technology on a timely basis and to ensure minimum basic functions are carried out in the interim.

2005 Management Comments:

Data is currently maintained offsite on backup tapes which are periodically rotated. The TPS has an approved three year plan to populate its systems at a Disaster Recovery Centre and have classified all current systems as to their importance and impact to the organization. All new systems which are deemed to be Class "A" (critical) will be targeted to run simultaneously at both the Disaster Recovery Centre and the normal Operations Centre. Hardware is currently being installed at the Disaster Recovery Centre and the operation of the architecture and Class 'A' systems at both sites is scheduled to proceed to mid 2006. Class 'B' and 'C' systems are currently being evaluated and a decision on the best method of providing recovery facilities is expected to be implemented in 2006.

2006 Update:

We understand that a disaster recovery project is currently under way and will concentrate on those applications and supporting infrastructure deemed 'Class A' systems. We support this initiative and encourage management to ensure that plans for the 'Class B' systems (including the financial systems) are developed to allow Toronto Police Services to restore its information technology on a timely basis in the event of a disruption of service.

2006 Management Comments:

The Business Units associated with the Class B applications have reviewed the Disaster Recovery plans. Class B systems would be returned to full service over the course of one to four weeks. The Business Units have confirmed that during the period, transactions would be processed manually and any backlog can be managed.

2007 Management Comments:

The Disaster Recovery plan is the same as that referenced in the Ernst & Young 2006 report. Additional feasible options are dependent on the Disaster Recovery budget.

Currently, TPS is working on Class "A" applications and the activity to establish a disaster recovery environment with the City at 703 Don Mills. Once Class "A" applications are completed, the project will review the Class “B” applications should there be any funds remaining. No further plan is anticipated until additional funding is available.

2001 – TPS - Information Technology – Information Security

We recommend that consideration be given to improving information security across all of TPS’s administrative computer systems by improving password security at the network, operating system and application level. This would involve enforcing a minimum password length for all applications, a lockout after repeated invalid access attempts, and regular password aging. We also recommend that NT security logs be reviewed in order to detect potential invalid access attempts, or other unusual activity.

2005 Management Comments:

All logs for the log in system are captured centrally and used for investigation and audit purposes. The migration from the current NT environment to an XP environment will be completed by March 2006 and will enable system and application authorization and user authentication processes to be facilitated with Active Directory, a component of the XP operating system. Strong authentication requirements will be implemented late in the year with the development of a password policy which will specify the minimum length of password, password aging period and a limited period and a limited period to login in order to prevent unauthorized access. This will be completed by the end of 2006.

2006 Update:

This matter was unresolved as of the completion of our audit field work date.

2006 Management Comments:

Two Factor Authentication has now been implemented and meets all of the recommended requirements regarding length of password, password history, password aging and establishing an account lockout policy.

2007 Management Comments:

As reported in the Ernst &Young 2006 report, the Strong Authentication project has been completed and the recommended requirements regarding length of password, password history, password aging and establishing an account lockout policy have been implemented. The Service considers this recommendation to be fully addressed.

Conclusion:

Four on-going recommendations were contained in the 2006 Ernst & Young Letter of Recommendations that pertains to the Toronto Police Service. Two of the recommendations related to 2006 findings and two recommendations were carried forward from 2001. The recommendations related to employee terminations and information security have been fully addressed and the recommendation related to privileged access will be addressed once changes to the TRMS system are made in second quarter of 2008. The recommendation pertaining to Disaster Recovery Planning continues to be addressed.

Deputy Chief Jane Dick, Executive Command, will be in attendance to answer any of the questions that Board members may have.

The Board received the foregoing report.