TORONTO STAFF REPORT

March 30, 2004

To: Audit Committee

From: Auditor General

Subject: Toronto Maintenance Management System Application Review

Purpose:

The purpose of this audit was to assess how well the Toronto Maintenance Management System supports the Transportation Services Division's business objectives and whether the implementation and ongoing development of the system is carried out with due regard for economy and efficiency.

Financial Implications and Impact Statement:

There are no immediate financial implications resulting from the adoption of this report. The adoption of the recommendations in our view can be accommodated with existing resources.

Recommendations:

It is recommended that:

(1) City Council direct that this report be forwarded to all City Departments, Agencies, Boards and Commissions. These entities be required to review the recommendations in this report to determine whether or not they have relevance to their operations and take appropriate action where necessary;

(2) the Commissioner, Works and Emergency Services, review the current practice for entering data in the Toronto Maintenance Management System. Such a review ensure that:

   (a) the exercise to harmonize business practices is completed;

   (b) the rules and requirements for entering data into the Toronto Maintenance Management System are developed and are appropriately and consistently followed in the Districts; and

(c) the data requirements are sufficient to create meaningful reports that will allow management to monitor activity and effectively carry out its responsibility;

(3) the Commissioner, Works and Emergency Services:

(a) identify all outstanding requests for enhancements or modifications to the Toronto Maintenance Management System;

(b) analyze the costs and benefits of each potential change;

(c) prioritize the enhancements based on the cost benefit analysis; and

(d) ensure that the above steps are documented and approved by appropriate supervisory staff;

(4) the Commissioner, Works and Emergency Services, submit to the SAP Competency Centre a current updated version of its business case for implementing an electronic interface between SAP and the Toronto Maintenance Management System;

(5) the Commissioner, Works and Emergency Services, complete the necessary steps to mitigate security weaknesses within the Toronto Maintenance Management System. These steps to include; identifying threats to the data and resources, performing an analysis to determine how the existing security measures protect against these threats and, implementing additional processes and controls identified as a result of this analysis;

(6) the Commissioner, Works and Emergency Services, implement a security governance framework for the Toronto Maintenance Management System. The framework should outline the standards to be followed, the duties to be performed and the staff position responsible for overseeing the security for the system;

(7) the Commissioner, Works and Emergency Services, implement formal procedures, for granting or removing a user's access to the Toronto Maintenance Management System. These procedures to include, but not be limited to; approval requirements, assigning user group(s), procedures to deal with contractors, temporary workers, as well as transferred and terminated employees, and the maintenance of appropriate documentation in support of the access privileges granted;

(8) the Commissioner, Works and Emergency Services, direct that a review of current user access rights be performed and that such a review be conducted on a regular basis to confirm that user access rights are compatible with job functions and responsibilities;

(9) the Commissioner, Works and Emergency Services, ensure that:

(a) the assignment of individuals to the "Administrator" user group is commensurate with operational requirements; and

(b) individuals, who are required to perform administrative duties in addition to daily operational duties, be given a second user account for their operational function;

(10) the Commissioner, Works and Emergency Services, implement a process for tracking activity on the Toronto Maintenance Management System. The tracking strategy consider; the activities or actions to track, the generation of exception reports for review on a regular basis, and follow-up steps for exceptions noted. Further, the Division consult with Records & Archives Division of the Clerks Office, to determine the appropriate retention period for audit records maintained within the system;

(11) the Commissioner, Works and Emergency Services, ensure that passwords associated with the Toronto Maintenance Management System are encrypted and password management practices, such as setting a standard minimum length for the password forcing regular password changes, etc., are implemented;

(12) the Commissioner, Works and Emergency Services, ensure that each user is provided with a unique User-ID and that the naming convention used be designed to give indication as to the owner of the User-ID;

(13) the Commissioner, Works and Emergency Services, ensure that:

(a) a business continuity plan that integrates operational needs with the technology component of the Toronto Maintenance Management System is prepared, and that such a plan is documented and tested on a regular basis; and

(b) this plan be incorporated into the departments overall disaster recovery plan;

(14) the Commissioner, Works and Emergency Services, implement a process to prioritize, justify and approve the implementation of all changes to the Toronto Maintenance Management System;

(15) the Commissioner, Works and Emergency Services, ensure that staff sign the Task Control Sheet to signify the approval to proceed with the changes to the system and sign again to acknowledge acceptance of the completed change;

(16) the Commissioner, Works and Emergency Services, document procedures for emergency changes and that these procedures be complied with and include the necessary user validation and authorization after the change has been made;

(17) the Commissioner, Works and Emergency Services, investigate the opportunity for using the automated test tool available from the Corporate Information and Technology Division in future system changes or system development projects;

(18) the Commissioner, Works and Emergency Services, conduct a thorough analysis of the reporting requirements of the users of the Toronto Maintenance Management System and consider these needs in further developing the system;

(19) the Commissioner, Works and Emergency Services, ensure that the development of reports follow a consistent process. That process to include defining the user's requirements, obtaining the necessary approval, testing for accuracy and receiving final user acceptance before adding a customized report to the Toronto Maintenance Management System;

(20) the Commissioner, Works and Emergency Services, ensure that third parties granted access to the Toronto Maintenance Management System be contractually required to adhere to acceptable use policies similar to those in place for City employees;

(21) the Commissioner, Works and Emergency Services, ensure that all future development and enhancements to the Toronto Maintenance Management System adhere to project management practices and standards, including a system to capture and report on the costs of projects;

(22) the Commissioner, Works and Emergency Services, develop a project plan outlining all outstanding tasks appropriately prioritized, scoped, and approved and the estimated costs (including staff time) to complete the plan be reported to the Works Committee. The plan should be adhered to and any subsequent requests, unless deemed emergency or essential, be deferred;

(23) the Commissioner, Works and Emergency Services, ensure that Toronto Maintenance Management System response times (i.e., making the system faster for the user) are included as one of the outstanding enhancement projects to be analyzed and prioritized; and

(24) the Commissioner, Works and Emergency Services, report back to the Audit Committee scheduled for July 13, 2004, on a work plan in regard to the implementation of the recommendations contained in this report. Such report to include specific timelines for implementation.

Background:

The City of Toronto manages approximately 5,300 km of roads, 7,100 km of sidewalks, 530 bridges, 600 pedestrian crossovers, 160,000 streetlights, 1,940 traffic control signals, 4,100 bus shelters, one million signs, as well as over 100 km of bicycle lanes and trails. The Transportation Services Division, within the Works and Emergency Services Department, is accountable for the expansion and maintenance of the City's network of roads and infrastructure designed to meet the mobility needs of people and goods within and around the City of Toronto. The Division has divided its operations into four separate Districts to facilitate the management of its operations.

Managing the maintenance of the City's extensive network of roads is a formidable task, which can not be conducted manually. To assist in this task, City staff developed the Toronto Maintenance Management System. This is a comprehensive information system, used in the administration of the Transportation Services Division's annual budget of over $160 million and,

when fully implemented, will help in the management of the activities of more than 1,100 staff, as well as the management of various activities such as: emergency road repairs, pothole repairs, permanent asphalt repairs, curb repairs, replacing concrete in sidewalks, etc., performed by the operating units within the Transportation Services Division. The system is designed to capture service requests, route them to appropriate operating units, set up projects and work orders, and record labour, materials, and equipment used. Although primarily used by the Transportation Services Division, the Parks and Recreation Division also uses components of the system to manage its forestry operations.

The Toronto Maintenance Management System currently used by the City is the result of enhancements to one of the maintenance management systems in existence at the time of amalgamation. Since the year 1999, approximately $4 million has been invested by the City to enhance the system. This investment was made to increase efficiencies, reduce costs, and improve customer service in maintaining and improving the road system within the City of Toronto.

Audit Objectives and Scope

The Toronto Maintenance Management System is a critical tool for the management of the Transportation Services Division's operations. Our objectives for auditing the Toronto Maintenance Management System were to assess how well the system supports the operations of the Transportation Services Division and whether the ongoing development and delivery of the system is in accordance with best practices and with due regard for economy and efficiency. The audit objectives were achieved through the evaluation of:

- the effectiveness of the Toronto Maintenance Management System in meeting business objectives;

- the contribution of the Toronto Maintenance Management System to the efficiency of operations within the Division;

- the administrative and system controls in effect to ensure data accuracy and integrity;

- the security practices/procedures governing transactions and data handled by the Toronto Maintenance Management System;

- the ability of the Transportation Services Division to recover the system and continue operations if a disaster were to occur; and

- the strategy and plan in place for making changes to the Toronto Maintenance Management System.

Our review was based on published standards such as the Control Objectives for Information Technology issued by the Information Systems and Control Association and best practices related to systems, policies, and procedures that the Division should have in place. The scope of our audit included discussions with staff, a review and analysis of relevant policies, procedures,

and related documents provided by the Division, and included such tests and other procedures as we considered necessary in the circumstances.

Summary of Significant Audit Observations

The following is a summary of the major issues identified during our review. Details supporting these observations, along with our recommendations, are provided in the body of this report.

1. The Toronto Maintenance Management System supports the operations of the Transportation Services Division. The use of the system has resulted in considerable improvements in the Division's ability to effectively manage the maintenance of roads and traffic signs. Contracts in excess of $100 million annually are managed using the system. In addition the system is used for in-house services and has the ability to track work requests and is used to plan, schedule and track the use of staff resources.

2. The Toronto Maintenance Management System has been beneficial in bringing automation to those districts and areas, which in the past relied on paper-based systems. The system provides management with timely information to track, monitor and manage activities carried out to expand or maintain the City's road infrastructure.

3. The Toronto Maintenance Management System has the potential to provide management with the ability to:

   - identify costs associated with key activities, such as the cost to repair a pothole;
   - optimize performance based on analysis of data captured by the system;
   - perform best practice comparisons using data provided by the system; and
   - monitor and track infrastructure assets and make informed business decisions.

   Significant work is still required to allow the system to reach its full potential. As an example, business practices for entering data into the system are not the same in all districts. This lack of consistency detracts from the effectiveness of reports produced by the system.

4. The Transportation Services Division's attempts to integrate the Toronto Maintenance Management System with the City's financial and human resource systems have proven unsuccessful. There is no framework in place to address requests from departments to integrate individual business systems with the corporate wide financial and human resource systems. We have previously addressed this issue in our report dated April 4, 2003, entitled "SAP Financial and Human Resources/Payroll Information System – Post Implementation Review" where we recommended that the Commissioner, Corporate Services, work with departments to coordinate the implementation and integration of major information systems. This coordination process is underway and will address the integration of the Toronto Maintenance Management System with other City systems.

5. The development of the Toronto Maintenance Management System was not managed in accordance with generally accepted project management principles. In general, little attention was given to controlling the project, particularly in the areas of planning, scoping the project, and reporting progress against the plan.

6. There is a need to strengthen the security policies, procedures and practices for the Toronto Maintenance Management System. Several security-related practices should be implemented by management to protect data from unauthorized changes, access or disclosure. Good security is critical to the successful use of the system. If security is inadequate, the Transportation Services Division risks not having accurate and reliable information to achieve its goals.

7. The adoption and enforcement of a set of common data entry rules and requirements is required to ensure that data for labour, material, equipment usage and performance measurements (for example, number of potholes repaired) is complete and consistently entered by the Districts.

8. Third party contractors are being given access to the Toronto Maintenance Management System in order to input details of work completed. The agreements covering this access do not identify any accountability or responsibility on the part of the Contractor for the use of the City's information technology infrastructure. Third party users should be bound by standards such as the "Acceptable Use Policy" that exists for City employees.

9. The backup and recovery procedures for the Transportation Services Division are not formalized, documented and integrated into the overall corporate business continuity plan. The plan should include the processes to be followed by the business user, as well as the steps to be followed to recover the required information technology resources. Further, the existing informal procedures are not tested on a regular basis to ensure the ability to provide database processing in the event of a disaster.

Further details relating to these observations are contained in the following paragraphs.

Comments:

Certain recommendations contained in this report may have relevance to other systems throughout the City as well as those managed by the Information and Technology Division. In addition, the recommendations may also have relevance to systems at the City's Agencies, Boards and Commissions. As the Auditor General's Office does not have the resources to perform reviews of all systems in the City and its Agencies, Boards and Commissions, it is suggested that this report be forwarded to each one of these entities for their review, analysis and consideration.

Recommendation:

1. City Council direct that this report be forwarded to all City Departments, Agencies, Boards and Commissions. These entities be required to review the recommendations in this report to determine whether or not they have relevance to their operations and take appropriate action where necessary.

Effectiveness

Effectiveness is defined as the degree to which the Toronto Maintenance Management System contains reliable information, is available to the user, and its features and capabilities meet the users' needs.

Reliability of Information

Management relies on reports from the system for analysis, action and future planning. Effective, value added and useful information from the Toronto Maintenance Management System is based on the premise that data entered into the system is complete and accurate. Business processes that require staff in all districts to enter the same level of data into the system are necessary to ensure the reliability of the information in the system.

Information Technology staff in the Transportation Services Division and the Works and Emergency Services Department recognized the need for harmonized business processes early in the systems development. The Information Technology Strategic Plan authored for the Works and Emergency Services Department in 1999 states, "the effective use of the Toronto Maintenance Management System requires the harmonization of business processes across the former municipalities". The 1999/2000 "Unified Business Case Cost Avoidance Assumptions" paper, also prepared by staff in Works and Emergency Services indicated that "the efficiency will come from more readily accessible information on activity based financial reporting, performance measurement, standards, and resources utilization".

Currently, the level of detail entered into the system for labour, material, equipment usage and accomplishments varies between the four districts. There are no common data entry rules outlining the data that must be entered or the level of detail to be entered. The absence of a standardized approach makes it difficult to implement data verification and validation routines, which could be built into the system. Such routines help improve the accuracy of data input, thereby increasing the level of confidence with respect to the integrity of information contained in reports generated by the system. Reports generated by the system are a key tool used by management to monitor operations. The lack of a common set of data entry rules reduces the level of confidence in the information provided through management reports, and increases the risk that management may make decisions based on reports created from incomplete data.

Recommendation:

2. The Commissioner, Works and Emergency Services, review the current practice for entering data in the Toronto Maintenance Management System. Such a review ensure that:

   a. the exercise to harmonize business practices is completed;

   b. the rules and requirements for entering data into the Toronto Maintenance Management System are developed and are appropriately and consistently followed in the Districts; and

   c. the data requirements are sufficient to create meaningful reports that will allow management to monitor activity and effectively carry out its responsibility.

Features and Capabilities

Generally, systems are designed to meet the needs of the various users. These needs represent a clear articulation of users' goals, how they currently work, what they expect to be able to do and how they wish to do it. The purpose of defining these needs is to provide systems development staff with a comprehensive understanding of the users' expectations of how the new system will function and the features it must include to support operational needs.

In the early stages of amalgamation, there were several maintenance management systems in use at the City. After some consideration, the system operated in the former Municipality of Metropolitan Toronto was chosen as the base system. Enhancements to this system were recommended to meet the requirements of the newly formed City. Documentation made available to the Auditor General suggests that these enhancements were, and continue to be, based on annual work plans, developed from a set of high level user requirements which were stated in broad terms. A comprehensive "user requirements" document, which sets out what the enhanced Toronto Maintenance Management System must provide, was not prepared at the beginning of the project.

Staff of the Transportation Services Division has identified numerous enhancements that would expand the usefulness of the system. There is a need to place some parameters around future development and the resources required to deliver user requirements in a timely and cost effective manner and to prioritize user requests for changes to the system.

Recommendation:

3. The Commissioner, Works and Emergency Services:

   a. identify all outstanding requests for enhancements or modifications to the Toronto Maintenance Management System;

   b. analyze the costs and benefits of each potential change;

c. prioritize the enhancements based on the cost benefit analysis; and

d. ensure that the above steps are documented and approved by appropriate supervisory staff.

Integration with Other Business Systems

Implementation of the Toronto Maintenance Management System has brought with it certain efficiencies in the management of road operations. This is particularly true for the Districts that did not previously have automated work management software. However, the planned integration of the Toronto Maintenance Management System with other systems such as the City's SAP HR/Payroll and Financial systems has not yet been completed. The lack of these electronic interfaces means that information must be separately input into both systems, an obvious duplication of effort. In addition to the duplicate effort required, manual data entry creates an opportunity for human error. These data entry errors could be avoided if the information was electronically transferred from one system to the other.

Although requests to implement an interface were submitted to the Financial Information System's User Group, there has not been any significant progress in implementing such an interface. In April 2003, the Auditor General's Office issued a report recommending the Commissioner of Corporate Services and the Chief Financial Officer and Treasurer be required to develop a long-term City-wide strategic plan relating to the future direction of the SAP information system. This plan is to include the appropriate staffing and processes to work with departments to coordinate the implementation and integration of major information systems within the City. It is in this context that the following recommendation is made.

Recommendation:

4. The Commissioner, Works and Emergency Services, submit to the SAP Competency Centre a current updated version of its business case for implementing an electronic interface between SAP and the Toronto Maintenance Management System.

Security

The protection of data processed by the Toronto Maintenance Management System is critical in ensuring the integrity of the data is maintained and that it is protected from unauthorized changes or access. Although there are various layers of security in place to protect the City's data, this report focuses on security practices that are associated with the system itself.

Security Requirements

In any system development, it is most efficient to document the security standards, or the desired level of protection for the data, before actual development begins. This provides the development team with direction, and forms the basis for ensuring that the appropriate security features are built into the system. At various points during the development of the system, these requirements are reviewed and tested to validate that the standards identified at the outset have

been adequately addressed. Since the security model is built at the very first step, one is assured that the security constraints will be appropriately considered throughout the implementation process.

When the development of the Toronto Maintenance Management System began, comprehensive security requirements were not established. While security features were designed into the system, they were limited in scope and functionality. As the system began to be used, additional security needs were identified. For example, users discovered that unauthorized changes were being made to Service Requests and Work Orders. As a result, a security procedure was put in place to track these changes (e.g., who, when and what). Security requirements and management trails continue to be added when the business user voices valid security concerns.

The lack of clearly thought out and implemented security procedures increases the risk that data may be compromised, and unauthorized access to critical data and resources may go unnoticed. When security is inadequate, it puts at risk the integrity, and reliability of the data on which the business user depends, invariably affecting the effectiveness and efficiency of the application. It is also fairly well known in the systems development field that retrofitting security after a system has been deployed is more costly than designing the necessary controls into the system as it is being initially developed. While it is too late to apply this approach to the Toronto Maintenance Management System, the current process of improving security as weaknesses are identified by users should be replaced by a thorough review of security needs followed by a planned implementation of the necessary security procedures.

Recommendation:

5. The Commissioner, Works and Emergency Services, complete the necessary steps to mitigate security weaknesses within the Toronto Maintenance Management System. These steps to include; identifying threats to the data and resources, performing an analysis to determine how the existing security measures protect against these threats and, implementing additional processes and controls identified as a result of this analysis.

Security Responsibilities

Systems security is comprised of many different activities. For example, there is a security component to activities such as approving a new user, adding or deleting a user from the system, changing the privileges, (what a person can actually do on the system) assigned to a particular user, etc. The preferred practice and trend is to divide or segregate these duties between at least two individuals. Generally, this is accomplished by having one person or group authorize changes, and a different person or group actually makes the change on the system. Segregating these functions prevents the concentration of duties in one person. Defining these kinds of security practices should be the responsibility of one person, often referred to as the security manager. While these responsibilities are not necessarily a full-time endeavour, they should be assigned to one individual.

Responsibility for administering overall security of the Toronto Maintenance Management System has not been formally assigned. There is no one employee with the responsibility to ensure effective security policies are developed, circulated, promoted, and monitored. Security concerns are currently the responsibility of the Lead Developer and the Quality Assurance Lead. These individuals assumed the task of looking after the security of the system during the system development phase. By default, they have continued to perform this role. The absence of a formally appointed security manager increases the risk that certain security activities such as monitoring user activity, documenting security rules, monitoring for compliance with good security practices, naming conventions, etc. may not be performed.

Recommendation:

6. The Commissioner, Works and Emergency Services, implement a security governance framework for the Toronto Maintenance Management System. The framework should outline the standards to be followed, the duties to be performed and the staff position responsible for overseeing the security for the system.

User Permissions and Privileges

Giving a user the ability to view, add, change, or delete data on the Toronto Maintenance Management System is a two step process. The first step is to grant the individual access to the system and the second is to provide the ability to perform various tasks such as input data, edit data, produce reports as required by the individual's work related responsibilities.

The Toronto Maintenance Management System does this through the use of a number of defined "user groups", designed to allow an employee to complete his or her assigned tasks. Each user group has a predefined set of authorities on the system which dictate which menus, data, functions, and reports all members of that group can access. For example, an employee required to administer contracts would be assigned to a user group that is designed to provide the ability to add, change, delete or view data necessary to carry out that particular function.

There are no procedures or standard forms used in adding, changing, or deleting a user from the Toronto Maintenance Management System. Users are granted access to the system based on their verbal request to their local administrator. The local administrator may follow-up on the verbal request with an e-mail to the applicable senior management for approval, but this is at the discretion of the local administrator. This situation increases the risk that accountability for use of the system will weaken and that inappropriate access to the Toronto Maintenance Management System may be granted. This is an example of the need to segregate security duties described above. The system administrator may grant access but only after having been advised, preferably in writing, by specific and identified user staff that such access is required.

Given the weakness in controls in granting users access to the system as noted above, managers are unlikely to know which staff has access to the system and what functions they can perform on the system. As such, it would be prudent to conduct a review of user access rights to ensure appropriate management staff is aware of all system users and their rights on the system.

Recommendations:

7. The Commissioner, Works and Emergency Services, implement formal procedures, for granting or removing a user's access to the Toronto Maintenance Management System. These procedures to include, but not be limited to; approval requirements, assigning user group(s), procedures to deal with contractors, temporary workers, as well as transferred and terminated employees, and the maintenance of appropriate documentation in support of the access privileges granted.

8. The Commissioner, Works and Emergency Services, direct that a review of current user access rights be performed and that such a review be conducted on a regular basis to confirm that user access rights are compatible with job functions and responsibilities.

Administrator User Group

One of the user groups in the Toronto Maintenance Management System supports the tasks associated with overall administration of the system. This user group named "Administrator" is a group designed to give individuals the ability to view, modify or delete any data on the system. Approximately 20 individuals are assigned to the "Administrator" user group. Given the privileges associated with this group, the higher the number of individuals assigned to this group the higher the risk of unauthorized access and changes to the application.

A second concern with respect to Administrators arises where these individuals are also required to perform the functions of a regular user of the system. In such cases, a separate user account should be assigned to these individuals. This will avoid accidental misuse of administrative privileges while performing regular operational activities. The separation of these user accounts will also provide management with an audit trail based on the appropriate user group assigned for the activity performed. Our review of the list of users assigned to the Administrator user group revealed six users who are using their administrative privileges to complete activities that should be conducted using an operational user account.

Recommendation:

9. The Commissioner, Works and Emergency Services, ensure that:

   a. the assignment of individuals to the "Administrator" user group is commensurate with operational requirements; and

   b. individuals, who are required to perform administrative duties in addition to daily operational duties, be given a second user account for their operational function.

Monitoring System Activity

Sophisticated software systems are generally designed to include logs to record key activities carried out by users. These logs contain a significant amount of data including information as to who accesses the system, when and from where. To ease the burden of reviewing this data,

reports, called exception reports, are usually designed to highlight events or activities that may warrant closer scrutiny by staff. Although such exception reports are produced by the system, they are not currently being used. There is no plan or procedure to ensure that exception reports are reviewed and acted upon accordingly. In addition, there are no escalation procedures outlining how to deal with situations where the review of exception reports indicate follow-up action is required. Failure to review the audit logs on a regular basis increases the risk that unauthorized access to the data may not be detected on a timely basis. Follow-up action may not be timely, efficient or effective without documented escalation procedures.

Although the system has been set up to audit and log changes to certain forms such as service requests and work orders, expiry dates for these audit records have not been defined. Consequently, as of March 30, 2004, there were 3.4 million audit records on the system and this will continue to increase. The absence of a defined life cycle for the audit records increases the storage space required and will eventually impact overall system performance.

Recommendation:

10. The Commissioner, Works and Emergency Services, implement a process for tracking activity on the Toronto Maintenance Management System. The tracking strategy consider; the activities or actions to track, the generation of exception reports for review on a regular basis, and follow-up steps for exceptions noted. Further, the Division consult with Records & Archives Division of the Clerks Office, to determine the appropriate retention period for audit records maintained within the system.

Management of User-IDs and Passwords

Access to a system is normally granted after a user enters both a valid user identification combined with a password. Once the correct combination of these two items is entered, the user is granted access to the system.

Compromised passwords are among the most common vulnerabilities of any secured system. Generally, users are not always careful with their passwords, policies are difficult to enforce and there are many tools available for use by individuals who are intent on obtaining someone’s password. Once an individual has a User-ID and a password, they have all of the rightful user's privileges. While training users will help minimize policy violations, additional processes, which can be built into the system, must be put in place to mitigate attempts to compromise passwords.

The common practice is to store passwords on the system in a format where an algorithm has been used to scramble the data to make it unreadable to everyone except the recipient. This is known as encryption. Storing the passwords in an encrypted format provides an additional level of security in the event that someone might gain access to the file that contains all the passwords. We found that, for the Toronto Maintenance Management System, passwords are not encrypted but stored in clear-text, a form that is easily read and copied.

We also observed that many of the standard practices associated with passwords are not in effect for the system. For example, we found that:

- the user is not required to change the password at the time of initial logon;

- there is no minimum password length;

- the user is not forced to periodically change the password;

- there is no expiry date for passwords; and

- the Toronto Maintenance Management System is programmed such that after three unsuccessful logon attempts the individual is forced to exit the system. However, the user is not locked out and simply exits the system and can then re-enter getting three more attempts at the password.

Recommendation:

11. The Commissioner, Works and Emergency Services, ensure that passwords associated with the Toronto Maintenance Management System are encrypted and password management practices, such as setting a standard minimum length for the password forcing regular password changes, etc., are implemented.

Like most systems, access to the Toronto Maintenance Management System is gained by entering a User-ID in combination with a password. User-IDs are also often used for linking activity to a particular individual. Best practices recommends each individual granted access to the system has a unique User-ID.

We reviewed all the User-IDs in effect for the system and found over 50 generic/shared User-IDs. As well, the practice of following a naming convention, (such as first initial and last name), when setting up User-IDs is not used. This leads to situations, as is the case for a number of User-IDs for the Toronto Maintenance Management System, where the assigned User-ID gives no indication of who the owner of the User-ID might be. For example, we found User-IDs such as “1954”, 12345”, “66666”, and “WEST”. This makes it more difficult to identify situations where users may have been inappropriately granted access.

Recommendation:

12. The Commissioner, Works and Emergency Services, ensure that each user is provided with a unique User-ID and that the naming convention used be designed to give indication as to the owner of the User-ID.

<u>Business Continuity Plan</u>

A Business Continuity Plan provides the framework for a controlled response to emergency situations and how to recover from such events regardless of how unlikely they may seem. In

any business environment, whether it is the public sector or private industry, there needs to be a commitment by the stakeholders that a critical system and the associated business functions are maintained and working in the event of business disruptions. The loss of critical data or computing facilities could have significant impact on the City's residents and also result in financial losses to the City.

A comprehensive business continuity plan normally involves various levels of management, crosses many organization units, and ranges from global statements down to describing the policies and procedures to be followed in the event of a business disruption. In this report, our comments are limited to the ability of Transportation Services Division to continue the business processes, which complement and support transactions processed by the Toronto Maintenance Management System or to restore the system itself.

The Transportation Services Division does not have a comprehensive business continuity plan. In the event of a business disruption, the Division will likely experience an uncoordinated recovery effort, resulting in inefficiencies, and an extended period of time to become operational or offer services to the public. Although the Information and Technology Support Group has developed procedures and processes to deal with the technology aspects such as making sure appropriate computers are available, there is no plan outlining what is required from the business user both while the computers are out of service and again once they are back on line.

Recommendation:

13. The Commissioner, Works and Emergency Services, ensure that:

    a. a business continuity plan that integrates operational needs with the technology component of the Toronto Maintenance Management System is prepared, and that such a plan is documented and tested on a regular basis; and

    b. this plan be incorporated into the departments overall disaster recovery plan.

Change Management Strategy

An effective change management strategy provides a systematic approach to implementing planned changes, emergency changes, and major enhancements to the Toronto Maintenance Management System. Such a strategy should support a cost-effective approach to changes by ensuring that user requirements are cost justified, prioritized, and approved, and that system integrity is maintained through user acceptance testing and the requirement for authorization prior to the changes being moved from testing to the actual application.

In January 2003, formal policies and procedures governing changes to the Toronto Maintenance Management System were introduced. These procedures address such areas as:

- the review and prioritization of change requests received;

- the documentation requirements from point of request through to the implementation of the change to the Toronto Maintenance Management System;

- the testing strategy, training and communication requirements; and

- the approval required prior to implementing a change and the management trail over such changes.

Overall, these procedures are reasonable and consistent with good practice although improvements could be made to how change requests are reviewed, prioritized, and approved for further development, and secondly, with respect to user sign-off of the test results.

Prioritization of Change Requests

Requests for changes are received from various sources and are logged in a master control list. Each request is assigned a priority by a group of individuals consisting of the Toronto Maintenance Management System Project Manager and a representative from each of the four business areas. At the time of our review, the master control list contained 36 issues raised in 2000, 22 issues presented in 2001, and 7 issues created in 2002 that had not been acted upon.

The group responsible for prioritizing change requests does not have any defined criteria for making their decisions. The absence of a formal process to prioritize requests may lead to situations where non-critical requests are addressed first or changes, which could provide a greater benefit to the division, are inappropriately deferred.

Recommendation:

14. The Commissioner, Works and Emergency Services, implement a process to prioritize, justify and approve the implementation of all changes to the Toronto Maintenance Management System.

Authorization of Changes

The term “sign-off” used in the context of developing or implementing systems means an agreement, as evidenced by a customer’s signature. These are usually required to initiate a change and signify that the changes made to the system meets the specified requirements and that the system continues to operate as expected. It is the user’s responsibility to ensure the system is meeting the specifications originally established before they accept the system as complete.

According to the procedures outlined in the “Toronto Maintenance Management System Project Control and Structure” document, the business user is required to authorize (sign-off) any request for a change to the system. This sign-off is only provided after there is a clear understanding of the request between the business user and the information technology group and feedback has been received as to the effort required to complete the task. A Task Control Sheet has been

developed to spell out the user's request and summarize the information technology resources required to satisfy the request.

This approach is consistent with the steps and processes normally followed in developing a new system or implementing changes to an existing system. However, we found no evidence that management is actually approving the change requested before the information technology group proceeds with the change. The Task Control Sheets designed for this purpose did not have any approval signatures on them. We were informed that verbal agreement is obtained from the users prior to making changes to the system.

Lack of documentary evidence to indicate that approval is obtained increases the risk that unauthorized changes may be implemented or that changes are implemented without adequate testing being done by the user. The accuracy and functionality of the Toronto Maintenance Management System is at greater risk under this situation. Finally, this scenario weakens accountability for the implementation of changes, which may lead to potential disputes as to whether or not the user actually accepted the change.

Recommendation:

15. The Commissioner, Works and Emergency Services, ensure that staff sign the Task Control Sheet to signify the approval to proceed with the changes to the system and sign again to acknowledge acceptance of the completed change.

Emergency Changes

Emergency changes are unplanned changes that require immediate resolution and often, by necessity, bypass the normal process of technical, operational and management assessment prior to implementation. The nature of an emergency change is such that the window for implementation is often very narrow.

Currently, there is no definition of what constitutes an emergency change, and the procedures to be followed to make these changes are not documented. Under these circumstances, there is increased risk that unauthorized changes may be made or alternatively, due to the rushed nature of the change, there may be unintended consequences.

Recommendation:

16. The Commissioner, Works and Emergency Services, document procedures for emergency changes and that these procedures be complied with and include the necessary user validation and authorization after the change has been made.

Testing Methodology

Testing the system is a critical component of developing, enhancing or implementing changes to a system such as the Toronto Maintenance Management System. Although different stakeholders, at different times participated in the testing of the system, the documentation

supporting the various testing and the extent of testing are not always retained. Retention of test results and related documents allow for an independent assessment of the adequacy and completeness of the testing.

Although business users from all the districts participated in the testing of the Toronto Maintenance Management System, the documentation supporting the various testing and the extent of testing were not always retained. Beginning in July 2003, appropriate documentation is being maintained.

Use of Automated Testing Tools

Today there are automated tools available which are designed with the purpose of allowing organizations to be more effective in conducting tests by increasing the amount of testing that can be done. These tools can also improve efficiency by shortening the overall time that is required to complete the various types of tests that are normally conducted when making changes to systems.

Changes made to the Toronto Maintenance Management System are tested without the aid of automated tools. This can be a time consuming exercise and often requires the rekeying or re-entering of routines previously designed to test specific transactions and certain functions of the system. As the system expands and continues to grow in complexity there is a greater risk that all areas will not be adequately tested and that deficiencies will not be detected on a timely basis.

Recommendation:

17. The Commissioner, Works and Emergency Services, investigate the opportunity for using the automated test tool available from the Corporate Information and Technology Division in future system changes or system development projects.

Customized Reports

Although many customized reports have been developed for the Toronto Maintenance Management System, we observed that a limited number of reports are actually being used by the division to manage the effective and efficient delivery of the services it provides.

In many cases, there is little or no documentation supporting the development of customized reports. There are no user requirements supporting the development of these reports, test documentation outlining the extent of testing performed prior to implementation and evidence of user sign-off prior to putting the reports into use. To ensure that information technology resources are used effectively, users' needs for reports should be fully documented and appropriate reports developed. Where subsequent customized reports are deemed necessary, these should only be developed as a result of user requests, or alternatively, after confirmation that the users see a need for reports suggested by systems development staff.

Recommendations:

18. The Commissioner, Works and Emergency Services, conduct a thorough analysis of the reporting requirements of the users of the Toronto Maintenance Management System and consider these needs in further developing the system.

19. The Commissioner, Works and Emergency Services, ensure that the development of reports follow a consistent process. That process to include defining the user's requirements, obtaining the necessary approval, testing for accuracy and receiving final user acceptance before adding a customized report to the Toronto Maintenance Management System.

Third Party Access to the System

The Toronto Maintenance Management System presents the City with the opportunity to allow limited access by contractors, thereby improving both the service level to the contractor, and the overall efficiency and cost effectiveness of performing administrative tasks. Although this approach has benefits, it means providing someone, who is outside of the City, with direct access to the system. This requires the City to carefully consider what additional risk this brings and take appropriate action to limit the City's exposure.

At the time of our review, only one outside company contracted to install and maintain traffic signs on City streets has access to the system. The contractor uses this access privilege to input the resources expended for the work completed and to invoice the City. Plans are in place to allow for more contractors to directly access the Toronto Maintenance Management System.

The City has a proposed standard that requires all individuals not employed by the City to sign an Acceptable Use Policy prior to being given access to the City's network. This standard was not followed. We also observed that the contract with the Contractor does not identify any accountability and responsibility on the part of the Contractor for the use of the City's information technology infrastructure.

A standard such as the "Acceptable Use Policy" document is designed to protect the City's information assets. Failure to comply with such a standard increases the City's exposure to an undesirable event (such as infection by a computer virus) and not having it signed could allow the third party to claim they were not aware of the City's requirements, thus potentially avoiding any liability for inappropriate actions.

Recommendation:

20. The Commissioner, Works and Emergency Services, ensure that third parties granted access to the Toronto Maintenance Management System be contractually required to adhere to acceptable use policies similar to those in place for City employees.

Project Management Practices

Tracking actual costs against budgeted costs, and reporting on project milestones and deliverables are standard project management practices. Steering Committee minutes for the Toronto Maintenance Management System make no reference to costs and it appears that the cost of the system was not reported to the committee overseeing the project. These minutes also indicate that key deliverables or milestones to be achieved by the project team were not reported.

In July 2000, City Council approved $11.3 million for the preparation of the Strategic Information Technology Plan for the Works and Emergency Services Department and transition funding for a Unified Business Application System, which consisted of 15 individual projects. The Toronto Maintenance Management System was one of the 15 projects and had an estimated cost of $3.5 million for external consultants to work on the system in the years 2000, 2001 and 2002. Another project in the list of 15 projects is the Work Order Tracking System with an estimated cost of $1 million. The Information Technology Group within Works and Emergency Services indicated that the Work Order System Tracking System was part of the Toronto Maintenance Management System project, which brought the approving funding for developing the system to $4.5 million.

Works and Emergency Services does not have a reliable system in place to capture, track and report on the costs of the 15 individual projects. Based on analysis from available records, as of December 31, 2003, the total development cost for the Toronto Maintenance Management System was $4,457,041. We were unable to definitively confirm that planned functionality was completed within the original budget for the system. As the system continues to be enhanced, it is important to ensure appropriate project management practices are in place to ensure actual costs do not exceed approved amounts, milestones are achieved on time, and that any necessary corrective action is taken in a timely manner.

Recommendation:

21. The Commissioner, Works and Emergency Services, ensure that all future development and enhancements to the Toronto Maintenance Management System adhere to project management practices and standards, including a system to capture and report on the costs of projects.

Project Scope

A project plan, which identifies the scope of the project, is a necessary tool to map out activity and keep a project on track.

Enhancements to the Toronto Maintenance Management System began in 1999 with a considerable investment of resources applied from 2000 to 2003. However, there are numerous outstanding tasks and features which need to be addressed and developed. There is no evidence of a formal project plan, which outlines the scope of these outstanding tasks.

Unless there is a final document, which states the requirements for the application, and remaining work to be done, there will be continual pressures to change the scope of the project which will likely lead to increased costs in enhancing the application.

Recommendation:

22. The Commissioner, Works and Emergency Services, develop a project plan outlining all outstanding tasks appropriately prioritized, scoped, and approved and the estimated costs (including staff time) to complete the plan be reported to the Works Committee. The plan should be adhered to and any subsequent requests, unless deemed emergency or essential, be deferred.

System Acceptance

Having a system that meets performance expectations, which is easy to use and that is friendly to all users, is extremely important in gaining the acceptance of the business user. User acceptance, in turn, is critical to the success and effectiveness of any system.

In the course of our review, we were told on several occasions by the business users that the system is too slow, and the "window" for entering or viewing data is too small for most users. These problems detract from the many good features of the system and can cause users to resent having to use what they often see as a slow and unfriendly piece of software.

Recommendations:

23. The Commissioner, Works and Emergency Services, ensure that Toronto Maintenance Management System response times (i.e., making the system faster for the user) are included as one of the outstanding enhancement projects to be analyzed and prioritized.

24. The Commissioner, Works and Emergency Services, report back to the Audit Committee scheduled for July 13, 2004, on a work plan in regard to the implementation of the recommendations contained in this report. Such report to include specific timelines for implementation.

Conclusions:

The base functionality of the Toronto Maintenance Management System has been implemented, is being used widely in the Transportation Division and, has automated many processes previously done manually. The System has the potential to further improve the management and control of the development, repairs and maintenance of the City's vast infrastructure of roads. The system was carried forward from a former municipality and continues to be upgraded to meet the needs of the amalgamated City. As of the date of this report, management staff has identified a number of changes that will provide managers the information they need to more effectively carry out their day-to-day duties. In addition, there is a need to harmonize business practices to ensure the data in the system is complete and consistent across the City. Another

major improvement would be the integration with other systems in the City, most notably SAP, the City's financial information system.

In addition to the developmental issues, several security-related practices must be put in place to protect data from unauthorized changes, access or disclosure. Good security is critical to the successful use of the system. If security is poor, the Transportation Services Division risks not having accurate and reliable information to achieve its goals.

In order to achieve maximum efficiencies, the Toronto Maintenance Management System allows outside contractors to access the system for purposes of entering certain data. There is no agreement between the City and the contractors covering their usage of the system. Third party users of City systems should be contractually required to adhere to acceptable use policies similar to those in place for City employees.

Transportation Services Division needs to implement a business continuity plan that includes the processes to be followed by the business user, as well as the steps to be followed to recover the required information technology resources lost in a potential disaster situation.

This report contains recommendations, several of which deal with establishing a more formal framework and process to ensure future enhancements to the Toronto Maintenance Management System are effectively managed. The report also makes recommendations to ensure that security practices receive the necessary attention and are applied consistently across all four districts. The implementation of the recommendations contained in this report will enhance the effectiveness of the Toronto Transportation Management System and provide additional assurances as to system security and the ability of the City to restore the system in the event of a disaster.

Contact:

Jerry Shaubel
Director, Auditor General's Office
Tel: (416) 392-8462, Fax: (416) 392-3754
E-mail: JShaubel@toronto.ca

Ben Smid
Senior Audit Manager, Auditor General's Office
Tel: (416) 392-8478, Fax: (416) 392-3754
E-mail: BSmid@toronto.ca

Jeffrey Griffiths
Auditor General

List of Attachments:

Appendix I: Toronto Maintenance Management System Application Review – Management Response

APPENDIX I

Toronto Maintenance Management System Application Review
Management Response

No.	Recommendation	Management Response
1.	City Council direct that this report be forwarded to all City Departments, Agencies, Boards and Commissions. These entities be required to review the recommendations in this report to determine whether or not they have relevance to their operations and take appropriate action where necessary;	No Comment

No.	Recommendation	Management Response
2.	The Commissioner, Works and Emergency Services, review the current practice for entering data in the Toronto Maintenance Management System. Such a review ensure that: (a) the exercise to harmonize business practices is completed; (b) the rules and requirements for entering data into the Toronto Maintenance Management System are developed and are appropriately and consistently followed in the Districts; and (c) the data requirements are sufficient to create meaningful reports that will allow management to monitor activity and effectively carry out its responsibility;	The exercise to harmonize business practices has been completed and the implementation process started earlier this year is scheduled to be completed this summer. New rules and requirements for data entering are part of the harmonization process.

No.	Recommendation	Management Response
3.	the Commissioner, Works and Emergency Services: (a) identify all outstanding requests for enhancements or modifications to the Toronto Maintenance Management System; (b) analyze the costs and benefits of each potential change; (c) prioritize the enhancements based on the cost benefit analysis; and (d) ensure that the above steps are documented and approved by appropriate supervisory staff;	All the enhancements have been identified with their costs and prioritized. A Steering Committee within WES now reviews the enhancements and recommends a priority ranking. Additional work should be done on the benefits of each enhancement and improved documentation will be made to address the audit concerns.

No.	Recommendation	Management Response
4.	the Commissioner, Works and Emergency Services, submit to the SAP Competency Centre a current updated version of its business case for implementing an electronic interface between SAP and the Toronto Maintenance Management System;	WES is currently working with Corporate I.T. on the issue of the interface. An updated business case will be developed for the implementation of an electronic interface between SAP and TMMS.

No.	Recommendation	Management Response
5.	the Commissioner, Works and Emergency Services, complete the necessary steps to mitigate security weaknesses within the Toronto Maintenance Management System. These steps to include; identifying threats to the data and resources, performing an analysis to determine how the existing security measures protect against these threats and, implementing additional processes and controls identified as a result of this analysis;	We are in agreement that the security system within TMMS should be enhanced. It is understood Corporate I.T. is developing new security guidelines for computer systems such as TMMS. Security enhancements for TMMS will be addressed in connection with the Corporate I.T. initiative.

No.	Recommendation	Management Response
6.	the Commissioner, Works and Emergency Services, implement a security governance framework for the Toronto Maintenance Management System. The framework should outline the standards to be followed, the duties to be performed and the staff position responsible for overseeing the security for the system;	See # 5 response.

No.	Recommendation	Management Response
7.	the Commissioner, Works and Emergency Services, implement formal procedures, for granting or removing a user's access to the Toronto Maintenance Management System. These procedures to include, but not be limited to; approval requirements, assigning user group(s), procedures to deal with contractors, temporary workers, as well as transferred and terminated employees, and the maintenance of appropriate documentation in support of the access privileges granted;	See # 5 response.

No.	Recommendation	Management Response
8.	the Commissioner, Works and Emergency Services, direct that a review of current user access rights be performed and that such a review be conducted on a regular basis to confirm that user access rights are compatible with job functions and responsibilities;	See # 5 response

No.	Recommendation	Management Response
9.	the Commissioner, Works and Emergency Services, ensure that: (a) the assignment of individuals to the "Administrator" user group is commensurate with operational requirements; and (b) individuals, who are required to perform administrative duties in addition to daily operational duties, be given a second user account for their operational function;	See # 5 response

No.	Recommendation	Management Response
10.	the Commissioner, Works and Emergency Services, implement a process for tracking activity on the Toronto Maintenance Management System. The tracking strategy consider; the activities or actions to track, the generation of exception reports for review on a regular basis, follow-up steps for exceptions noted, and the retention period for audit records maintained within the system;	We are in agreement.

No.	Recommendation	Management Response
11.	the Commissioner, Works and Emergency Services, ensure that passwords associated with the Toronto Maintenance Management System are encrypted and password management practices such as setting a standard minimum length for the password, forcing regular password changes, etc. are implemented;	See # 5 response

No.	Recommendation	Management Response
12.	the Commissioner, Works and Emergency Services, ensure that each user is provided with a unique User-ID and that the naming convention used be designed to give indication as to the owner of the User-ID;	See # 5 response

No.	Recommendation	Management Response
13.	the Commissioner, Works and Emergency Services, ensure that: (a) a business continuity plan that integrates operational needs with the technology component of the Toronto Maintenance Management System is prepared, and that such a plan is documented and tested on a regular basis; and (b) this plan be incorporated into the departments overall disaster recovery plan;	As part of the WES 2004 budget, funds have been allocated to develop a disaster recovery plan for all WES I.T. systems including TMMS.

No.	Recommendation	Management Response
14.	the Commissioner, Works and Emergency Services, implement a process to prioritize, justify and approve the implementation of all changes to the Toronto Maintenance Management System;	This recommendation is now being implemented for TMMS. The process will be completed by September 2004.

No.	Recommendation	Management Response
15.	the Commissioner, Works and Emergency Services, ensure that staff sign the Task Control Sheet to signify the approval to proceed with the changes to the system and sign again to acknowledge acceptance of the completed change;	This recommendation is now being implemented for TMMS.

No.	Recommendation	Management Response
16.	the Commissioner, Works and Emergency Services, document procedures for emergency changes and that these procedures be complied with and include the necessary user validation and authorization after the change has been made;	This recommendation is now being implemented for TMMS.

No.	Recommendation	Management Response
17.	the Commissioner, Works and Emergency Services, investigate the opportunity for using the automated test tool available from the Corporate Information and Technology Division in future system changes or system development projects;	The automated test tool is now being used for TMMS.

No.	Recommendation	Management Response
18.	the Commissioner, Works and Emergency Services, conduct a thorough analysis of the reporting requirements of the users of the Toronto Maintenance Management System and consider these needs in further developing of the system;	The analysis is part of the 2004 work plan for TMMS.

No.	Recommendation	Management Response
19.	the Commissioner, Works and Emergency Services, ensure that the development of reports follow a consistent process. That process to include defining the user's requirements, obtaining the necessary approval, testing for accuracy and receiving final user acceptance before adding a customized report to the Toronto Maintenance Management System;	The analysis is part of the 2004 work plan for TMMS.

No.	Recommendation	Management Response
20.	the Commissioner, Works and Emergency Services, ensure that third parties granted access to the Toronto Maintenance Management System be contractually required to adhere to acceptable use policies similar to those in place for City employees;	The contracts to third parties already include clauses to state they are required to adhere to City policies. However, WES contract administration procedures will be reviewed to ensure contractors are made aware and adhere to the policies.

No.	Recommendation	Management Response
21.	the Commissioner, Works and Emergency Services, ensure that all future development and enhancements to the Toronto Maintenance Management System adhere to project management practices and standards, including a system to capture and report on the costs of projects;	WES staff are now using project management and standards from the Project Management Institute to manage enhancements.

No.	Recommendation	Management Response
22.	the Commissioner, Works and Emergency Services, develop a project plan outlining all outstanding tasks appropriately prioritized, scoped, and approved and the estimated costs (including staff time) to complete the plan be reported to the Works Committee. The plan should be adhered to and any subsequent requests, unless deemed essential, be deferred;	The yearly project plan will be part of annual budget submissions to Works Committee.

No.	Recommendation	Management Response
23.	the Commissioner, Works and Emergency Services, ensure that Toronto Maintenance Management System response times (i.e., making the system faster for the user) are included as one of the outstanding enhancement projects to be analyzed and prioritized; and	Recently, the response times have improved due to changes in TMMS to optimize codes to allow the system to run faster. The corporate initiative to refresh desk top and lap top computers will also result in improvement in response times.

No.	Recommendation	Management Response
24.	the Commissioner, Works and Emergency Services, report back to the Audit Committee scheduled for July 13, 2004, on a work plan in regard to the implementation of the recommendations contained in this report. Such report to include specific timelines for implementation.	A work plan report will be submitted to the Audit Committee meeting scheduled for July 13, 2004.