

# Deloitte

Deloitte & Touche LLP  
Two World Financial Center  
New York, NY 10281-1414  
USA

Tel: +1 212 436 2000  
Fax: +1 212 436 5000  
www.deloitte.com

April 16, 2008

The Audit Committee  
Metropolitan Transportation Authority  
New York, New York

And

The Management of MTA Long Island Rail Road  
New York, New York

Dear Members of the Audit Committee and Management:

In planning and performing our audit of the financial statements of MTA Long Island Rail Road (the "MTA LIRR"), a wholly owned public benefit corporation subsidiary of Metropolitan Transportation Authority ("MTA"), as of and for the year ended December 31, 2007 (on which we have issued our report dated April 16, 2008), which contains an explanatory paragraph regarding the adoption of Governmental Accounting Standards Board Statement (GASB) No. 45, *Accounting and Financial Reporting by Employers for Post Employment benefits Other Than Pensions*, in accordance with auditing standards generally accepted in the United States of America, we considered the MTA LIRR's internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the MTA LIRR's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the MTA LIRR's internal control over financial reporting.

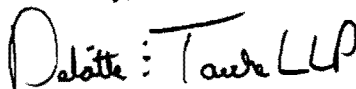
Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting. However, in connection with our audit, we identified, and included in the attached Appendix, control deficiencies related to the MTA LIRR's internal control over financial reporting and other matters as of December 31, 2007, that we wish to bring to your attention.

The definition of a control deficiency is also set forth in the attached Appendix.

Although we have included management's written response to our comments in the attached Appendix, such responses have not been subjected to the auditing procedures applied in our audit and, accordingly, we do not express an opinion or provide any form of assurance on the appropriateness of the responses or the effectiveness of any corrective actions described therein.

This report is intended solely for the information and use of management, the Audit Committee, and others within the organization and is not intended to be, and should not be, used by anyone other than these specified parties.

Yours truly,



## SECTION I – OTHER CONTROL DEFICIENCIES

We identified the following other control deficiencies involving the MTA LIRR's internal control over financial reporting as of December 31, 2007 that we wish to bring to your attention:

### 1. UNIX Security- Procurement Logistics System (PLS) and Maximo

**Observation:**

Security can be further strengthened on the UNIX (PLSjam) and UNIX (maximoprod) environments.

**Background:**

During our assessment of the UNIX (PLSjam) environment and UNIX (maximoprod) environment, we identified the following areas for improvement:

*UNIX Security:*

**Password Controls:** Currently the following password controls are in place for PLSjam:

- Minimum password change interval – 60 days
- Maximum password change interval – 90 days

However, according to the document “Centralize Computer System Security Policy,” the following password control should be implemented:

- Passwords expiration – 60 days

Inconsistencies exist between documented procedures and implemented procedures. Lack of complex passwords could increase the risk of unauthorized access if the passwords become common knowledge amongst system users.

**Trivial Passwords:** The accounts “dwasser” and “tsc” have trivial passwords. Weak passwords increase the risk of unauthorized access to the system and information resources. Weak password controls can also result in a loss of accountability for actions performed on the system.

**World-Writeable Files and Directories:** 555 files have world-writeable permissions. 77 of these files are owned by “Root.” Every user defined on the system has write access to these files and directories. This could increase the risk of unauthorized changes or deletions to these objects.

*UNIX (maximoprod) Security:*

**Password Controls:** Currently the following password controls are in place for maximoprod:

- Maximum password change interval – 13 weeks
- Lockout duration – 10 seconds
- Password history – not set

However, according to the document “Centralized Computer Systems Security Policy,” the following passwords controls should be implemented:

- Passwords expiration – 60 days
- Password history size – 5

Inconsistencies exist between documented procedures and implemented procedures. Lack of complex passwords could increase the risk of unauthorized access if the passwords become common knowledge amongst system users.

**Groups and Their Members:** There are 15 users on the system assigned to groups that they no longer require access to. If users are assigned to groups with excessive permissions to system resources, such users may have access to unnecessary system functions and information resources. As a result, access is not commensurate with job responsibilities.

**Recommendation:**

*UNIX (PLSjam) Security:*

**Password Controls:**

- **Minimum password change** – The minimum password change setting determines the earliest a user can change their password after resetting it. Management should consider changing the minimum password change interval to 1. This allows users to change their password after one day, in the event that someone discovers the password.
- **Maximum password change-** Management should determine appropriate maximum password change interval and ensure it is consistent with documented procedures.

**Trivial Passwords:** Management should consider changing the password for “dwasser” and “tsc” or deleting these accounts. These passwords should be changed to be more complex and be less easily guessed passwords reducing the risk of unauthorized access within the UNIX system.

**World-Writeable Files and Directories:** Management should consider reviewing the world-writeable files and directories owned by root on the UNIX (PLSjam) system. The business reasons for maintaining these files to have world writeable permissions should be clearly documented. The files that do not require such permissions should be modified or removed. Management’s monitoring and understanding of the necessity for these files can prevent unauthorized modifications.

*UNIX (maximoprod) Security:*

**Password Controls:** Management should consider implementing the documented policies around password controls. UNIX (maximoprod) passwords should be modified to match the requirements of the *Centralized Computer Systems Security Policy*. Per this document:

- UNIX passwords should expire after 60 days
- History size should be 6

Also management should consider increasing the lockout duration to 600 seconds (10 minutes).

**Groups and Their Members:** Management should consider reviewing the users defined in the different groups. The business reasons for maintaining users in certain groups should be documented and reviewed on a regular basis to prevent users from being assigned to groups with excessive permissions.

***Corrective Action Taken:***

The following corrective actions were taken by management and observed by the audit team.

*UNIX (PLSjam) Security:*

**Password Controls:** Minimum password change interval has been lowered to 1 and maximum password change interval has been lowered to 60 days as of January 17, 2008.

*UNIX (maximoprod) Security:*

**Password Controls:** As of January 17, 2008, management has lowered the password change interval to 8 weeks. They have also increased the Lockout Duration to 600 seconds.

Password history is not supported at this time. Per management, this will be addressed with the central password management that is scheduled for 2008.

**Groups and Their Members:** As of January 17, 2008, management has removed the 15 users from groups they did not need access to. Users have been deleted from the groups *maximo*, *nobody*, *noaccess*, and *other*. Nuucp was assigned to group nuucp.

***Management's Response:***

*UNIX (PLSjam) Security:*

**Trivial Passwords:** The userid "dwasser" password has been changed to conform to Policy and the userid "TSC" has been removed.

**World-Writeable Files and Directories:** The 77 root world-writeable permissions have been reviewed and are required by the associated applications.

*UNIX (maximoprod) Security:*

**Password Controls:** In SOLARIS 9, this setting is not available. We would require a change to the operating system by adding PAM modules to provide this functionality and possibly lose support.

## 2. Application Security – Maximo

### **Observation:**

Security can be strengthened on the Maximo application.

### **Background:**

During our assessment of the Maximo application, we identified the following area for improvement:

**Application Password Controls:** Currently the following password controls are not in place for the Maximo application:

- Passwords expiration
- Password history

This could increase the risk of unauthorized users gaining access to system information.

### **Recommendation:**

**Application Password Controls:** Management should consider implementing password parameters for Maximo to prevent unauthorized users from gaining access to the system.

Recommendations include the following parameters:

- Password Expiration – 60 days
- Password History Size – 6
- Password History Period – 180 days

### **Management's Response:**

#### **Application Password Controls:**

- **Password Expiration:** The Expiration will be set to 60 days expiration and 5 days notice of expiration. The user community will be notified via email and this change can be implemented by early 2008.
- **Password History Size Period:** At this time, the LIRR is running IBM Maximo Release 5.2, which does not support password history retention. The LIRR is scheduled to upgrade our Inventory Management application to Maximo - Release 6.0 by November 30, 2008. As per IBM documentation, Maximo 6 is configured to authenticate against an LDAP server directory. In the first quarter of 2009, plans will be established to test and employ this functionality.

## SECTION II – DEFINITIONS

The definition of a control deficiency is established in AU 325, *Communicating Internal Control Related Matters Identified in an Audit*, are as follows:

A *control deficiency* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A deficiency in *design* exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that even if the control operates as designed, the control objective is not always met. A deficiency in *operation* exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

\* \* \* \* \*