OFFICE OF THE
INSPECTOR GENERAL

LA County Metropolitan
Transportation Authority

818 W. 7th Street, Suite 500
Los Angeles, CA 90017

Telephone: 213.244.7300

Mailing Address
Post Office Box 811190
Los Angeles, CA 90081-1190

EXECUTIVE MANAGEMENT AND AUDIT COMMITTEE
August 19, 2004

SUBJECT: OFFICE OF INSPECTOR GENERAL (OIG) AUDIT ACTIVITIES REPORT

ACTION: RECEIVE AND FILE

RECOMMENDATION

Receive and file subject report.

ISSUE

The MTA Board of Directors requested the OIG to report on audit activities.

BACKGROUND

The OIG Charter mandated the creation of a unit to report directly to the MTA Board of Directors. The OIG has numerous responsibilities as defined in the Charter, and the OIG Audit Unit has a broad responsibility for oversight in a cooperative support mode with MTA management for increased accountability and improvement of MTA organizational performance.

A large measure of the OIG audit focus is to provide the MTA Board of Directors and MTA management with independent analyses, evaluations, and appraisals of performance effectiveness, accuracy of information, efficient use of resources, and adequacy of internal controls. In addition, the Audit Unit is charged with the detection and analysis of those items indicative of fraud, waste, or abuse.

DISCUSSION

The OIG recently issued the following audit reports:

1. Review of Policies and Procedures in the MTA

2. Review of Bus Operator Training and Medical Certification Procedures

3. Audit of Security Controls Over the Advanced Interactive Executive (AIX) Computer Operating System

4. Audit of MTA Miscellaneous Expenses, October 1, 2003 to December 31, 2003

The above audit reports were previously submitted to the Board and MTA management in their entirety.

Review of Policies and Procedures in the MTA

Many of the weaknesses cited in past audit reports resulted from deficiencies in agency-wide policies and procedures. Prior audit reports found that policies and procedures:

- were not established,
- were not followed when issued,
- were not disseminated to all appropriate officials and departments,
- were not up-to-date,
- did not cover key control areas of programs and activities, or
- were not dated, approved, and numbered.

The problems cited above indicate a need for increased management attention in the area of developing and disseminating policies and procedures. We found that:

- The guidelines for developing, processing, approving, and disseminating MTA policies were outdated and were not being followed.
- The list of policies and procedures was incomplete.
- Many policies were not posted on the MTA intranet.

Review of Bus Operator Training and Medical Certification Procedures

We found three areas where bus operator training could be improved.

- The Transit Operations Department's policy for annual line ride training for each operator was not being followed at all 11 divisions reviewed.
- Additional training needs could be met if certified instructors were not required to perform administrative tasks such as maintaining bus operator folders.
- A uniform training program had not been established.

We also noted several areas where medical testing procedures should be evaluated to determine whether there is a need to expand or refine current medical exam procedures.

Audit of Security Controls Over the Advanced Interactive Executive (AIX) Computer Operating System

We found that MTA needs to improve security over the AIX Operating System, which runs MTA's major computer application systems such as the Financial Information System, the Payroll System, and the Transit Operations Trends System.

Information Security policies and procedures, issued in 1996, had not been updated, and other procedures on AIX security were not officially approved and published. We also found several areas where AIX security procedures need strengthening:

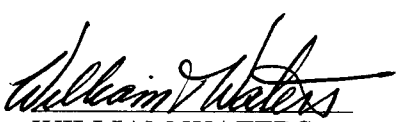
- Security controls over user account passwords were inadequate. The default security settings for the host machines we reviewed were not configured to meet all of the password security control standards established by ITS. For example, some passwords had not been changed for over 3 years although the security standards required that they be changed every 60 days.

- Procedures were not established for controlling changes made to the AIX Operating System. As a result, MTA was vulnerable to unauthorized changes made to the system.

- AIX terminals were not configured to automatically logoff at a specified length of time. Without this control, the risk is increased that unauthorized individuals could gain access to a logged-on terminal.

MTA Management agreed with the findings and recommendations discussed in this report and initiated the recommended corrective actions.

Prepared by: Jack Shigetomi, Deputy Inspector General - Audits



WILLIAM WATERS
Inspector General