Regional Transportation Authority

REVIEW OF THE INTERNAL CONTROLS OF THE RTA'S INFORMATION SYSTEM

INTRODUCTION

In accordance with the 2009 work plan, this report summarizes the results of the Audit & Review Division's annual review of the internal controls of the RTA's Information System, which is managed by the Information Technology (IT) Division. The annual review is performed in connection with a recommendation made by the RTA's external auditors (McGladrey & Pullen) that the Internal Audit Department perform detailed information systems control reviews and audits during the internal audit cycle to ensure that the Authority's information systems controls are adequate.

SUMMARY

The IT Division is responsible for overseeing the RTA's information resources and technology needs, which is monitored by the Manager of Information Technology under the authority of the Director, Administrative Services. The IT Division is also staffed by a Programmer Analyst, Senior Network Administrator, Help Desk/LAN Technician, Computer Systems Web Designer, Telecommunications Specialist and the TIC Systems Administrator.

The IT Division is responsible for the security, purchase, installation, maintenance, and repair of network equipment, printers, computers, and software. The RTA computer network is composed of the following:

- Network servers which maintain the corporate applications and databases.
- The distribution system which includes wiring, switches, hubs, and routers.
- Desktop computers, printers, and other peripherals.

The network servers are a critical part of the IT environment. The loss of a server for any reason would impair the ability of the RTA to perform essential mission tasks. The servers are connected to Uninterruptible Power Supplies (UPS), which will maintain the server in an operation status during short interruptions of power supply. The RTA utilizes 36 servers to operate its Information System.

Desktop computers are in place for the support of all RTA employees. The units are all Intel or compatible processor systems running the Windows 2000 or XP operating systems. There are also notebook computers assigned to the RTA senior staff and other employees as well. The primary software applications loaded on the desktop and laptop computers is MS Office 2003.

These systems are also running Norton Anti Virus software (Corporate Edition) to guard against computer viruses which can interfere with computer operation.

SCOPE OF REVIEW

The scope of the review included the following activities:

- Reviewed the progress in implementing the contingency plan.
- Reviewed the IT Policy and Procedures Manual.
- Reviewed the back-up tape schedule and off-site storage location.
- Reviewed the documentation related to the latest recovery testing.
- Reviewed the process for issuing/deactivating user access rights.
- Reviewed the process for obtaining IT loaner equipment.
- Reviewed the process for training employees on the RTA's information and telephone systems.
- Reviewed the process for submitting a help desk request.
- Surveyed employees who submitted help desk requests.
- Reviewed the telephone bills related to cellphone usage.
- Reviewed the physical, environmental, and logical security controls utilized to protect IT equipment.
- Reviewed the local area network security controls utilized to ensure the RTA's Information System is properly monitored and protected.
- Determined if there is adequate insurance coverage for the computer equipment.
- Reviewed the password policies and procedures in place.
- Reviewed the internet security controls utilized to ensure the RTA's Internet system is properly monitored and protected.
- Reviewed the written policies and procedures in place to process software changes and upgrades.
- Reviewed the procedures in place to protect the RTA's Information System from computer viruses or other security threats.
- Reviewed the monitoring procedures in place to ensure that the RTA's Information System is not accessed by outsiders and properly utilized by RTA staff.
- Reviewed the encryption policies and procedures in place.

OBSERVATIONS AND RECOMMENDATIONS

Overall, we found that the IT Division carries out its responsibilities efficiently and effectively to ensure the RTA's Information System is properly controlled. We offer the following eight recommendations to strengthen controls.

1. **Improve Monitoring of Network Access**

   Observation:

   A system is not in place to adequately monitor the individuals who access the RTA network.

   Recommendation:

   The Manager of IT should develop a system for monitoring the log on activity to the RTA network to determine if any unauthorized individuals are accessing the system. This review should be performed on a frequent basis and as part of the IT Division's monitoring of the security of the RTA's Information System.

   Management's Response:

   The Information Technology Division now has a more improved network monitoring system which will log the activity of users more efficiently. We will frequently monitor users' activity.

2. **Review RTA Staff Internet Access Rights**

   Observation:

   Staff access rights to internet websites are not reviewed periodically.

   Recommendation:

   The Manager of IT should periodically review the internet websites accessed by RTA employees for appropriateness and to determine compliance with written IT policies and procedures.

   Management's Response:

   The Information Technology Division will periodically review the internet websites accessed and attempted to be accessed by RTA users. In addition, the Information Technology Division maintains a web filtering software which monitors and denies access to all inappropriate websites.

3. **Improve Controls over Computer Equipment**

Observation:

The computer equipment stored in the IT staff office needs to be better secured.

Recommendation:

The Manager of IT staff should ensure that computer equipment is properly safeguarded to limit the possibility of misappropriation. Any equipment that is currently not being used by the RTA should be properly disposed of or donated.

Management's Response:

The IT staff office is locked whenever all staff members leave the office. The Information Technology Division currently does not have enough storage space to store the entire agency's resources/supplies; the agency is expected to expand its space by November 1, 2010. After the expansion, the Information Technology Division is expected to receive additional storage space which we will ensure adequately secures the RTA's assets. We will continue to dispose of broken equipment as needed.

4. **Inform RTA Staff of System Updates/Changes**

Observation:

IT staff does not consistently inform users in advance of the changes/updates to be made to the information system and the possible difficulties they may encounter.

Recommendation:

The Manager of IT should ensure proper notice is given before any changes are made to the RTA's Information System that could potentially affect the user's ability to access the system and perform daily tasks. This includes changes to be made to ancillary systems such as RTA - At Work Everywhere.

Management's Response:

In the future, the Information Technology Division will give as much notice as possible to users regarding system updates or changes.

5. **Improve Controls over Training for New Employees**

Observation:

Based upon the review of IT New Employee Orientation Check List forms:

a. An orientation check list form is not on file for two employees hired in 2009 to document the training provided. If training was not provided to those employees, a training session should be conducted and documented as soon as possible.

b. The applicable employees are trained on the IT equipment they will be issued (such as cellphones, Blackberrys, and laptops). However, there is no documentation on file recording the issuance of those items to the employee.

c. The IT staff member conducting the orientation does not consistently record on the orientation check list form the date of the IT policy manual being distributed to the new employee or ensure that the employee properly completes the form.

d. The completed new hire orientation check list forms are not maintained in the IT Division's files.

Recommendation:

The Manager of IT should ensure that adequate training is provided to each new employee and evidenced by a properly completed orientation check list form. A copy of each orientation check list form should be maintained by IT. In addition, a process needs to be developed to track the IT equipment issued to staff to ensure there is a record of the items to be retrieved if the employee leaves the RTA.

Management's Response:

The Information Technology Division will:
   a) Contact HR to obtain the names of the two employees hired in 2009 to document training as soon as possible.
   b) More efficiently document training of cellphones, blackberrys and laptops when given to the employee at the time of issuance. The Division will keep better documentation on file for the issuance of those items given to employees. In addition, the Division will have each employee with RTA devices sign the updated loan issuance form for better tracking. The IT Division and HR will maintain copies. This will be completed by April 30, 2010.
   c) Update the orientation check list to include the date of the IT policy manual given to the employee.
   d) Maintain a copy of the completed new hire orientation check list in the department files.

6. Ensure Accuracy of Loaner Equipment Requests

Observation:

Based upon the review of IT Loan Request Forms:

a. RTA staff does not always provide the correct date to be utilized as the start of the loan period.

5

b. The loan request form does not include all equipment options available for staff.

Recommendation:

The Manager of IT should update the loan request form to ensure RTA staff is provided with all loaner equipment options available and ensure that RTA staff is properly trained on how to complete the form.

Management's Response:

The Manager of IT has already updated the IT Loan Request Form to include all loan options available. The Information Technology Division will provide help/training to RTA staff on how to complete the form by April 30, 2010.

7. **Improve Controls over IT Loaner Equipment**

Observation:

Based upon the review of iApprove forms which detail the activity of equipment loaned to RTA staff:

a. IT's current loan equipment tracking system is a manual system that does not provide the department with the necessary features to be able to properly issue, track, and return to inventory the RTA assets loaned to employees.

b. The equipment loan request made by an employee is not linked to IT's loan equipment tracking system. Because of that, we found instances where the items requested on the loan request form do not agree with the items checked out/in on the iApprove form. This occurs most often when an employee requests additional loaner equipment and IT staff has to manually record those items. In those cases, IT staff does not consistently record comments on the iApprove form to state the additional items requested by the employee. Furthermore, even though the employee must provide a return date on the loan request form, there is no system in place to track if the IT equipment is returned by that date.

c. IT staff does not consistently record the asset tag numbers of the equipment loaned to staff.

d. The status of the loan request does not appear to be properly reflected on the iApprove form. We found that when an employee cancels their loan request, the status is recorded in the iApprove form as 'Denied'. We also found that when an employee returns the equipment, the status is recorded on the iApprove form as 'Check In' when a more appropriate option would be 'Returned'.

e. IT staff does not track the equipment loaned to an employee for use on the RTA premises in the same manner as equipment taken off-site. Because of this, RTA assets are not being properly monitored to limit the possibility of misappropriation.

Recommendation:

The Manager of IT should determine if there is a loan equipment system that would more effectively serve the needs of the RTA than the manual system currently utilized. An efficient loan equipment system would be linked to the employee's request and the inventory of IT equipment. Therefore, once the request is submitted, the employee would be informed immediately if the request can be fulfilled. The system would track all equipment loaned, whether for use on the RTA premises or off-site, to ensure the equipment is properly returned to IT to lessen the chances of RTA assets being misappropriated.

Management's Response:

The Information Technology Division is currently designing (in-house) an updated Loaner Equipment form and process to accomplish better tracking. This new process and form will address the concerns of Audit & Review. We anticipate a completion date of April 30, 2010.

8. Improve Controls over Help Desk Requests

Observation:

Based upon the review of help desk requests:

   a. Help desk requests do not always appear to be assigned to an IT staff member in a timely manner.

   b. Help desk requests are not always completed by the requested due date.

   c. Help desk requests are not always closed promptly once the technician has completed the work.

Recommendation:

When an employee submits a help desk request, the request should be promptly assigned to an IT staff member to handle. If the request can not be completed by the requested due date, the employee should be notified and the appropriate actions should be taken by IT to work towards a resolution. Once the request has been completed, the ticket should be promptly closed. It would be helpful for the system to alert IT staff of the status of each help desk ticket. This would allow IT staff to stay better informed of the progression of the help desk request, pending due dates and when help desk requests are completed and should be properly closed.

Management's Response:

Once a help desk request is input into the system, the system will assign a technician based on the category of the support. If the request can not be completed by the requested due date, the technician will notify the requestor verbally of an estimated completion date. The technician will also be in contact with the requestor as needed until the request is completed. All completed tickets should be closed at the end of that day; or they will be closed by the

close of business each Friday and will state the completed/closed date for which the ticket was actually closed.

Catherine M. Clark
Manager, Internal Audit & Review Division
February 11, 2010