AUDITOR'S REPORT

HARRIS COUNTY TOLL ROAD AUTHORITY
GENERAL CONTROLS REVIEW

December 16, 2016

Barbara J. Schott, C.P.A.
Harris County Auditor

Mike Post, C.P.A.
Chief Assistant County Auditor
Accounting Division

Mark Ledman, C.P.A., M.P.A.
Chief Assistant County Auditor
Audit Division

1001 Preston, Suite 800
Houston, Texas 77002-1817
(713) 755-6505

FAX (713) 755-8932
Help Line (713) 755-HELP

BARBARA J. SCHOTT, C.P.A.
HARRIS COUNTY AUDITOR

December 16, 2016

Mr. Gary Trietsch, P.E.
Executive Director
Harris County Toll Road Authority
7701 Wilshire Place Dr.
Houston, TX 77040

RE: Harris County Toll Road Authority General Controls Review – As of May 6, 2016

The Audit Services Department performed procedures relative to Harris County Toll Road Authority's (HCTRA) information technology (IT) general controls. The objective of the engagement was to determine whether HCTRA IT addressed satisfactorily the IT related findings noted in the Deloitte & Touche 2014 Management Letter.

Our procedures included the following:

1. Selectively examined Automated Toll & Traffic Law Administration System (ATTLAS), Central Host Audit System (CHAS) and EZTAG configuration documentation and system-generated password management features to verify that passwords complied with County policy (i.e., expiration, complexity, history, length, etc.) at the application, database and operating system levels.

2. Selectively examined new, terminated and transferred user (employees and contractors) access for ATTLAS, CHAS and EZTAG to confirm their accounts had been approved and provisioned appropriately at the application, database and operating system levels.

3. Selectively examined "User Access Review" reports for HCTRA applications (ATTLAS, CHAS and EZTAG), to determine whether user access reviews were being performed routinely for appropriateness.

The engagement process included providing you with engagement and scope letters and conducting an entrance and exit conference with your personnel. The purpose of the letters and conferences were to explain the process, identify areas of concern, describe the procedures to be performed, discuss issues identified during the engagement, and solicit suggestions for resolving the issues. A draft report was provided to you and your personnel for review.

Mr. Gary Trietsch, P.E.
Executive Director

The work performed required our staff to exercise professional judgment in completing the scope objectives. As the procedures were not a detailed examination of all transactions, there is a risk that error or fraud was not detected during this engagement. The official therefore, retains the responsibility for the accuracy and completeness of their financial records and property and ensuring sufficient controls are in place to detect and prevent fraud, errors and omissions.

The enclosed Auditor's Report presents the significant issues identified during our procedures, recommendations developed in conjunction with your staff, and any actions you have taken to implement the recommendations.

We appreciate the time and attention provided by you and your staff during this engagement.

Sincerely,

Barbara J. Schott
County Auditor

cc: District Judges
County Judge Ed Emmett
Commissioners:
R. Jack Cagle
Jack Morman
Steve Radack
Gene Locke
Devon Anderson
Vince Ryan
William J. Jackson

TABLE OF CONTENTS

OVERVIEW

HCTRA was established in 1983 by the Harris County (County) Commissioners Court pursuant to Chapter 284 of the Texas Transportation Code. Also in 1983, County voters authorized issuance of up to $900 million in bonds to construct, operate and maintain toll roads in the County. The first two components of the toll road system, the Hardy Toll Road and the Sam Houston Tollway-West were completed in 1987 and 1990 respectively. In 1994, the County purchased the Jesse H. Jones Memorial Bridge toll facility from the Texas Turnpike Authority, which was renamed the Sam Houston Ship Channel Bridge. In 2004, HCTRA opened the Westpark Tollway; in April 2009, the Katy Managed Lanes were opened for full operations; and in February 2011, the 13-mile Sam Houston Tollway Northeast section opened with all-electronic tolling. Revenues collected are used to recover costs and retire outstanding debt on roadway projects.

Since October 2004, HCTRA completed an extensive program to revitalize their automated toll collection and information management system to accommodate a significant increase in new roadways, customers, and revenues. HCTRA entered into a contract with third-party vendor Electronic Toll Collection (ETC), a subsidiary of Autostrade International U.S. Holdings, Inc., to provide back office toll software.

The HCTRA system is comprised of the following five distinct subsystems responsible for toll collection and control: EZTag Store, Online EZTag Store, CHAS, Plaza Host System, and ATTLAS. With the exception of ATTLAS, all HCTRA applications were developed and are managed by ETC. ATTLAS was developed by third-party vendor Transcore.

ETC manages both the application and database environment for EZTAG, CHAS and the Plaza Host System. HCTRA IT manages the hardware. The contractor also provides technical guidance relative to operating the information management function. HCTRA's IT department serves as the primary point-of-contact with ETC on matters related to the toll collection system. Transcore manages both the application and database environment for ATTLAS.

HCTRA is in the process of implementing ETC's new RITE 2.0 back office toll system that will replace the ATTLAS, CHAS and EZTAG applications. Full implementation is scheduled for June 2017.

RESULTS

Based on procedures performed, Audit Services determined that the IT related findings in the Deloitte & Touche fiscal year 2014 Management Letter were not addressed sufficiently.

Audit Services identified opportunities for improvement in HCTRA's IT general controls environment as noted below:

- Enhance the new hire provisioning process to better align employee and contractor access to HCTRA applications and their respective databases to their assigned job role.

- Ensuring that Helpdesk Expert Automation Tool (HEAT) tickets are submitted to remove or disable contractor access to all HCTRA systems in a timely manner upon termination of service.

- Establishing a formal process to track inter-departmental employee and contractor transfers; requiring managers to submit HEAT tickets to modify or remove transferred user access from systems based on their newly assigned roles; and removing access that is no longer warranted.

- Performing a formal user access review that includes documented manager review of employee access to HCTRA computer applications to confirm that users are granted appropriate levels of privileges based on their job responsibilities.

- Configuring password parameter settings on all HCTRA applications, databases and server operating systems that comply with HCTRA published standards.

These issues are explained in more detail in the Issues and Recommendations section.

ISSUES AND RECOMMENDATIONS

New-Hire Employee and Contractor Access

Background:

HCTRA Human Resources (HR) submits approval for HCTRA IT to grant new hire employees or contractors access to the HCTRA computer network and systems using the HEAT software.

Issue:

HCTRA IT does not uniformly grant newly hired employees and contractors access to the ATTLAS, CHAS and EZTAG applications and databases with the user's specific job requirements. As a result, ATTLAS, CHAS and EZTAG users may be granted excessive or inappropriate access to HCTRA systems that is inconsistent with their assigned duties. Below is the result of our testing procedures:

1. 4 of 20 (20%) full time employees CHAS application user accounts have administrator-level privilege to the CHAS database through an assigned database role (TXNUSER).

2. 1 of 20 (5%) EZTAG database accounts assigned to a former employee of EZTAG's third-party software developer (ETC) had inappropriate administrator-level access.

3. 1 of 20 (5%) full time employees did not have a HEAT ticket approval submitted prior to access being granted.

4. 1 of 20 (5%) new-hire full time employees was granted privileges to the ATTLAS and EZTAG applications that exceeded the level of access granted to the user the HEAT ticket instructed to mirror.

5. 1 of 20 (5%) of HEAT tickets for new hire full time employees did not document the approved privileges to grant in ATTLAS and EZTAG.

6. 1 of 20 (5%) of HEAT tickets for new hire full time employees did not document the approved privileges to grant in CHAS.

7. HEAT tickets are routinely submitted with instructions to mirror a new employee or contractor's access from the access granted to an existing user. The HEAT tickets for 7 of 20 (35%) new hire full time employees and 3 of 20 (15%) new contractors provided instructions to mirror the user after terminated employees whose access was removed from ATTLAS, CHAS and/or EZTAG. As a result, assessing whether the appropriate level of access to ATTLAS, CHAS and/or EZTAG was granted, based on the HEAT ticket approvals, could not be determined.

Inappropriate or excessive privileges granted to HCTRA applications and databases could allow unauthorized access to HCTRA data.

ISSUES AND RECOMMENDATIONS

Recommendation:

In addition to correcting the issues noted above, HCTRA management should develop access roles to the ATTLAS, CHAS and EZTAG applications and their supporting databases that align to each specific HCTRA job title and assign those roles to new hire employees and contractors based on their assigned duties and with the appropriate approvals.

Management Response:

HCTRA agrees that roles should be developed for a majority of job titles and is working towards developing roles primarily for those with job assignments within Customer Service. In addition, roles are being developed and defined for the new Back Office System (BOS).

With the exception of item 1, which was addressed on October 6, 2016 via RFC20160140, HCTRA attempted to correct items as the findings were made.

ISSUES AND RECOMMENDATIONS

Terminated Employee and Contractor Access Removal

Background:

HEAT tickets are submitted by HCTRA HR notifying the HCTRA IT Help Desk of terminated users that require access removal from the HCTRA computer network and systems.

Issue:

HCTRA HR does not submit all HEAT tickets authorizing removal of system access of terminated employees in a timely manner. As a result, 2 of 20 (10%) HCTRA contractors were submitted in excess of 60 days from their termination date. One of these 2 HEAT tickets was submitted after 128 days of the contractor's termination date and the other after 68 days. Audit Services noted both contractors did not gain access to HCTRA applications and databases as of our audit engagement's start date as accounts are locked out after 60 days of inactivity.

Untimely removal of user access to application and databases could allow a terminated contractor to log in and manipulate or compromise HCTRA data.

Recommendation:

HCTRA HR should ensure that all HEAT tickets with requests to remove or disable terminated employees or contractors are created timely and properly closed within a pre-determined amount of time from their termination date. A termination checklist should be considered to follow up and complete termination steps, including removal of all network and system access. A continuous monitoring process should be implemented to follow up on terminated employees and contractors to minimize the risk of unauthorized access after termination.

Management Response:

HCTRA HR will be responsible for submitting HEAT tickets for employees change of status as related to the system access. HCTRA HR will consider best practices to create a termination checklist to complete all terminations steps. HCTRA will continue to set all contractor accounts to expire either at the end of the contract term or every 6 months, whichever is shorter in duration. In addition, HCTRA reviews and purges inactive accounts once a quarter regardless of the contractor’s status.

ISSUES AND RECOMMENDATIONS

Transferred User Tracking and Notification

Background:

Based on HCTRA's "Data Access and User Authentication Standard" HCTRA HR notifies all affected departments of all user transfers. These departments include: Administrators of Windows, UNIX, databases, ATTLAS, EZ Tag and Physical Security.

Issue:

HCTRA HR does not have a process in place to track transferred employees and contractors and to notify HCTRA IT of these transfers so the required changes in levels of system access (i.e., removal of unneeded access) are made on a timely and efficient basis. As such, this access could allow those users to retain system privileges inconsistent with their job requirements.

Recommendation:

HCTRA HR should design and implement a process to track inter-departmental employee and contractor transfers and to require managers to submit HEAT tickets to modify or remove transferred user access from systems based on their new job requirements. HCTRA IT should then perform the necessary changes on users' access based on employee and contractor transfers documented in HEAT tickets.

Management Response:

HCTRA IT has developed the ability to capture and report on a "Change in Status" within IFAS for employees. Information Security is notified of changes nightly and has a process in place to review those changes in order to determine if user access needs to be modified. Once ITMS (new ticketing system) is implemented, HCTRA should be able to create a process workflow to help automate the review and approval process. HCTRA IT will consider developing the ability to track the change in status of a contractor.

ISSUES AND RECOMMENDATIONS

User Access Review

Background:
Based on HCTRA's "Data Access and User Authentication Standard", access to each system, application, or database shall be reviewed annually at a minimum.

Issue:
HCTRA management has not performed a formal user access review for the CHAS, ATTLAS and EZTAG applications and their respective databases and server operating systems. As a result, inappropriate user access may exist on applications, databases and operating systems that could compromise HCTRA business data. HCTRA IT management informed us that higher priority projects had taken precedence and that a user access review had not yet been performed.

Recommendation:
HCTRA IT should conduct a formal user access review for the CHAS, ATTLAS and EZTAG applications and their respective databases and server operating systems on a semi-annual basis. This process would allow for a more efficient rights and privileges data conversion into the future RITE 2.0 application.

Management Response:
HCTRA completed a review of all user accounts in June 2016 for ATTLAS, CHAS and EZTag with plans to conduct annual reviews in the future and/or at the time of conversion to the new Back Office System (BOS).

HCTRA performs quarterly reviews of all user accounts in order to insure that there are no "orphaned" accounts from the HCTRA terminations process and that inactive users still require access to the application. Semi-annual reviews of user access and appropriateness is not believed to be necessary since HCTRA deals more with staff turn-over than transfers.

HCTRA agrees that a review of all system accounts would be desirable; however, reviewing and testing changes required for just one system account took HCTRA and its primary tolling vendor, ETC, 4 months to complete. HCTRA believes that it is a better use of resources to insure that all system accounts for the new BOS are reviewed and documented before system implementation.

ISSUES AND RECOMMENDATIONS

Application and Database Layer Password Configurations

Background:

Password configuration settings for the ATTLAS, CHAS and EZTAG applications are governed through a combination of application and database rules as set forth in the HCTRA published standards.

Issue:

Password configuration settings for the ATTLAS, CHAS and EZTAG application and database layers do not fully comply with the HCTRA Password Management Standard as indicated in the following:

1. ATTLAS, CHAS and EZTAG passwords have a minimum length of 7 characters and do not meet the HCTRA Password Management Standard's minimum length requirement of 8 characters for applications users and 12 for privileged database-level access.

2. CHAS and EZTAG users can reuse the same password repeatedly.

3. CHAS and EZTAG passwords are set to expire after 90 days and are also allowed a grace period of an additional 90 days past the expiration date before the user's account is locked. As such, the combination of the two settings could allow the same password to potentially be used a total of 180 days before the account is locked.

Weak password configuration settings could allow passwords to be easily guessed by intruders, exposing and compromising HCTRA applications and financially-sensitive data.

Recommendation:

HCTRA Management should configure password parameter settings for the ATTLAS, CHAS and EZTAG application and database layers that comply with HCTRA published standards.

Management Response:

HCTRA agrees with the recommendation, however access to ATTLAS, CHAS and EZTag require access to HCTRA's network through a Windows Active Directory Account. HCTRA's Password Management Standards are in force and Active Directory is configured to enforce HCTRA Standards.

Some applications have user accounts and passwords for both the application and corresponding database. Within some of the legacy applications, some password parameters are enforced within the application and others within the database. Changing password parameters within the ATTLAS, CHAS and EZTag applications/databases will require extensive testing within the Development and UAT environments in order to determine the impact of any changes. Resources are better utilized in getting HCTRA onto the new Back Office System (BOS) which uses Active Directory for authentication.

ISSUES AND RECOMMENDATIONS

Operating System-Layer Password Configurations

Background:

Password configuration settings for the Unix operating system are governed by documented HCTRA approved Password Management standards.

Issue:

Password configuration settings for the Unix server operating systems supporting the ATTLAS, CHAS and EZTAG applications do not fully comply with the HCTRA Password Management Standard.

The following password configuration settings for the Unix servers supporting the ATTLAS, CHAS and EZTAG applications did not fully meet the requirements of the HCTRA Password Management Standard (the seven servers tested were the ATTLAS dbs06vp server; CHAS app03vp, app04vp and dbs07vp servers; and, the EZTAG app05vp, app06vp and dbs05vp servers):

1. 7 of 7 (100%) servers tested had the password minimum length set to eight characters. The HCTRA Password Management Standard requires 12 characters for privileged users.

2. 3 of 7 (43%) servers (dbs05vp, dbs06vp and dbs07vp) did not require that a new password be different from the previous 5 passwords, and therefore, did not comply with the HCTRA Password Management Standard.

Weak password configuration settings could allow passwords to be easily guessed by intruders, exposing and compromising the servers and corresponding operating systems.

Recommendation:

HCTRA Management should configure operating system password parameter settings on the Unix servers that comply with HCTRA published standards.

Management Response:

HCTRA agrees with the recommendation.

HCTRA plans to utilize a Privileged Identity/Access Management application to integrate the security of HCTRA's Unix, Linux and Solaris servers into Windows Active Directory to help us achieve compliance. HCTRA estimates that the project will take approximately 12 months to completely implement once procured. This project should begin in January 2017.