CITY OF SAN ANTONIO

OFFICE OF THE CITY AUDITOR

Audit of Aviation Security Division

Project No. AU19-003

December 18, 2019

Kevin W. Barthold, CPA, CIA, CISA
City Auditor

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted an audit of the Aviation Department, specifically the security division. The audit objectives, conclusions, and recommendations follow:

Determine if Aviation security division operations are in compliance with regulations and policies and operations are managed effectively and efficiently.

Aviation security division operations are in compliance with required rules and regulations. They have developed effective policies and procedures and implemented controls to ensure the safety and security of Airport.

However, there are opportunities to strengthen controls associated with accounting for processing fees collected and the physical access to IT server rooms that host sensitive security information.

We recommend that the Aviation Security Management:

- Develop a process to reconcile the badge activities performed to the processing fees collected.

- Remove any inappropriate users from accessing the server rooms and perform a periodic user access review that restricts employee access to a level necessary to perform employee job duties.

Aviation Security Division agreed with the audit findings and has developed positive action plans to address them. Management's verbatim response is in Appendix B on page 6.

Table of Contents

Background

The Aviation Security Division is responsible for the security and compliance of the San Antonio International Airport (Airport). Security is a collaborative effort facilitated by the Transportation Security Administration (TSA), San Antonio Airport Police Department and the Aviation Department's Security Division. The Aviation Security division oversees the following groups: Security Compliance, Security Operations, Security Systems, and Badge & ID.

The Compliance group ensures the Airport as well as its tenants remain in compliance with Title 49 Code of Federal Regulations (CFR) 1542, the Airport Security Program, and the Transportation Security Administration Security Directives. Operations provides uniformed patrol and access control alarm response to the airport 24 hours a day. This group controls entry and exit into sensitive areas of the concourses, Air Operations Area (AOA), and Secured Areas of the Airport and assists Airport Police as needed.

The Security Systems group is responsible for maintaining and ensuring the Airport security systems and applications are operational. Additionally, the Badge and ID Office issues and maintains Airport badges for employees and contractors who work and require access to the Airport. The Aviation Security Division collected a total of $538,604.83 and $380,761.07 in badging fees for fiscal year 2018 and 2019 respectively.

Audit Scope and Methodology

The audit scope included the Airport security operations for fiscal years 2018 through June 2019.

We obtained and reviewed the Airport Security Program to determine if policies were established and in accordance with Federal Security Requirements. We performed walk-throughs and interviewed Aviation Security staff to gain an understanding of controls and techniques utilized to ensure the security of the airport.

Additionally, we reviewed 25 comprehensive badge audits performed by the Security Division to determine if all tenants and facilities were included and performed in accordance to TSA regulations.

We also reviewed a sample of 40 new badge applications to determine if all required documentation was obtained, approved, accurately processed, and appropriately safeguarded. Finally, we reviewed the Badge and ID Office's cash handling process to determine compliance with City Cash Handling AD 8.1.

We relied on computer-processed data in from Velocity Access Control System to validate user access is based on the principle of least privilege. Our direct testing included reviewing the user access listing and comparing it to active employee's job responsibilities to determine appropriate user access. We tested the general and applications controls of the Velocity and Genetec servers to determine if servers were adequately backed-up and scanned for vulnerabilities. We also reviewed the CCTV system for proper functionality and archiving.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results and Recommendations

A. Badge and ID Processing

The Aviation Badge and ID office does not reconcile the badge activities performed to the processing fees collected. Currently, the only reconciliation performed compares the amount of cash collected to the amount of cash deposited.

The Airport Badge and ID office is responsible for issuing and maintaining badges for employees and contractors who work and require access to the Airport. The Badge ID office processing fees include but are not limited to new badges ($100), renewals ($35), and non-returned badges ($150).

Over a six-month period, the Badge and ID office collected a total of $70,435 in processing fees, $19,345 in cash or cash equivalents, and $51,090 in credit cards. Additionally, Badge and ID office personnel have the ability to waive fees for CoSA employees or not collect payment and bill contractors for services provided.

Reconciliations help ensure that all collections for services provided are accurate and complete. Failure to adequately reconcile and account for payments for activities performed increases the risk of lost revenue.

Recommendations

Aviation Security Management should develop a process to reconcile the badge activities performed to the processing fees collected. The reconciliation should also include those activities where fees were waived or not collected.

B. Excessive User Access

Physical Badge Access to IT server rooms is excessive. Additionally, Badge and ID systems division does not perform periodic physical user access reviews.

We reviewed the physical user access listing and identified 242 individuals with access to server room A and 267 individuals with access to server room B. However, badge activity for a seven-month period identified only 35 (14%) users accessed server room A and 47 (18%) accessed server room B. Additionally, due to lack of adequate support documentation, we were unable to determine if 85 non-CoSA user's physical access was appropriate.

According to City Administrative Directive 7.8d, a periodic review of user access should be performed no less than annually and access authorization should be well defined and documented. Additionally, access should be granted in

accordance to the principle of least privilege. Inappropriate physical access to server rooms and its supporting infrastructure can increase the risk of tampering and potentially compromise airport security.

Recommendation

Aviation Security Management should remove any inappropriate users from accessing the server rooms and perform a periodic user access review that restricts employee access to a level necessary to perform employee job duties. In addition, obtain appropriate justification and approval for those employees requesting access to server rooms.

Appendix A – Staff Acknowledgement

Gabriel Treviño, CISA, Audit Manager
Lawrence Garza, CFE, Auditor in Charge
Daniel Kuntzelman, CIA, CISA, Auditor

Appendix B – Management Response

CITY OF SAN ANTONIO
SAN ANTONIO TEXAS 78283-3966

December 3, 2019

Kevin W. Barthold, CPA, CIA, CISA
City Auditor
San Antonio, Texas

RE: Management's Corrective Action Plan for the Audit of Aviation Security Division

Aviation has reviewed the audit report and has developed the Corrective Action Plans below corresponding to report recommendations.

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
1	**Badge and ID Processing** Aviation Security Management should develop a process to reconcile the badge activities performed to the processing fees collected. The reconciliation should also include those activities where fees were waived or not collected.	3			
	Action plan: • Aviation Security is working on a long term technology solution called Identity Management System (IDMS) scheduled to go live in early 2020 which will address this audit recommendation. The implementation of IDMS will provide a reporting capability that will allow for reconciliation and improved tracking of all customers seen and fees collected or waived by the Badge & ID Office. IDMS has a unique work flow process that will not allow one Badge & ID staff member to take a badge applicant from start to finish without all required steps being completed (ID verification, payment, photographs, fingerprints, etc.). • The Badge & ID Office has implemented an interim solution until IDMS goes live by using a spreadsheet to capture badge processing activities to include fees waived or not collected. • In January 2020, the Badge & ID Office will reduce the types of payment methods accepted by going cashless which should minimize the possibility of fraudulent activity and/or counterfeit bills being accepted.				

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
2	**Excessive User Access** Aviation Security Management should remove any inappropriate users from accessing the server rooms and perform a periodic user access review that restricts employee access to a level necessary to perform employee job duties. In addition, obtain appropriate justification and approval for those employees requesting access to server rooms.	3			
	Action plan: • Aviation Security worked with ITSD (Network Administrator) to conduct a thorough review of users having access to airport server rooms. The list of users with access to server rooms were reduced to sections and individuals with an operational need to perform duties, to include CoSA ITSD, CoSA Fire Protection, Aviation Security and contractor personnel approved by ITSD. • All future access requests to server rooms will be required to complete an access request form and must be approved by ITSD prior to Aviation Security granting access. • Twice annually at a minimum, Aviation Security and ITSD will review user access activity to server rooms and ensure users have an operational need to have access to server rooms.				

We are committed to addressing the recommendations in the audit report and the plan of actions presented above.

Sincerely,

For Russell J. Handy
Director
Aviation Department

12-3-19
Date

Carlos J. Contreras, III
Assistant City Manager
City Manager's Office

12/6/19
Date

2