Audit Team
Jared Miller, CISA, CFE, IT Audit Supervisor
Nicholas Jimroglou, CISA, Lead IT Auditor
Brian Cheli, CISA, CISSP, Senior IT Auditor

Audit Management
Timothy M. O’Brien, CPA, Auditor
Valerie Walling, CPA, Deputy Auditor
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Director

Audit Committee
Timothy M. O’Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000 • Fax (720) 913-5253

Or download and view an electronic copy by visiting our website at: www.denverauditor.org.
September 19, 2019

AUDITOR’S LETTER

The objective of our audit of cybersecurity operations at Denver International Airport was to determine the effectiveness of the airport’s cybersecurity processes, policies, and governance. We assessed how well the airport’s Business Technologies department and cybersecurity operations team were prepared to identify, protect, detect, respond, and recover from cybersecurity incidents. Our review period covered calendar year 2018 through July 31, 2019. I am pleased to present the results of this audit.

The audit revealed the airport’s Business Technologies department needs to better integrate its cybersecurity operations team with the rest of the airport and City to effectively protect airport assets, data, and systems. The lack of communication with other airport operations and with other City agencies weakens the effectiveness of the Security Operations Center and results in missed opportunities to improve the IT security of the airport. We also identified security-related findings, which have been communicated separately to the airport’s Business Technology management for remediation.

Through implementing recommendations for stronger integration and communication with other airport and City stakeholders, Business Technologies will be better equipped to protect airport assets, data, and systems.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, “General Powers and Duties of Auditor,” and was conducted in accordance with generally accepted government auditing standards. Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We extend our appreciation to the airport’s Business Technologies personnel who assisted and cooperated with us during the audit. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor’s Office

Timothy M. O’Brien, CPA
Auditor
Objective
The objective of our audit of cybersecurity operations at Denver International Airport was to determine the effectiveness of the airport’s cybersecurity processes, policies, and governance. We assessed how well the airport’s Business Technologies department and cybersecurity operations team were prepared to identify, protect, detect, respond, and recover from cybersecurity incidents.

Background
The airport’s Business Technologies department is responsible for managing and safeguarding the airport’s network and technology equipment, including data and infrastructure. This department also provides cybersecurity services to protect the airport from threats and vulnerabilities.

Report Highlights

Highlights
In our audit of cybersecurity operations at Denver International Airport, we determined that the Security Operations Center needs to improve communication and collaboration within its cybersecurity operations.

The Airport’s Security Operations Center Needs To Improve Communication and Collaboration with Internal and External Stakeholders

- There is limited collaboration between the airport’s Security Operations Center and its key stakeholders.
  - Meetings between Security Operations Center staff and other information technology officials at the airport focus largely on business goals, rather than processes and tool-sharing for cybersecurity purposes.
  - The Security Operations Center does not communicate with airport personnel who manage vendors.
  - Security Operations Center personnel do not formally communicate with other airport divisions on actions such as network scans, which has caused system disruptions at times.

- The Security Operations Center uses unapproved and ineffective policies and procedures.
  - There is no evidence of a signed nondisclosure agreement for one IT security contractor.
  - The Security Operations Center uses policies and procedures that have not been signed by executive management.
  - The Security Operations Center should improve its lessons-learned process following a security incident.

For a copy of this report, visit www.denverauditor.org or contact the Auditor’s Office at (720) 913-5000.
# TABLE OF CONTENTS

## BACKGROUND  
1

## FINDING  
7

The Airport’s Security Operations Center Needs To Improve Communication and Collaboration with Internal and External Stakeholders

- There Is Limited Collaboration between the Airport’s Security Operations Center and Its Key Stakeholders 7
- The Security Operations Center Uses Unapproved and Ineffective Policies and Procedures 10

## RECOMMENDATIONS  
14

## AGENCY RESPONSE TO AUDIT RECOMMENDATIONS  
16

## OBJECTIVE, SCOPE, AND METHODOLOGY  
20
BACKGROUND

Denver International Airport, operated by Denver’s Department of Aviation, was established and is governed by Denver’s City Charter. Denver’s airport is the fifth-busiest airport in the United States and the 20th-busiest in the world. In 2018, the airport served 64.5 million passengers.¹

As the airport continues to grow, it faces constant challenges involving information security and cybersecurity.

Business Technologies and Cybersecurity

The airport’s Business Technologies department is responsible for managing information security and cybersecurity activities. Business Technologies manages data centers and provides services for technical infrastructure, maintenance, voice and data networks, wireless networks, and cybersecurity.

To adapt to the rapidly changing environment in the information security industry, the airport’s Business Technologies department created a five-year strategic plan to develop security strategies and goals. These strategies include:²

- “Promoting business and information technology innovation while protecting investments, data, and service availability”
- “Maturing the airport’s cybersecurity program through continuous improvement”
- “Advancing cybersecurity capabilities by aligning with recommended frameworks, such as the National Institute of Standards and Technology”
- “Measuring all information technology systems at the airport using specific security standards in conjunction with aviation industry experts”

Business Technologies also uses a standards-based approach aligned with the National Institute of Standards and Technology’s cybersecurity framework to identify, protect, detect, respond, and recover to cybersecurity risks occurring at the airport.³ This framework, as shown in Figure 1 on the next page, is meant to protect airport digital assets,

³ The National Institute of Standards and Technology is a laboratory and nonregulatory federal agency within the U.S. Department of Commerce that develops measurements and standards for science and technology.
The National Institute of Standards and Technology’s “Framework for Improving Critical Infrastructure Cybersecurity” offers ways to address cybersecurity, including cybersecurity’s effect on physical, cyber, and people elements.\(^4\)

Cybersecurity can be defined as the protection of information or the preservation of the integrity, confidentiality, and availability of information in cyberspace. Cyberspace is the environment in which people, software, and services interact through internet and network connections. The National Institute of Standards and Technology also provides a comprehensive approach to information security and managing risk by providing organizations, such as the airport, with security control best practices that strengthen their information systems and the environments in which they operate.\(^5\)

Business Technologies uses these standards and has developed four primary initiatives:

- **Information Technology Risk Management**: To identify and manage information technology risk in accordance with industry standards and risk management principles.

---


• **Cybersecurity Threat Management**: To protect data, reputation, and service availability from cybersecurity incidents.

• **Threat Intelligence and Information Sharing**: To establish relationships to aid in strategic development and incident response assistance, as well as to foster the sharing of intelligence related to imminent or emerging threats.

• **Payment Card Industry Data Security Standards and Sensitive Security Information Regulatory Compliance**: To maintain compliance with required regulatory standards and for information falling under the U.S. government’s information sharing and control rules.

The overall goal of the airport’s cybersecurity threat management initiative is to protect the airport’s reputation, data, and service availability from cybersecurity threats or threat actors. As shown in Figure 2, threat actors can be anything from insider threats—such as airport employees, vendors, and contractors—to foreign nations. Foreign threats are often highly sophisticated and from well-funded entities such as other governments who may wish to disrupt operations at the airport.

**FIGURE 2.** Common Threat Actors

![Common Threat Actors](source: U.S. Department of Homeland Security. Graphic designed by Auditor’s Office staff.)

Threat actors can exploit critical systems and pose risks to the airport’s security and reputation and to the safety of travelers. Critical systems and assets are those that, if compromised or disrupted, would have a debilitating impact on security, public health or safety, or economic security.

**Security Operations Center**

The airport’s Security Operations Center executes the airport’s cybersecurity threat management initiative. The Security Operations Center is a team dedicated to monitoring and responding to cybersecurity threats across the airport. The Security Operations Center’s mission includes using tools and intelligence to identify and respond to threats that target the airport’s passengers, employees, processes, and technology.
This team is responsible for responding to cybersecurity alerts occurring within the airport that may impact airport assets. These assets include:

- Servers and storage devices;
- Employee workstations or mobile devices issued by the airport;
- Network and other infrastructure devices;
- Regulatory data, such as information that identifies a specific person; and
- Remote access services, such as virtual private networks.⑥

The airport’s Security Operations Center identifies, gathers, monitors, and reports cybersecurity-related events or incidents using tools and software to other Business Technologies teams and to airport management. This process of reporting events is better known as “security event management.”

One of the tools the airport’s Security Operations Center leverages in this process is known as a “security information and event management” application, or SIEM. SIEMs provide a central location where data is collected and can be analyzed by airport Security Operations Center personnel to determine if a cybersecurity event has occurred. The airport’s Security Operations Center then determines whether an event is merely a benign occurrence in a system or whether it is a potentially harmful event or threat.

Harmful events in an information system can be things such as unauthorized data removal or the presence of malicious files on a system, more commonly known as malware. Figure 3 on the following page lists common types of malware that have cost companies, governments, and the public millions of dollars.

**Network Operations** – The airport’s network operations team in the Business Technologies department is another important element of threat management. A network operations team—in this case the airport’s Network Operations Center—is a team with the goal of managing, controlling, and monitoring network infrastructure. This includes equipment such as routers, switches, wireless systems, etc. The Network Operations Center also can handle issues such as power outages, network failures, configuration of hardware, and network communication.

When events or incidents occur, the Security Operations Center and Network Operations Center share accountability and varying levels of authority in addressing each incident. The partnership between both groups is important in establishing an understanding of the risks, threats,

⑥ Virtual private networks are private connections to a network that encrypt all data passing through from one point to another.
and security vulnerabilities possible as a result of each incident. Further, this relationship is crucial in kicking off the incident response process effectively.

**Incident Response Process**

The airport’s incident response process involves organizations and personnel highly likely to be at the forefront of a cybersecurity event. The core incident response team includes Business Technologies’ leadership, the Security Operations Center team, Business Technologies information security personnel, and Business Technologies technical staff. Other airport departments may be called upon during an incident response, including:

- Office of Human Resources
- Airport Legal Services
- Finance and Risk Management

**FIGURE 3.** Common Types of Malware

*MyDoom* is considered to be one of the costliest viruses ever causing an estimated $38 billion in total damages. *MyDoom* impacted technology companies as recently as 2004, such as Microsoft and Google, and spammed junk mail to infected computers with text that read “Andy; I’m just doing my job, nothing personal, sorry.”

*Stuxnet* was a computer worm that infected key software in Iran’s nuclear facilities. *Stuxnet* infected computers, such as USB drives, and the worm spread to other computer systems the drives connected to. This outbreak caused the destruction of over 900 uranium enriching centrifuges.

*Storm Worm* was a trojan horse computer virus that infected computers in 2006. Through infected emails titled with intriguing headers, such as “230 dead as storm batters Europe,” people would open emails and click links infecting their computers.

In March 2018, the City of Atlanta, Georgia was hit by a massive ransomware attack. Known as *SamSam Ransomware*, attackers used this malware to infect multiple city computers and databases impacting services and the city airport. The Atlanta Airport, Hartsfield-Jackson, voluntarily took down its wireless internet services as a result to diagnose the problem. Attackers demanded a $51,000 payment via cryptocurrency, which the city did not pay, but the city did pay an estimated $9.5 million in recovery costs.

*Source:* Norton by Symantec, “The Eight Most Famous Computer Viruses of All Time.” Graphic designed by Auditor’s Office staff.
As a part of this process, the incident response team determines whether an event constitutes a potential threat or is merely a benign occurrence. Events considered potential threats are escalated to alerts or incidents.

- **Alerts:** An alert is a formal notification to the Security Operations Center team of one or more potentially adverse events. If an alert is considered severe, alerts are escalated to incidents.

- **Incidents:** An incident is the highest urgency and severity type of event. Incidents are defined as “an adverse event in an information system or network, or the threat of the occurrence of such an event.” Incidents may violate laws or be unacceptable acts that involve data, computers, or networks.7

After an incident is declared, the incident response team will notify appropriate parties in the airport and will determine how to respond. The National Institute of Standards and Technology describes the incident response process in six phases. These phases include preparation, detection and analysis, containment, eradication and recovery, and post-incident activity—or “lessons learned” discussions. Figure 4 describes each of these phases in greater detail.8

---


FINDING
The Airport’s Security Operations Center Needs To Improve Communication and Collaboration with Internal and External Stakeholders

Denver International Airport needs to improve communication and collaboration between its cybersecurity operations and City and airport departments. Specifically, the airport’s Security Operations Center does not effectively communicate and share knowledge with other airport and City information security stakeholders, and the Security Operations Center has not approved and implemented IT security policies to protect airport data. The airport Security Operations Center’s lack of communication and approved policies increases the risk the airport’s digital assets could be stolen and data could be leaked.

In 2014, the airport purchased a “security information and event management” application to begin centralized monitoring of its cybersecurity data. Using this tool, the airport investigated cybersecurity issues in an effort to expand its knowledge and awareness. Following this trend, the airport’s Chief Information Security Officer initiated and designed the airport’s Security Operations Center in August 2016 to detect and monitor threats and vulnerabilities.

However, the Security Operations Center decided to operate independently, and was never fully integrated into the airport’s Business Technologies operations. For example, the Network Operations Center monitors its own set of tools, which collects information that could be valuable to the Security Operations Center team, but does not regularly share this information.

While isolating the Security Operations Center might seem appropriate for security reasons, segregating this group does not promote strong communication practices with the rest of the airport’s Business Technologies groups. Designing the Security Operations Center to remain isolated has resulted in limited collaboration and ineffective policy implementation, impacting the cybersecurity of the airport.

Throughout the audit, we determined there is minimal—and often a lack of—collaboration between the airport’s Security Operations Center and its key stakeholders. When establishing an organizational structure, airport management should consider how its teams interact with one another to fulfill their responsibilities, as well as establish reporting lines so teams can share information necessary for each one to fulfill their
overall responsibilities. If quality information is not distributed and shared with the relevant areas of the airport and the City, there is a likelihood some teams will continue to operate in silos and miss key information useful to not only them, but the airport as a whole.

**Lack of Collaboration with City Agencies** – There is minimal communication and no collaboration on the use of resources between the City’s Security Operations Center and the airport’s Security Operations Center. While there are members of the airport’s Security Operations Center who participate in a monthly citywide Information Governance Committee meeting, there is a limited focus on business processes and tool-sharing. Instead, the purpose of these meetings focuses on high-level leadership items, such as aligning IT infrastructure with business goals.

Additionally, there are no collaborative efforts between the Technology Services agency’s management at the City and the airport’s Business Technologies department. If City and airport departments or agencies with similar objectives—like a Security Operations Center—do not find ways to share their information, there is a high risk duplicative efforts exist, airport revenue is wasted, and cooperation is not maximized.

**Minimal Collaboration with Other Airport Business Units** – The Security Operations Center does not regularly communicate with airport personnel responsible for managing third-party contracts. In addition, we sampled contracts involving third parties critical to the airport’s operations. We found no obligations in the contracts establishing communication between the airport and third parties. This lack of communication limits the airport’s ability to monitor third-party conflicts and reduces the security of the airport’s network.

For example, when a system managed by a third party needs to be updated, the Security Operations Center should work with managers to ensure updates do not jeopardize the Security Operations Center’s ability to protect the network. During the audit, we found one instance when airport vendor managers reached out to the Security Operations Center for assistance in patching a system. However, the Security Operations Center provided the manager only with approval for the patch but did not answer further questions about how to apply the update.

We also found that vendor managers at the airport focus more on financial monitoring and do not have the technical expertise to protect the airport network from third-party managed systems. Third-party

---

managed systems at the airport include important infrastructure, such as baggage belts and the train. We performed a judgmental sample of airport contracts related to airport infrastructure, such as baggage belts, and found no contract language specifying that anyone should perform monitoring over a vendor’s access to information systems. Vendor management is a key aspect of safeguarding the airport’s network but relies on thorough communication between those responsible for the network’s security and the vendor managers.

**Minimal Collaboration with Other Areas under Business Technologies** – Auditors also determined there were issues with collaboration internal to the airport’s teams, which includes areas under the umbrella of Business Technologies. Auditors chose to evaluate the Network Operations Center’s relationship with the Security Operations Center due to the two operations centers’ sharing network security responsibilities.

Though it is part of the Business Technologies department, the Network Operations Center’s staff informed auditors that Security Operations Center personnel do not have formalized communication channels, which has caused issues for the staff in the past. For example, the Security Operations Center does not always inform the Network Operations team when a network scan occurs, which has caused issues in the past. Had the Security Operations Center communicated to the Network Operations Center when these scans were occurring and how they impacted systems, the issues could have been prevented. And while the airport’s Business Technologies department created a scan schedule, the department did not share the availability of this document with all potentially affected parties.

The Security Operations Center also does not collaborate with the Network Operations Center to share tools. For example, the Network Operations Center uses network discovery tools that scan the airport’s network for connected devices but does not share the results of those scans with the Security Operations Center. This lack of collaboration increases the risk that the Security Operations Center is unaware of unauthorized devices or malicious activity on the airport’s network.

**RECOMMENDATION 1.1**

**Share Information** – The airport’s Chief Information Officer should share information, such as successful processes, identified risks, cybersecurity tools, and other data that could be integrated with the City’s or Business Technologies’ cybersecurity operations on a semiannual basis with the City’s information security team.

**Agency Response: Agree, Implementation Date – November 2019**
RECOMMENDATION 1.2

**Improve Communication with Airport Vendor Managers** – The airport’s Chief Information Officer should formalize and document Information Security Team involvement and processes for communicating with airport managers who monitor third-party contracts. This involvement could include:

- Monitoring vendors’ access to the airport’s systems
- Facilitating communication between vendor managers and airport information security teams
- Communication of identified risks and risk remediation activities from vendor managers to airport security teams.

**Agency Response:** Agree, Implementation Date – November 2019

---

RECOMMENDATION 1.3

**Formalize Communication with Business Technologies Teams** – The airport’s Chief Information Officer should formalize cybersecurity operations communication on a weekly basis between managers of the airport’s Business Technologies teams.

**Agency Response:** Agree, Implementation Date – October 2019

---

**The Security Operations Center Uses Unapproved and Ineffective Policies and Procedures**

The airport’s Security Operations Center does not have effective policies and procedures to ensure security and operability of the airport. The Security Operations Center employs contractors who have not signed nondisclosure agreements, it uses policies and procedures that have not been authorized by airport management, and it does not document lessons-learned meetings following an IT cybersecurity incident.

These issues are the result of how the Security Operations Center was created and how processes accompanying the creation of the Security Operations Center were not formalized. The lack of policies and process could jeopardize the security of the airport’s information systems and data and limit the Security Operations Center’s opportunities for improvement.

**Unsigned Policy by Management** – The Security Operations Center follows a policy that has not been authorized by executive management for official use. This policy is for data classification.
and handling, which is essential for the Security Operations Center’s functionality. While this document contains high levels of detail, the lack of signed approval by executive management does not ensure Business Technologies management has authorized and agreed to these procedures.

We also found that the Security Operations Center has several other policies that do appear to have the appropriate signatures for authorization.

The National Institute of Standards and Technology recommends organizations develop, document, and disseminate IT control policies.\(^\text{10}\) Policies provide the overall structure for the specific actions and functions that need to occur. A lack of approved policies and procedures for IT controls does not demonstrate management’s endorsement of planned-upon activities and could jeopardize the security of the airport’s information systems and data.

**Missing Nondisclosure Agreements** – The Security Operations Center was unable to provide evidence a nondisclosure agreement was signed by one contractor who works within the facility. However, auditors did determine the remaining contractors within the Security Operations Center had signed nondisclosure agreements.

The National Institute of Standards and Technology requires governmental organizations to monitor for evidence of unauthorized disclosure of data and to put controls in place to prevent data loss.\(^\text{11}\) While signing a nondisclosure agreement does not prevent an individual from leaking data, it does hold that individual accountable should they do so. Because the airport’s Security Operations Center is composed primarily of contractors, and because they have inside knowledge of the airport’s cyber vulnerabilities, their signing a nondisclosure agreement is essential.

**Lessons-Learned Meetings to Review Incidents Need Improvement** – The airport’s Security Operations Center does not have a formal post-review “lessons learned” process after an incident has occurred.

As shown in Figure 5 on the following page, once the Security Operations Center has resolved a security incident, the case is closed. We found a lack of documented investigatory procedures conducted by the Security Operations Center to improve the incident response


Discussing lessons learned is an important step in the closeout of cybersecurity incidents and should include internal stakeholder discussions to determine how the incident occurred, where it originated from, whether the incident has spread to other devices in the network, and how it could be avoided in the future.

The National Institute of Standards and Technology recommends organizations incorporate lessons-learned meetings from ongoing incident-handling activities into incident response procedures, training, and testing, and that the organization implement the resulting lessons accordingly.\textsuperscript{12}

With limited processes in place to document lessons-learned meetings, the airport is susceptible to the same types of cyberattacks, and the Security Operations Center loses an opportunity to improve its processes to prevent future attacks.

\textbf{RECOMMENDATION 1.4}

\textbf{Sign Nondisclosure Agreements} – The airport’s Chief Information Officer should establish a process to ensure Security Operations Center contractors with access to sensitive data sign a nondisclosure agreement upon hire.

\textbf{Agency Response: Agree, Implementation Date – September 2019}

RECOMMENDATION 1.5

Establish Process to Approve Documents – The airport’s Chief Information Officer should establish a process to ensure all Security Operations Center policies and procedures are approved and updated annually.

Agency Response: Agree, Implementation Date – December 2019

RECOMMENDATION 1.6

Formalize Lessons Learned – The airport’s Chief Information Officer should improve the lessons-learned step in the Security Operations Center incident response process that formally documents how an incident occurred, where it originated from, whether the incident has spread to other devices in the network, and how it could be avoided in the future.

Agency Response: Agree, Implementation Date – October 2019
RECOMMENDATIONS

1.1 **Share Information** – The airport’s Chief Information Officer should share information, such as successful processes, identified risks, cybersecurity tools, and other data that could be integrated with the City’s or Business Technologies’ cybersecurity operations on a semiannual basis with the City’s information security team.

*Agency Response: Agree, Implementation Date – November 2019*

*Agency Narrative: We will work with Technology Services to identify opportunities for information, tool, and process sharing.*

1.2 **Improve Communication with Airport Vendor Managers** – The airport’s Chief Information Officer should formalize and document Information Security Team involvement and processes for communicating with airport managers who monitor third-party contracts. This involvement could include:

- Monitoring vendors’ access to the airport’s systems
- Facilitating communication between vendor managers and airport information security teams
- Communication of identified risks and risk remediation activities from vendor managers to airport security teams.

*Agency Response: Agree, Implementation Date – November 2019*

*Agency Narrative: We will formalize and document the Information Security Team’s involvement and processes for communicating and collaborating with vendor managers.*

1.3 **Formalize Communication with Business Technologies Teams** – The airport’s Chief Information Officer should formalize cybersecurity operations communication on a weekly basis between managers of the airport’s Business Technologies teams.

*Agency Response: Agree, Implementation Date – October 2019*

*Agency Narrative: We will formalize cybersecurity operations communication methods and protocols for Business Technologies teams.*

1.4 **Sign Nondisclosure Agreements** – The airport’s Chief Information Officer should establish a process to ensure Security Operations Center contractors with access to sensitive data sign a nondisclosure agreement upon hire.

*Agency Response: Agree, Implementation Date – September 2019*

*Agency Narrative: The onboarding process documentation for Security Operations team members has been updated and will be followed for all new hires to the team.*
1.5 Establish Process to Approve Documents – The airport’s Chief Information Officer should establish a process to ensure all Security Operations Center policies and procedures are approved and updated annually.

Agency Response: Agree, Implementation Date – December 2019

Agency Narrative: We will implement a process to review, update, communicate, and approve policies and procedures annually.

1.6 Formalize Lessons Learned – The airport’s Chief Information Officer should improve the lessons-learned step in the Security Operations Center incident response process that formally documents how an incident occurred, where it originated from, whether the incident has spread to other devices in the network, and how it could be avoided in the future.

Agency Response: Agree, Implementation Date – October 2019

Agency Narrative: We will review our current lessons-learned step for the Security Operations Center and make improvements as needed to ensure that we document the items listed above.
AGENCY RESPONSE TO AUDIT RECOMMENDATIONS

September 9, 2019

Auditor Timothy M. O’Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O’Brien,

The Office of the Auditor has conducted a performance audit of DEN Cybersecurity Operations.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on August 19, 2019. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
The Airport’s Security Operations Center Needs To Improve Communication and Collaboration with Internal and External Stakeholders

RECOMMENDATION 1.1
Share Information – The airport’s Chief Information Officer should share information, such as successful processes, identified risks, cybersecurity tools, and other data that could be integrated with the City’s or Business Technologies’ cybersecurity operations on a semiannual basis with the City’s information security team.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>November 2019</td>
<td>Tim Coogan (303) 342-4741</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.1
We will work with Technology Services to identify opportunities for information, tool, and process sharing.
RECOMMENDATION 1.2
Improve Communication with Airport Vendor Managers – The airport’s Chief Information Officer should formalize and document Information Security Team involvement and processes for communicating with airport managers who monitor third-party contracts. This involvement could include:
- Monitoring vendor’s access to the airport’s systems
- Facilitating communication between vendor managers and airport Information Security Teams
- Communication of identified risks and risk remediation activities from vendor managers to airport security teams.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>November 2019</td>
<td>Tim Coogan (303) 342-4741</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.2
We will formalize and document the Information Security Team’s involvement and processes for communicating and collaborating with vendor managers.

RECOMMENDATION 1.3
Formalize Communication with Business Technologies Teams – The airport’s Chief Information Officer should formalize cybersecurity operations communication on a weekly basis between managers of the airport’s Business Technologies teams.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>October 2019</td>
<td>Tim Coogan (303) 342-4741</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.3
We will formalize cybersecurity operations communication methods and protocols for Business Technologies teams.
RECOMMENDATION 1.4
Sign Nondisclosure Agreements – The airport’s Chief Information Officer should establish a process to ensure Security Operations Center contractors with access to sensitive data sign a nondisclosure agreement upon hire.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>September 2019</td>
<td>Tim Coogan (303) 342-4741</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.4
The onboarding process documentation for Security Operations team members has been updated and will be followed for all new hires to the team.

RECOMMENDATION 1.5
Establish Process to Approve Documents – The airport’s Chief Information Officer should establish a process to ensure all Security Operations Center policies and procedures are approved and updated annually.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 2019</td>
<td>Tim Coogan (303) 342-4741</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.5
We will implement a process to review, update, communicate, and approve policies and procedures annually.
RECOMMENDATION 1.6
Formalize Lessons Learned – The airport’s Chief Information Officer should improve the lessons-learned step in the Security Operations Center incident response process that formally documents how an incident occurred, where it originated from, whether the incident has spread to other devices in the network, and how it could be avoided in the future.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>October 2019</td>
<td>Tim Coogan (303) 342-4741</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.6
We will review our current lessons-learned step for the Security Operations Center and make improvements as needed to ensure that we document the items listed above.

Please contact Chris Larivee at (303) 342-4933 with any questions.

Sincerely,

Chris Larivee
Sr Director, Acting Chief Information Officer and Senior Vice President, Business Technologies

cc: Valerie Walling, Deputy Auditor, CPA, CMC®
Jared Miller, Audit Supervisor
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Manager
Chris Larivee, Senior Director, Acting Chief Information Officer and Senior Vice President of Business Technologies
OBJECTIVE

The objective of our audit of cybersecurity operations at Denver International Airport was to determine the effectiveness of the airport’s cybersecurity processes, policies, and governance. We assessed how well the airport’s Business Technologies department and cybersecurity operations team were prepared to identify, protect, detect, respond, and recover from cybersecurity incidents.

SCOPE

The audit examined Denver International Airport’s Business Technologies’ cybersecurity operations from January 1, 2018, through July 31, 2019. This included the airport’s network but did not include external networks, such as the Federal Aviation Administration network and third-party vendor networks.

METHODOLOGY

We performed the following steps to achieve the audit objective:

- Interviewing key personnel from the airport’s Business Technologies department
- Interviewing key personnel from the City’s Technology Services agency
- Reviewing Business Technologies’ mission, goals, policies, and procedures
- Reviewing Business Technologies’ incident response procedures and remediation efforts
- Reviewing samples of incidents formally reported to Business Technologies management
The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies and contractors for the purpose of ensuring the proper and efficient use of City resources. He also provides other audit services and information to City Council, the Mayor, and the public to improve all aspects of Denver’s government.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City’s finances and operations, including the reliability of the City’s financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Our Mission

We deliver independent, transparent, and professional oversight in order to safeguard and improve the public’s investment in the City of Denver. Our work is performed on behalf of everyone who cares about the City, including its residents, workers, and decision-makers.