ASSESSMENT REPORT

Denver International Airport

Cybersecurity: Network Operations Center

DECEMBER 2021

TIMOTHY M. O'BRIEN, CPA
DENVER AUDITOR

OFFICE OF THE AUDITOR
AUDIT SERVICES DIVISION, CITY AND COUNTY OF DENVER

Assessment Team

Jared Miller, CISA, CFE, CDPSE, Information Systems Audit Manager
Karin Doughty, CISA, CDPSE, Information Systems Audit Lead

Contractors

CP Cyber
Bill Evert, Partner
Donald McLaughlin, Lead Consultant
Brian Cather, Lead Consultant
Tristan Neate, Associate Consultant

Audit Management

Timothy M. O'Brien, CPA, Auditor
Valerie Walling, CPA, CMC, Deputy Auditor
Dawn Wiseman, CRMA, 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.

Cover illustration by Denver Auditor's Office staff.

City and County of Denver

TIMOTHY M. O'BRIEN, CPA
AUDITOR

201 West Colfax Avenue, #705, Denver, Colorado 80202
(720) 913-5000 | Fax (720) 913-5253 | www.denverauditor.org

AUDITOR'S LETTER

December 16, 2021

On behalf of the Auditor's Office, CP Cyber conducted a cybersecurity assessment of Denver International Airport. This assessment found some areas of strength and some areas that need improvement. Because of the information security sensitivities involved with this assessment, these issues have been communicated separately to the airport for its remediation.

This assessment is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, "General Powers and Duties of Auditor."

We extend our appreciation to the airport personnel who assisted and cooperated with us and CP Cyber during the assessment. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

BACKGROUND

Denver International Airport

Denver International Airport is the third-busiest airport in the United States and the eighth busiest airport in the world. In 2019, 69 million passengers traveled through the airport.[1]

Because of the COVID-19 pandemic, passenger traffic declined in 2020 — to almost 35 million. However, airport officials expect passenger traffic to rebound and reach 100 million passengers sometime between 2030 and 2035.[2]

The airport, which is owned and operated by the City and County of Denver, operates like a business. It generates more than $33 billion for the region annually and employs almost 33,000 people.[3]

Business Technologies Division

The airport continues to address emerging risks involving information security and cybersecurity.

Denver International Airport's Business Technologies division is responsible for managing and safeguarding the airport's network and technology equipment — including data and infrastructure that provides services to airport operations, airlines, other business partners, and passengers.

While many individuals make this technology possible, two teams within the division are instrumental in managing and securing the network: the Network Operations Center and the Security Operations Center.

Network Operations Center

A network operations center acts as the backbone for an organization's network infrastructure. It is often tasked with managing and controlling one or more networks and the technology that resides on those networks. Some of the technology a network operations center may manage include servers, switches, routers, firewalls, databases, and wireless systems.

[1] "About DEN," Denver International Airport webpage, City and County of Denver, accessed Oct. 11, 2021, https://www.flydenver.com/about.
[2] "Message from CEO Phillip A. Washington: Vision 100: Our Journey to 100 Million Passengers," Denver International Airport webpage, City and County of Denver, last updated Sept. 27, 2021, accessed Oct. 11, 2021, https://www.flydenver.com/message_ceo_phillip_washington_vision_100_our_journey_100_million_passengers.
[3] "Vision 100," Denver International Airport webpage, City and County of Denver, accessed Oct. 12, 2021, https://www.flydenver.com/vision100.

Staff in a network operations center receive alerts from a variety of monitoring systems 24 hours a day, seven days a week. By monitoring and responding to these alerts, the network operations center provides continuous monitoring for network-related abnormalities, such as critical events or incidents including:

- Power outages or network failures.
- Configurations to hardware.
- Port management.
- Indicators of compromised network devices.

Similar to a network operations center, a security operations center is "a team organized to detect, analyze, respond to, and report on cybersecurity incidents within an enterprise network."[4] Both the network operations center and the security operations center monitor the security of an organization. As such, if there is an alert or indication of compromise, these two teams collaborate to investigate and respond quickly.

Staff in both the network operations center and the security operations center should have an established understanding of their roles and streamlined communication protocols to efficiently respond to potential cybersecurity and network-related incidents.

Cybersecurity Frameworks

The National Institute of Standards and Technology — a laboratory and nonregulatory federal agency within the U.S. Department of Commerce and a leading organization in developing cybersecurity guidance — provides a framework of standards, controls, and guidance on best practices for managing and securing information systems.[5] The agency notes that organizations must select and implement appropriate security and privacy controls to address their own sets of risks.[6]

As shown in Figure 1 on the next page, this cybersecurity framework defines five categories: identify, protect, detect, respond, and recover.

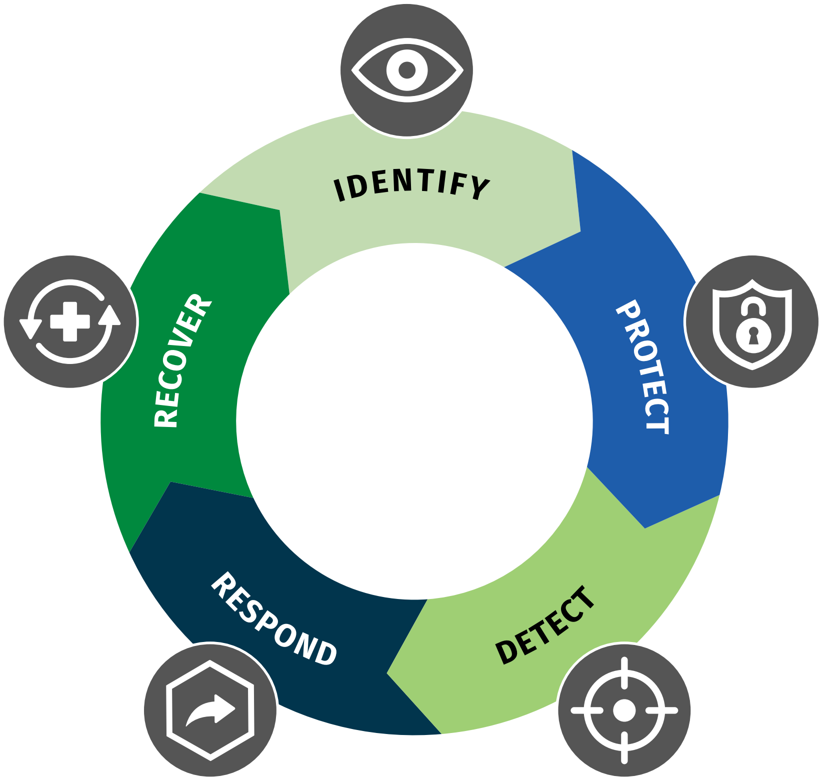
Denver International Airport's Network Operations Center and its Security Operations Center are involved in each of these steps. The airport's cybersecurity program continues to improve with the ongoing development of security controls implemented and maintained by these two teams.

[4] Nelson Hernandez, "NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security," SANS Institute, Feb. 14, 2018, accessed Oct. 12, 2021, https://www.sans.org/white-papers/38290/.

[5] "About NIST," National Institute of Standards and Technology, last updated June 14, 2017, accessed Oct. 13, 2021, https://www.nist.gov/about-nist.

[6] National Institute of Standards and Technology, Special Publication 800-53 (Revision 5), accessed Oct. 13, 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

FIGURE 1. National Institute of Standards and Technology's Cybersecurity Framework



Source: *Graphic design by Auditor's Office staff based on federal framework.*

The National Institute of Standards and Technology recommends key considerations for improving the effectiveness of a network operations center.

The federal agency says managing risk is "a complex, multifaceted undertaking." Therefore, it is critical for a network operations center to:

- Define a security strategy.
- Obtain quality information systems that provide trustworthy, accurate information.
- Adhere to the best practices of asset management.
- Integrate security into its systems.
- Document these efforts.
- Monitor security controls to ensure they operate effectively.[7]

By following the federal guidance, the airport's Network Operations Center will continue to effectively identify risk, protect the organization, detect security events, respond in a timely manner, and recover assets back to operational status when services are disrupted.

[7] National Institute of Standards and Technology, Special Publication 800-53 (Revision 5), accessed Oct. 13, 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Office of the Auditor

The **Auditor** of the City and County of Denver is independently elected by the residents 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 residents' confidence and avoiding any appearance of a conflict of interest.

201 West Colfax Avenue #705

Denver CO, 80202

(720) 913-5000 | Fax (720) 913-5253

www.denverauditor.org

Our Mission

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