PARAS

PROGRAM FOR APPLIED
RESEARCH IN AIRPORT SECURITY

PARAS 0046 March 2024

Security at Tenant and Third-Party Controlled Facilities at Airports

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Roger W. Shoemaker
Anne Marie Pellerin
Rose Marengo
LAM LHA USA LLC
Washington, DC

Jessica Gafford
TransSolutions, LLC
Fort Worth, TX

Donald Zoufal
CrowZnest Consulting, Inc.
Chicago, IL

Richard Duncan
RL Duncan Consulting, LLC
Atlanta, GA

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0046 PROJECT PANEL

Lance Bagnoff *Allegheny County Airport Authority*
Ethan Barske *Portland International Airport*
Frank Capello *Broward County Aviation Department*
Michael DeVault *Burns & McDonnell*
Jeanne Olivier *Port Authority of New York and New Jersey (Retired)*
Gary Smedile *Aviation Security Subject Matter Expert*
Nikola Vucicevic *John F. Kennedy International Airport*
Robert Wheeler *Covenant Security*
Jeremy Worrall *State of Alaska Department of Transportation*

AUTHOR ACKNOWLEDGMENTS

The research conducted for this guidebook was performed by LAM LHA USA LLC with the assistance of TransSolutions, LLC, Crowns Consulting, and RL Duncan Consulting, LLC.

Roger W. Shoemaker with LAM LHA USA LLC was the Principal Investigator for the project. Anne Marie Pellerin and Rose Marengo, also with LAM LHA, and Jessica Gafford from TransSolutions were the primary authors of the guidebook. Donald Zoufal and Richard Duncan assisted with the research, data collection, and editing.

The Research Team would like to acknowledge the airport staff who took time out of their busy schedules to help make this guidebook robust and useful to airports of any size. It is only through the support of airports that Safe Skies is able to continue to provide the aviation industry with valuable research on practical airport-related topics.

Finally, the Research Team would like to thank the panel of volunteers who lent their expertise and time to ensuring the guidebook would be useful and applicable.

CONTENTS

TABLES AND FIGURES

PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ACS	Access Control System
ASP	Airport Security Program
ATSP	Airport Tenant Security Program
CHRC	Fingerprint-Based Criminal History Records Check
CISA	Cybersecurity and Infrastructure Security Agency
CT	Computed Tomography
EAA	Exclusive Area Agreement
EMIS	Electromagnetic Inspection Scanner
ETD	Explosive Trace Detection
FAP	Facility Access Plan
GIS	Geographic Information System
IATA	International Air Transport Association
IP	Internet Protocol
MMW	Millimeter Wave
NSI	National Suspicious Activity Reporting Initiative
PIN	Personal Identification Number
SAR	Suspicious Activity Reporting
STA	Security Threat Assessment
VMS	Video Management System
VSS	Video Surveillance System

SECTION 1: INTRODUCTION

This guidebook continues the concepts explored in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*. PARAS 0025 offered an in-depth description of regulatory frameworks applied in the context of tenant security. This guidebook builds on that information and identifies security solutions with straightforward applications that can improve everyday tenant security operations and processes. It details the range of physical, technological, and procedural solutions available to airports and their tenants to increase security, streamline processes, and respond to some of the challenges they might face.

The guidebook discusses technologies for physical security, access control, and surveillance and inspection, and provides an objective review of the potential advantages and limitations of these technologies. Interviews revealed that while more advanced systems, such as automated access control systems [ACS], biometrics, and explosives detection systems, offer clear security benefits, smaller airports might find it difficult to allocate the necessary funds.

As highlighted throughout the guidebook, procedural changes can also have a major impact on security operations at tenant facilities, especially if they are implemented in combination with an assessment and enforcement process based on routine inspection and audits. Airports that cannot afford some of the more advanced security systems can still benefit from the procedures outlined in the guidebook.

This is especially the case for vulnerability assessments, which have emerged as one of the best ways to respond to a wide range of security issues and concerns. Vulnerability assessments can, for example, be used to identify deficiencies and inefficiencies in security operations, employee training, or facility design; to identify and prioritize security enhancement projects; or to help identify the root cause of recent security trends. The Vulnerability Assessment Guide (Section 3.1) can be used by tenants and airports as a guiding tool when assessing the effectiveness of their security measures

The process of developing this guidebook revealed the necessity for airports to adopt a broader, more encompassing outlook on security at tenant facilities. A comprehensive tenant security approach should integrate physical security measures, technology enhancements, well-trained employees, a high degree of security presence, and a mature set of security policies and practices. The relationship between tenants and airport operators also emerged as an essential component of an effective security implementation. Tenants rely on guidance materials provided by their respective airports, and both parties highly value active and straightforward communication channels.

The guidebook is based on information collected during interviews with a range of airports and tenants based in the United States and Europe. The diversity of examples and case studies illustrates the wide applicability of the guidebook across industry stakeholders.

1.1 Overview of the Guidebook

Section 1: Introduction
This section gives an overview of the guidebook's structure, scope, and the methodology used. It also presents the different types of tenants, and the role and responsibilities associated with each.

Section 2: Tenant Security Measures and Processes
This section describes the physical, technological, and procedural security measures accessible to airports and tenants or third-party controlled facilities. Notable physical security and access control challenges are identified, and potential solutions are discussed. Particular attention is given to new and

emerging technologies. A range of procedural measures are explored, including mechanisms to enhance communication between tenants and airport operators. Tenant engagement and training strategies are also detailed.

Section 3: Assessing and Enforcing Tenant Security Performance
This section investigates assessment and enforcement mechanisms to maximize tenant security performance. In particular, the benefits of vulnerability assessments are highlighted, and a Vulnerability Assessment Guide template is provided in Section 3.1.

1.2 Overview of Tenants

Airport tenants perform a wide range of functions and services. Tenants include:

- Fixed-Based Operators (FBO)
- Corporate-Based Operators
- Aircraft Hangers
- Aircraft Fuel Farms/Fueling Areas
- Deicing Operators
- Remote Bag-Drop Operators
- Private Charter Companies
- Cargo Facilities
- Mailing Facilities
- Tour Operators
- Cruise Ship Operators
- Seaplane Operators
- Aircraft Maintenance Operators
- Airport Maintenance Operators
- Food Service Areas/Catering Operators
- Police Substations
- Aircraft Rescue and Firefighting Facilities
- Military Bases
- Customs and Border Protection Processing Centers

Airports have varying numbers of tenants operating within their AOA and other regulated zones. Depending on the type of operations conducted, tenants will either operate out of facilities directly adjacent to or within the AOA. While most tenants only operate from one specific area of the AOA, some larger tenants operate from two separate areas of the AOA.

SECURITY ROLES AND RESPONSIBILITIES

Project interviews revealed that some larger tenants have their own security personnel or contract security services, but most tenants do not have dedicated security staff. Despite not having dedicated security staff, tenants are responsible for maintaining security in their facilities in the majority of airports.

Tenants that operate independently might have some general corporate security policies, but their security operations are primarily structured around the security requirements put in place by the airport. This is also the case for large tenants that are active in several airports throughout the United States. The security procedures and systems they employ are designed and managed by their central corporate security department but align with the security requirements established by local airport authorities.

1.3 Regulatory and Legislative Frameworks

Airport rules and regulations. Airports have several formal methods for setting security standards and requirements for their tenants. The broadest method is the airport rules and regulations, which set the security standard for all airport users (e.g., workers, passengers). These rules and regulations frequently

reference and incorporate the provisions of federal regulations but include additional airport-specific security requirements.

Airport Security Program (ASP) security requirements (49 CFR § 1542.101 & 103). The ASP describes security requirements for airport tenants, particularly badge holders. Security language in the ASP is often general in nature and references other documents, such as TSA security directives.

To support the overarching ASP, airports may develop a suite of documentation, including SOPs, handbooks, and security standards to outline policies, procedures, operational guidance, and instructions. Airports use these documents to set minimum security standards and tenant responsibilities.

Security of the AOA (49 CFR § 1542.203). This regulation applies to TSA-regulated airports, mandating that the airport operator take measures to prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into or within the AOA.

Exclusive Area Agreements (EAA) (49 CFR § 1542.111). EAAs enable the airport to assign security responsibilities to regulated entities, such as airlines and air cargo carriers, with the entity being provided exclusive use of the area over which they are claiming responsibility. Requirements to enter an EAA must be approved by TSA.

Airport Tenant Security Program (ATSP) (49 CFR § 1542.113). For non-regulated entities, airports can execute an ATSP. An ATSP looks and functions like an EAA but requires much more airport oversight to ensure the non-regulated entity complies with the program.

Local ordinances. Local governments can establish ordinances (laws or decrees) to restrict access, control safety and security, and enable enforcement activities, (e.g., the issuance of citations).

Identification Systems (49 CFR § 1542.211). This regulation outlines the requirements for an identification system for the secured areas of the airport. Identification systems range from simple laminated cards to cards embedded with access control proximity readers, but should all include the features listed in this Part, including the badge holder's full-face image, full name, employer, identification number, scope of access and movement privileges, and expiration date.

More information on regulatory and legislative frameworks is presented in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities.*

SECTION 2: TENANT SECURITY MEASURES AND PROCESSES

Security measures can be generally divided into physical, technological, and procedural measures, though there is much overlap between these categories.

Physical security measures are designed to deter, detect, and delay unauthorized parties from accessing the restricted areas of airports or the tenant or third-party controlled airport facilities (on or off airport property). These structures (buildings, walls, and fences) are intended to be both a perimeter and a physical barrier.

For existing construction, the physical security features of the facility, coupled with the factors of the airport location and layout, will help determine what physical security measures are needed to further enhance the security of the tenant facility. Construction guidance is discussed in Section 2.7.4.

Technological security measures refer to the systems and devices that can be used for monitoring areas and systems of interest, detection of unauthorized activity, and notification to enable response.

Procedural security measures are the policies and programs that encourage personnel compliance with security requirements, including training, engagement, and reporting strategies

2.1 Fencing, Gates, and Access Points

Perimeter fencing provides a visible barrier and can vary in type, design, and function, with gates and access points often incorporated into the fencing. Design features to enhance perimeter fencing include:

- Height
- Barbed/razor wire topping
- Opaqueness
- Cement base
- Buried fabric
- Anti-climb fence fabric
- Intrusion detection system incorporated with the fence

More information on addressing fencing at tenant facilities can be found in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*, Section 5.4.

Clear zones on both sides of the perimeter provide security patrols with an unobstructed view of the perimeter fence, walls, and buildings. They deter individuals from climbing the fence or breaching the perimeter, and eliminate hiding spaces or objects that could help them do so.

More information on clear zones at tenant facilities can be found in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*, Section 5.5.

Gates can be pedestrian or vehicle. They should be the only movable part of the perimeter fence. Operators should reference any industry or construction guidelines for these access points and ensure that the gates can be closed and locked when not in use.

Signage is an important aspect of a perimeter security system and indicates if an area is restricted. While most airports maintain the sole responsibility for signage, tenants work with airport operators to ensure the integrity of the signage. In some cases, tenants may also post their own signage and are then responsible for the signage maintenance.

More information on signage at tenant facilities can be found in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*, Section 5.2.

Access points are outlined in maps that are provided as exhibits within ASPs. Many ASPs also require tenants to:

- Provide detailed maps of their boundaries
- Disclose access points of their facilities
- Identify the location of access points
- Describe the access control measures, i.e., guard posts, security equipment, and technology.

2.2 Environmental Factors

Security lighting provides a level of protection during nighttime hours. If CCTV or an intrusion detection system is in use, adequate lighting is necessary to ensure activity can be monitored. Lighting should provide adequate visibility to the entire perimeter, including fencing, walls, gates, and buildings. It is recommended that any security lighting systems be connected to an emergency power source.

More information on lighting at tenant facilities can be found in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*, Section 5.3.

Natural barriers around the airport's perimeter can enhance the safety and security of the airport by reducing the risks associated with unauthorized access, wildlife, or certain environmental factors. Natural barriers serve as physical obstacles or parts of the airport's perimeter. Examples include bodies of water, wetlands or marshes, dense forests, or mountainous terrain. While unique to each location, understanding the environment will help ensure efficient management of the security needs of the facility.

2.3 Access Control

Detecting and preventing unauthorized access to areas where tenants operate is a vital component of airport security. Larger airports (Category X, Category I, Category II) typically use an automated ACS while smaller airports may rely on simple lock-and-key or physical guards.

Controlling airport vehicle access to restricted/secured area is also a critical component of airport security. Information on vehicle access control can be found in PARAS 0039: *Security, Operations, and Design Considerations for Airside Vehicle Access Gates*.

2.3.1 Automated Access Control Systems

Automated ACSs often comprise a server, a door controller, the airport's identification badge, and a card reader. Different readers and door lock types can be integrated with the card reader to provide additional security, including multifactor authentication.

Airport access control technologies typically perform the following functions:

- Credential authorization, verification, and management
- Physical and virtual access control and monitoring to secure areas and data
- Integration with other ACS and with other key airport processes, such as human resource management, video monitoring, security, and safety

The server has a database of all authorized users and should be able to limit access by area, date, and time. Card readers are linked to the door controllers that process information to the server and communicate control function information to the equipment controlling the door.

When a user places their airport badge on the card reader, information is processed from the door controller about the user. If the door controller receives information from the server that the user is allowed access through the portal, the door controller will unlock or activate the door, allowing the user access. Card readers in tenant areas of the airport may also be equipped with the capability to enter a station-specific or other unique code to access a door.

Ideally, access control technologies should use multifactor authentication to confirm the identity of the individual is the same as the badge. Adding supplementary authentication factors to access the security area reduces the likelihood of a lost or stolen card being used by an unauthorized individual.

Magnetic stripes and proximity cards: These card types are very easily copied and no longer considered secure. These cards and readers should be replaced as quickly as practicable.

Smart cards and readers: The currently accepted standards for smart cards and readers are desfire-EV2 and HID SEOS. Recent innovations within the area of access control credential technology include the development of more advanced contactless smart cards and readers. These cards are programmed to allow access through designated doors and are given a unique identifier for auditing purposes. The first generation of readers and cards originally used an encryption that was compromised and is now considered a non-secure media. More recent generations have moved to a more advanced encryption, which has gone through an evolution since the original smart card introduction. On their own, these offer single-factor authentication, but they are typically paired with a second credential, such as a personal identification number (PIN) or biometric scan.

Bluetooth-enabled readers: Many ACS manufacturers have a smartphone application that allows the user's phone to be used as a secondary credential at an enabled reader. The user swipes or taps their airport-issued badge, and the system pushes a secondary credential to the phone associated with the badge. The user can then enter the credential into the system for access. This process provides two-factor authentication.

Biometrics: Many airports are transitioning to include biometrics to support multifactor authentication for access control. Fingerprint is the most common format, but some airports use iris patterns or facial recognition. The latter two formats reduce touchpoints, which has been a priority for many airports since the COVID-19 pandemic. The biometric data is collected during the badging application process. Deploying biometric readers at tenant facilities will likely require an agreement with the tenant; however, mobile biometric readers can be used to perform random checks of airport worker identities in secure areas.

More information on biometrics can be found in PARAS 0045: *Guidance for Biometric Technology at Airports*.

Access door hardware: One trend in secure access doors has been the use of electrified hardware, including electrified mortise locks and electrified panic hardware. A benefit of this technology is that the status of the door lock can be monitored by the ACS and is seamless to system users. Another trend is the use of all-in-one type door locking technology. These locks are available with internal card readers and PIN pads and enable monitoring of the lock status. However, a potential drawback of these all-in-one locks is that it may be necessary to replace all door hardware when card reader technology needs to be upgraded.

2.3.2 Locks and Keys

Tenants in older facilities may rely on other locking solutions to secure pedestrian gates, vehicle gates, and other access control points. Examples of various lock types that may be in use include:

- **Key locks (lock-and-key padlock)** are inexpensive and commonly used for pedestrian gates, vehicle gates, and other access points.
- **Cipher locks** are push-button combination type locks that may be used to secure pedestrian doors or gates.
- **Combination locks**, while much less common, can be used to secure limited areas of a tenant or third-party controlled facility.

Airports often use a combination of the options listed above. An automated ACS may be used at common-use gates or gates with high traffic volume, while remote or emergency gates are secured with a lock-and-key system. One Category I airport reported having 80% of its facilities under an automated ACS and 20% lock-and-key controlled facilities.

Key control is one of the single most important factors for a lock-and-key system because there is no automated method to track key assignments. Airport operators can require or recommend that tenants use a key log to help with inventory control. The person in charge of key control will keep a log of everyone who maintains a key and which lock(s) the key opens. Regular audits of the keys and locks help to ensure all keys are accounted for. When there is a loss of key control, the keys and locks should be replaced or rekeyed.

Other considerations for effective key controls include:

- Keys issuance is limited to personnel based on operational needs
- Lock codes/combinations are changed regularly
- Lost keys are promptly reported and acted on to safeguard the system

Advanced key technologies, depending on the system, provide airport or tenant management with the ability to: (1) record a user's use of the key, (2) immediately disable a lost or stolen key from the system, and (3) limit a key to a specific door or lock.

2.3.3 System Ownership

Some airports own the ACS used in tenant facilities. In these circumstances, the airport is responsible for governance of the system and authorizing access through the portals.

Tenants may prefer to maintain exclusive access control for their critical facilities and deploy their own ACS with permission from the airport. This could be beneficial to the airport to reduce capital and operational expenditures, as the tenant takes on the responsibility of managing access and maintaining the system. A tenant-owned ACS does not exempt the tenant employees from complying with the airport's rules.

Tenant facilities that are partially or completely within the AOA must meet the access control standards specified in 49 CFR § 1542.203 and further described in 49 CFR § 1542.207. That is, "prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into or within the AOA." Tenants deploying an ACS in the AOA must meet the same standards and are subject to airport oversight. Similarly, tenant facilities that are partially or completely within the Secured Area must meet the access control standards set forth in 49 CFR § 1542.201. Due to the higher level of

security required, access to Secured Areas requires a personnel identification system (49 CFR § 1542.211) and vetting of individuals before authorizing unescorted access.

Below is sample language from a participating airport's alternate security measures agreement that discusses the tenant's use of their own ACS. The agreement requires the tenant to issue unique access cards to individuals and deactivate the card when the individual leaves the company.

> [Tenant] will maintain access control cards in a secured location. All access cards will have a unique alpha or numeric designator, and one card can be issued to only one individual at a time. When an individual no longer needs access to this area, their card will be immediately deactivated.

In agreements between tenants and airport operators permitting the tenant's ACS, airports should consider how they will gain access to the tenant's ACS records when needed. If a security incident occurs in the tenant's facility, the airport will need access to the ACS logs to investigate the incident and determine when doors were accessed and by whom.

Generally, tenants are amenable to requests for archived data reports, especially concerning a security incident. Tenants may be open to allowing access to the system databases. These factors and considerations should be discussed and outlined in the ACS agreement between the airport and tenant.

One Category X airport operates a centralized ACS that covers all access to regulated areas of the airport. All employees accessing those areas need to be enrolled in the airport's access control program, which is done in connection with the issuance of ID media. The ACS includes fingerprint-based biometric, two-factor access controls at most access points, which requires the presentation of ID media along with a fingerprint read. The centralized ACS is monitored 24/7 at the airport's operations center. The operations center is alerted when doors are forced opened, and the operations center can dispatch security personnel to tenant areas to address alarms or concerns over access control. The centralized systems also allow for auditing of tenant access control use and practices.

More detailed information about ACS can be found in PARAS 0017: *Access Control Card Technology Guidance*, PARAS 0020: *Strategies for Effective Airport Identification Media Accountability and Control*, PARAS 0028: *Recommended Security Guidelines for Airport Planning, Design, and Construction*, PARAS 0030: *Guidance for Access Control System Transitions*, and RTCA DO-230J: *Standards for Airport Security ACS*.

2.3.4 Dual Access Control Systems

Most tenants operate their own ACS within their tenant facilities. This often requires the tenant employees to possess dual access control media authorized by the airport and the tenant company, each granting limited access to the ACS (airport- and tenant-operated, respectively). The tenant will need to receive approval to use the airport's ACS from the airport operator and TSA to ensure the system will meet the security standards of the airport.

Once the agreement is in place and the system is deployed, the tenant will be responsible for maintaining and repairing the system if it is inoperable. The tenant will also be responsible for any security violations incurred as a result of a malfunctioning door if this is included in the agreement between the airport operator and the tenant. The existence of dual ACSs can often cause operational and security challenges for tenants and airport operators.

At a large Category X airport, a door within a tenant facility employee break room accesses the hangar area, which opens onto the AOA. Due to this AOA access, the door leading into the break room is equipped with an airport badge reader, which requires everyone entering the break room to have AOA access privileges. Other non-AOA access portals in the facility (like those leading to executive offices) are controlled by tenant access control readers and a separate tenant badge.

It was determined that the AOA access control reader would be better located at the doorway that leads directly from the break room to the AOA hangar. This will enable the break room door to be controlled by the tenant ACS, and AOA badges to be limited to only those employees who actually need to access the AOA. The tenant is in the process of coordinating a move of the access control readers.

While the tenant and airport operations closely coordinated on the development of the facility, the issue of the break room raises some of the difficulties that can occur by having two ACSs, in particular:

- Limited ability of the tenant to fully control access to their facility or even have visibility over who is accessing their facility, which remains a continuing matter of discussion between the tenant and the airport operator
- Inconvenience of requiring the tenant employees to possess and utilize two access control badges within their facility

2.4 Video Surveillance Systems

Video surveillance systems (VSS) are a critical component of an airport's security posture. These systems consist of surveillance cameras and may include a video management system (VMS) and video analytics. Depending on the system's components, a VSS may perform the following functions:

- Real-time visual monitoring of airport facilities and assets
- Analysis of data collected by the surveillance system
- Archiving and indexing of data collected by the surveillance system
- Integrating with airport security systems, such as the ACS

Some airports choose to use cameras in or covering tenant facilities to view activity, support alarm response, and review activity/alarm events.

There are many different types of surveillance cameras, The most common type used in airports is fixed cameras, but pan-tilt-zoom, panoramic, multi-imager, infrared (IR), and thermal cameras are also used in airports. PARAS 0034: *Optimization of Airport Security Camera Systems* outlines each camera type's advantages, disadvantages, and specific uses.

The selection of camera types should be based on the airport and tenant's surveillance goals and available mounting locations. Mounting location and the camera's field of view should be carefully considered to ensure the camera captures footage of vital areas to ensure facility security, employee safety, and compliance with airport rules and requirements. Important locations and fields of view in a tenant's facility include:

- Entrances
- Exits
- Secured access portals (vehicle and pedestrians)
- Inspection areas
- Perimeter fencing and gates

- Pointed at face level
- Pointed at license plates

Lighting is especially important for most surveillance cameras. The areas being monitored should be well lit to improve the quality of footage.

2.4.1 Video Management Systems

A VMS provides a single interface for airports to manage and review video from all surveillance cameras connected to the system. Many airports have acquired a variety of camera types from various manufacturers. The system allows the airport to connect the footage from all cameras to improve monitoring capabilities.

These systems are especially useful when paired with video analytics to automatically notify the user monitoring the system of unusual activities. Similarly, integration with the ACS can enable the VMS to call up footage of ACS alert and alarm locations. These types of integrations allow for faster alarm resolution and response times.

2.4.2 Video Analytics

Video analytic software can analyze live streams or recorded imagery to identify events, patterns, suspicious objects, or trends that are relevant to airport security. Advanced analytics are capable of detecting specific movements (e.g., in the wrong direction), left objects, and other undesirable behaviors. Leveraging this technology in tenant facilities can help airports identify behaviors such as tailgating and equipment tampering.

One of the primary safety and security challenges confronted by a Category II airport was ensuring security compliance at unstaffed access gates. With over 800 persons afforded access to the AOA, securing those access points against piggybacking and tailgating presented constant issues for the airport operator. The airport could not gain compliance despite having clearly established rules prohibiting piggybacking and tailgating and clear signage posted at the access gates to warn against that behavior.

Gate procedures require the driver of a vehicle to ensure the gate is secured behind them when entering or departing, and to not allow other vehicles to pass through the gate before it had closed. Recorded instances of vehicles intentionally and unintentionally entering the AOA through gates that were not properly secured were concerning.

To address the issue, the airport operator implemented a technology-based solution that involved the application of video analytic software to assess access control transactions at the gate to determine compliance with the access control procedures. The airport does not have a dedicated 24/7 operations center for monitoring its VSS and ACS. When the system detects a violation, a video record is created, and airport personnel can follow up with appropriate security measures.

2.4.3 System Ownership

Airports with a surveillance system in and/or covering tenant facilities can use the footage for auditing and compliance purposes. In this situation, the system is typically tied into the airport's centralized camera system, which allows for real-time monitoring from the operations or security center. Archived footage can be used for forensic analysis to determine who was involved in an incident and the sequence of events.

Tenants often want more control over the security of their facilities and deploy their own CCTV systems, even if the airport already has surveillance cameras installed. In many cases, airports choose not to install cameras in tenant facilities and rely on agreements with the tenant to access footage for auditing and compliance purposes. This is not a common practice, but it lowers the airport's equipment costs and improves the airport's awareness of activity in the tenant facilities. It is uncommon for tenants to provide real-time access, but access to the archive footage is often granted to the airport operator upon request. Many airports have no restrictions on their tenant's security projects and allow tenants to place cameras in their facilities without requiring more than a construction permit. An extract from an airport's CCTV Security Surveillance System Policies and Guidelines is included in Appendix A.

Often, airports outline requirements for surveillance cameras in the tenant or lease agreement or in Memorandums of Understanding (MOU) executed with the tenants. These agreements also outline the process for the airport to request or access the surveillance footage. Below is sample language from an MOU with a tenant allowing airport access to the footage.

> [Airport] Access to Tenant Cameras – Security and Emergency Situations: In the event of a security incident, emergency incident or situation, law enforcement investigation, or other official airport investigation or initiative, including without limitation access to footage in response to allegation of personal injury or property damage, Tenant agrees to allow [the Airport] to review and be entitled to a copy of any surveillance footage upon request for the reasons listed above, and Tenant will provide the access and copy without delay and as soon as reasonably possible.

The MOU also outlines provisions for moving, adding, or removing cameras after execution of the agreement.

> Physical Camera Provisions: Tenant surveillance cameras should only be used in locations mutually agreed upon by the Parties. Cameras should be mounted/housed in/on objects that are clearly marked as being surveillance cameras and supporting equipment. Items that could be mistaken as unattended luggage or other suspicious items may be confiscated by [Airport] Security and/or Law Enforcement. If Tenant plans to permanently remove or add a camera location after execution of this MOU, Tenant shall submit a [change form] to the Airport for review and approval before the Tenant makes any changes to its surveillance system.

One FBO maintains CCTV camera coverage inside their facility and of adjacent areas on the ramp. The tenant uses a VMS that is separate from the airport throughout its facilities. The CCTV and ACS deployed by the tenant are only accessible to tenant employees at the site and to other tenant personnel at a central monitoring facility or other locations designated by the tenant. The systems are operated and maintained by the tenant principally through their corporate security department. Airport operations personnel do not have access to the systems maintained by this tenant.

Another FBO maintains a camera system and is in the process of upgrading it to include the ability to share camera images with their corporate headquarters. The tenant's cameras are only accessible to tenant employees, and there is no plan to share real-time camera images with the airport. The airport operator does, however, maintain cameras that cover access gates and ramp areas in the tenant areas, but not in the tenant facilities.

A Category X airport operator has a centralized ACS for AOA access gates and a centralized CCTV system. These CCTV cameras are placed at gates and access portals as well as ramp areas and other common-use areas. Only the airport operator has real-time access to these cameras, but tenants are afforded the ability to review recorded video with security relevance to their operations. Tenants currently must make written requests to the airport to receive access and are given the relevant video on DVDs, but the airport operator is developing a portal that will enable tenant access to video through a digitized request process. Currently, the airport operator receives an average of 50 requests per month from tenants. The new portal is expected to expedite the overall process.

More information on surveillance cameras can be found in PARAS 0028: *Recommended Security Guidelines for Airport Planning, Design, and Construction* and PARAS 0034: *Optimization of Airport Security Camera Systems*.

2.4.4 Other VSS Enhancements

Apart from video analytics, there have been several other developments in surveillance technologies in recent years that may benefit tenant security operations:

EDGE COMPUTING

Until recently, airport surveillance technology relied on centralized, on-premises servers to store archived data and perform computing functions, such as generating alerts or delivering images to users. In the last several years, surveillance technology manufacturers have shifted to the use of edge computing, which refers to applications or functions that run within a device rather than at a central server. In the case of airport surveillance technology, this means that analysis of surveillance data occurs at the point of recording, within the surveillance device or camera itself, instead of sending video or other data to a main server for analysis. This computing approach offers potential benefits compared to the use of centralized servers, including:

- **Reduced latency:** Latency is the delay incurred when data is transferred over a network. If a surveillance device or camera must transfer or stream all its data to a central server, there can be delays caused by the large data file sizes. This may delay airport security personnel response to an event recorded by the surveillance device. By contrast, if a surveillance device has edge computing capabilities, it can send a security team smaller amounts of data that contain only the relevant information. In theory, this means that security teams can receive only the information they need with fewer delays.
- **Reduced data networking and storage costs:** By analyzing data at the point of surveillance and then only sending the relevant data to be stored and acted upon to a central location, edge computing has the potential to reduce bandwidth and data storage costs associated with airport surveillance activities.

IP-BASED SURVEILLANCE CCTV CAMERAS

Airports with dated surveillance systems rely on analog CCTV cameras that transmit a raw video signal over a coaxial cable. Integrating analog devices with newer surveillance analytics, edge computing technologies, or other elements of an airport's IT infrastructure that have been designed for IP (internet protocol) networking is possible. However, this can require additional time and cost for airports. As a result, one trend in airport surveillance technology has been the acceptance and implementation of IP-based cameras, which transmit all data digitally and support standardized interfaces for interoperability of IP-based surveillance devices.

2.5 Cybersecurity

Cybersecurity attacks, data breaches, ransomware attacks, and malware infections are increasingly prevalent in the aviation sector. Because most aviation systems rely on computer systems, digital technologies, and associated networks, cybersecurity is an essential component of aviation security. Airports, air carriers, cargo operators, and tenants must safeguard their systems from cyberthreats to maintain the integrity and safety of aviation operations. Tenants and third-party facilities should focus on how interruptions resulting from a cybersecurity attack might impact overall operations, safety, and security.

Tenants should also closely monitor and link with regulatory bodies and organizations on the latest rules, regulations, and best practices for cybersecurity. Aviation regulatory organizations have enacted rules, regulations, security program changes, and recommendations to strengthen cybersecurity measures. For instance, FAA, TSA, the International Civil Aviation Organization, the Cybersecurity and Infrastructure Security Agency (CISA), and Aviation ISAC have established cybersecurity best practices and guidelines for the aviation sector.

To reduce risks and successfully address possible cybersecurity incidents, tenants should 1) conduct thorough risk assessments, 2) enact security measures, 3) routinely check systems for vulnerabilities, and 4) create incident response plans. This cycle should be repeated regularly and conducted in collaboration with other tenants, air carriers, and airport operators. With multiple stakeholders cooperating and sharing information, best practices, and threat intelligence, there will be a more thorough understanding of the current risks associated with cybersecurity as well as a collaborative effort in countering these threats.

Many aviation systems have a number of entry points to information technology systems that hackers could use to their advantage. Inadequate security measures, outdated software, unsafe communication protocols, and flaws in the network infrastructure are a few examples. As cyber threats rapidly evolve, tenants must continuously monitor systems and networks for potential vulnerabilities. Regular software and firmware updates are important in addressing known security issues and for tenants to stay protected against emerging threats. Limiting access to servers and IT systems is also an important step in cybersecurity controls.

Training is an essential part of a tenant's role in countering cybersecurity threats and responding to incidents. All personnel involved in the tenant's operations need to be trained to recognize and respond to potential cyber threats.

By prioritizing cybersecurity in aviation security, tenants can mitigate risks, protect critical systems, and ensure the continuity of operations.

An example of an airport's cybersecurity policy requirements for tenants is included in Appendix B.

2.6 Screening Technologies

Airport physical security technologies refer to hardware, software, and other systems that airports deploy to protect their people, property, and physical assets from physical threats, actions, and events, such as theft, vandalism, and terrorism. Security inspection technologies are used to detect and identify concealed threats, such as stolen goods, contraband, narcotics, weapons, or explosives.

Airport inspection technologies cover a broad range of scenarios. In this section, we focus on three airport-specific use cases:[1]

- **People screening and inspection:** Technologies used to screen airport employees and contractors for contraband, concealed threats, or prohibited items on their person or concealed underneath their clothing.
- **Accessible property screening and inspection:** Technologies used to detect and identify potential threats in purses, backpacks, tool kits, briefcases, and other common carry-on items used by employees and other persons accessing the airport.
- **Vehicle-related security.** Technologies used to deter or prevent vehicle-based attacks on airport infrastructure. This includes technologies used to detect and identify threats concealed in cars and trucks.

Airport inspection technologies can be deployed at airports and tenant facilities in different concepts of operations:

- **Security checkpoint or portal:** In this scenario, airport employees are stopped and inspected, and detected alarms are resolved before the employee is allowed to enter a secure area.
- **Passive monitoring:** This applies to deployment of technologies for environmental threat detection. In this case, the technology detects threats or indications of threats in a particular area of the airport.
- **Dedicated/centralized inspection facility:** This approach is often used for screening airport mail or incoming packages.

A variety of physical security and inspection technologies are already used across different tenant security applications and use cases. These technologies are particularly relevant to airport tenant security as they can be used to deter and detect security-related risks from employees and contractors working for airport tenants.

More information on inspection technologies can be found in PARAS 0019: *Employee/Vendor Physical Inspection Program Guidance*.[2]

2.6.1 People-Screening Technologies

WALK-THROUGH AND HANDHELD METAL DETECTORS

These devices are widely used for people-screening applications, such as employee screening. Metal detectors are effective at detecting the presence and location of even small quantities of metal.

A limitation of metal detectors is their inability to detect non-metallic threats or other prohibited items. A second limitation is their inability to identify the specific metallic object detected or distinguish between threat and non-threat items. This can lead to false alarms or create the need for people to first divest themselves of all metallic items, such as keys, coins, and mobile phones, which adds delays and costs to the security screening process.

[1] Given the scope of this report, the technologies used by TSA for airport passenger screening at TSA checkpoints are not addressed.
[2] PARAS 0060: *Strategies for Developing an Aviation Worker Screening Program*, to be published in mid-2024, will also cover this topic.

To achieve random inspection schedules, airports often mobilize the inspection process and move between access portals without permanent inspection technology. Some walk-through metal detectors are mobile, allowing for setup anywhere with an electrical outlet. Many airports have reported success using these devices. Handheld metal detectors are useful for access points without electric outlets or as a low-cost alternative to walk-through devices.

OTHER PEOPLE-SCREENING TECHNOLOGIES

Other types of people-screening systems use passive millimeter wave and terahertz sensors, among other detection types, to identify if a person has objects concealed under their clothing. These systems can usually detect both non-metallic and metallic items, sometimes at a distance and as a person is moving, which makes them useful in employee screening.

Many of these systems alert on all detected items, and do not produce images that would enable security personnel to identify a concealed object. This means that people being screened may need to divest of all items to avoid false alarms, and that any detected item must be divested to determine whether it is a threat.

One large Category X airport has a vigorous program of physical inspection of aviation workers and air carrier employees in restricted areas. The airport also conducts 100% inspection of all vendors, contractors, and delivery workers. These search/inspection practices are recorded in the Terms and Conditions for the issuance of Airport ID badges and permits. All employees of companies that are permit holders are required to execute consent-to-search documents before they are issued ID media for AOA and SIDA access.

2.6.2 Property-, Goods-, and Vehicle-Screening Technologies

EXPLOSIVE TRACE DETECTION (ETD) SYSTEMS

ETD systems are used to detect explosive residue on the surface of items or on a person. ETDs can be used for a wide range of security applications and use cases, and they can detect and identify specific explosive threats in minute quantities (parts per billion).

A limitation of ETDs is that they are only useful for detection of explosives. In addition, ETDs can be highly sensitive to environmental conditions, and their performance can be negatively affected by the presence of dust and other contaminants.

There is a TSA National Amendment that will require airports to perform ETD inspections. Airports will need to ensure their inspection process will be capable of meeting this requirement.

Many tenants along the perimeter are charged with inspecting goods and vendor trucks before being permitted to enter restricted areas. ETD and image scanning are the two primary technologies used to inspect goods. ETD is limited to a small sample size, which can be a significant disadvantage for large shipments.

TWO-DIMENSIONAL (2D) X-RAY SCANNERS

These devices are widely used in a variety of airport security applications. They can detect and identify objects in packages, mail, cargo, accessible property, and vehicles, and can be deployed in a variety of configurations, such as with a conveyor belt, in a portal, or in an under-vehicle inspection system. They can generate high-resolution images of objects such as guns, bottles, knives, and other prohibited items, and they can distinguish between metallic and non-metallic items.

2D x-ray scanners have drawbacks. Their capability to find threats in cluttered bags is limited because they can only produce 2D images and cannot identify the material composition of items they detect, which can lead to false alarms. Without well-trained operators, their effectiveness can be significantly reduced.

Commercial, off-the-shelf artificial intelligence (AI) solutions can be integrated with 2D x-ray systems to automatically identify prohibited items, weapons, and other threats in x-ray images. In some cases, the AI software is fully integrated into the x-ray system; in other cases, an external computing unit is attached to x-ray scanner so that it can process the video output of the scanner. It is important to note that these solutions are not intended to replace security operators but rather to assist them and reduce the risk of human error.

COMPUTED TOMOGRAPHY (CT) DEVICES

CT systems provide three-dimensional images of goods or property as well as explosives detection capabilities. However, the devices are much more costly than x-ray machines.

ELECTROMAGNETIC INSPECTION SCANNERS (EMIS)

This technology can be used to quickly detect metallic objects in non-metallic shipments ranging in size from single packages up to palletized cargo. EMIS may have applications for screening product like food or textiles in centralized distribution centers or flight kitchens. While these systems can detect the presence of metallic items like detonators or metal parts for explosive devices, they have no imaging capabilities. This means a further inspection using additional technology or a physical examination of contents would be required to identify the exact location and type and of any detected items.

2.7 Procedural Security Measures

Effective communication and reporting programs can be used to provide structured messaging and deliver clear and concise security information to airport tenants. These programs play a key role in strengthening security around the airport and limiting potential threats. In addition, training and education for tenants are the core of a robust and sustainable security posture at airports. Airport tenants who are more prepared, confident, and competent in their security roles will feel empowered to perform their security responsibilities, such as challenging missing badges, stopping piggybacking, and reporting security concerns.

2.7.1 Airport-to-Tenant Notification Practices

Several notification practices can be used to help ensure that airport tenants receive current, actionable information:

Airport newsletters are commonly used to inform airport stakeholders (typically airport workers) of relevant airport news and non-sensitive security information, such as new inspection procedures or relevant badging changes.

Blogs and articles written by security subject matter experts in airport newsletters or posted on the airport's public-facing website provide an opportunity to discuss a topic in detail. Note that longer articles are less likely to be read than shorter ones.

Emergency notification systems can be used to send mass emails and text messages during security incidents and emergencies. This is especially useful for tenants with facilities away from the terminal, which may not receive notifications otherwise. Many emergency notification systems utilize a geographic information system (GIS) to create a virtual geographical boundary (geofence) around the

airport. During an emergency, the airport can send targeted alerts and notifications to any active mobile device within the geofence, which would allow the airport to reach tenants outside of the terminal and along the perimeter of the airport property. Many airports are already using GIS for their emergency notifications. More information on GIS can be found in ACRP Report 88: *Guidebook on Integrating GIS in Emergency Management at Airports*.

Before implementing an emergency notification system, airports should make sure to work with their legal department to develop a consent form permitting use of personal contact information. This form can be included in the badge application process.

Regular tenant meetings are held by many airports to update tenants on relevant airport information. The frequency of the meeting greatly depends on the airport's specific needs but can range from daily stand-up meetings to quarterly meetings with executive stakeholders. It is common to include security on the meeting agendas to inform the attendants of security concerns. It is also common to hold tenant security meetings that are separate from operational meetings and only focus on security topics.

The meetings should not focus on a specific tenant but should discuss general concepts. For example, ongoing trends in specific security violations (e.g., door propping), or how new requirements will affect the tenants' operations (e.g., vendor inspections).

Informal visits are another popular information-sharing mechanism. Rising trends in security violations may prompt a visit to the frontline tenant workers to help determine the root cause or to offer reminders of security responsibilities. These informal visits should be casual in tone and should focus on building relationships, not punitive measures. The airport may choose to quiz the workers to test their knowledge of security and determine if there are gaps in training that need to be addressed.

Airports can require tenants to designate a point of contact within their organization to be responsible for disseminating information shared by the airport to their tenant employees.

More information on airport-to-tenant information-sharing practices can be found in ACRP Report 170: *Guidebook for Preparing Public Notification Programs at Airports*, PARAS 0003: *Enhancing Communication & Collaboration Among Airport Stakeholders*, PARAS 0008: *Findings and Practices in Sharing Sensitive Information*, and PARAS 0044: *Strategies for Aviation Security Stakeholder Information-Sharing*.

2.7.2 Tenant-to-Airport Reporting Practices

Reporting mechanisms allow airport tenants to notify the airport of security concerns, open more communication channels, and engage in the airport security posture. Tenants can alert the airport to open vehicle gates, individuals lingering near secure areas, and other security concerns.

Operations centers: Sometimes referred to as security centers or communications centers, operations centers are a centralized and often shared space for airport stakeholders to improve communications and situational awareness, expedite response times during security incidents, and promote unity of mission in general.

Additional information on security operations center can also be found in PARAS 0043, *Security Operations Center: Planning and Design.*

Contact information and reporting channel: A significant barrier for stakeholders to report information is not having or not knowing the proper reporting channels. Relevant contact information should be posted in easy-to-reference locations, such as gathering spaces, the airport website, the

employee portal, and airport mobile applications. Simple reporting processes will enhance the airport reporting program. Additionally, providing methods to anonymously report security concerns will encourage tenant workers to report without fear of repercussions. Actionable reports are critical to help law enforcement and airport security investigate security concerns. Initial and recurring security training should include information on how to provide an actionable report. Campaign materials should also include reminders for reporters to include the "5 Ws" when reporting: who, what, when , where, and why, as shown in Figure 1.

Figure 1. The 5 Ws: What to Include in Your Report

Source: DHS How to Report Suspicious Activity

International Air Transport Association (IATA) has created the Security Management System, which provides a framework for a risk-based and data-driven approach to aviation security. The approach emphasizes the importance of reporting incidents and suspicious activity. IATA's security report form is a good starting point for airports looking to develop their own reporting template for employees.[3]

Informal discussions: Many airport security directors and airport police stop to have informal chats with the frontline tenant workers while they patrol the terminal. They use the opportunity to introduce themselves to the tenant workers and create a more familiar relationship with the airport community. These informal discussions provide an opportunity to remind the frontline tenant workers of their reporting responsibilities and the reporting mechanisms available to them. It is also an opportunity to learn about unreported activities that the tenant worker may not have felt comfortable reporting through formal channels.

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI): The NSI is a standardized process for gathering, documenting, processing, analyzing, and sharing SAR information. The DHS's "If You See Something, Say Something®" campaign that is often seen at airports and other transportation modes is part of the NSI.

Airports can build on the DHS efforts, established SAR infrastructure, and supporting promotional campaign materials to promote such programs to their tenant and aviation workers. Several airports reported promoting similar employee and public awareness campaigns.

2.7.3 Addressing Insider Threat

Insider threat continues to be a concern at airports and tenant and third-party controlled facilities. Airports and tenants work together to mitigate the threat of individuals within an organization who may abuse their access, privileges, or knowledge of the security system.

Managing insider threats is an ongoing challenge due to the high level of trust insiders are afforded. This makes harmful acts more difficult to detect, posing threats to the confidentiality, integrity, and

[3] **IATA Security Report Form:** https://www.iata.org/contentassets/3149bcf1b23b4bc0834dbef1ff9ea5a1/iata-security-report-form.pdf

availability of the organization's data, systems, or assets. Insiders' familiarity with the organization's security measures makes it easier for them to exploit flaws or loopholes. Because insiders have valid motives for accessing specific information or systems, it is challenging to differentiate between normal activity and malicious intent.

Airports and tenants should work together to develop SAR systems so that employees know they can report activity without the fear of reprisal and that their concerns will be acted upon. Some airports have also instituted physical inspections and random testing. As previously discussed, CCTV can provide an airport or tenant with the understanding of normal movements and activities at an airport or tenant facility and identify suspicious activity.

At one large Category X airport, the airport operators focus a significant amount of attention and resources on mitigating the threat from insiders. Direct measures to mitigate insider threats are reflected in the physical inspection programs that exceed current TSA requirements. These measures include employee screening checkpoints and inspections at access control points.

The airport operator also has its own Insider Threat Task Force, which includes participation from the airport's security department, DHS Homeland Security Investigations, the FBI, and airline security personnel.

More information on insider threat can be found in PARAS 0026: *Insider Threat Mitigation at Airports*.

2.7.4 Construction Guidance

Constructing and refurbishing buildings, cargo facilities, and tenant buildings is becoming increasingly common due to the evolving needs for tenant facilities. Airports should consider providing guidance to tenants to address security, both for the construction activities and for the completed facility.

Construction guidance documents can help ensure that adequate security measures are put in place during construction so that security gaps do not develop. These may include erecting temporary fencing or barriers, adjusting access control permissions or moving readers, reorienting existing CCTV cameras or installing new temporary cameras, and preparing administrative requirements like changed conditions or alternative measures notices for the TSA.

Guidance documents can also address permanent security standards and approvals for newly constructed spaces. These frequently involve specifications for new security systems consistent with evolving airport requirements.

One Category X airport has created a *Design and Construction Guidelines Manual for Tenant New Construction and Modification* that details construction and modification design guidelines, focusing on signage, architectural, civil, structural, electrical, and mechanical guidelines. The manual's table of contents is in Appendix C.

Another Category X airport has created a *Tenant Improvement Manual* with detailed construction guidelines. This 150-page document provides detailed instructions to tenants desiring to improve their leasehold space. For any improvements, tenants must provide (1) the defined scope, (2) graphic depiction (sketches, photos, specification sheets, and drawing mark-ups), (3) defined location, and (4) justification for requested change. The *Tenant Improvement Manual* table of contents is in Appendix D.

2.7.5 Tenant Engagement Strategies

Airport operators should cultivate stakeholder engagement in the security of the airport to reinforce the airport's security culture and remind them of their security responsibilities as an airport badge holder. Engaging airport tenants in security activities will also improve the airport's security culture as employees become more situationally aware. An interconnected airport tenant security culture is stronger when all tenants are engaged and committed to supporting security in their daily operations.

Many airports have switched to virtual or hybrid meetings and events. This allows for more participants from multiple shifts to join the discussion. However, many airports feel there is far less participation and retention of information because the participants are less focused on the meeting. Airports can strategically use virtual meetings to encourage greater participation from participants to boost engagement.

Detailed information on improving an airport's security culture and engaging airport tenants is provided in PARAS 0044: *Strategies for Aviation Security Stakeholder Information-Sharing* and PARAS 0049: *Creating and Maintaining a Strong Security Culture at Airports*.

SECURITY EVENTS

Security awareness events, such as annual tabletop and simulation exercises, are opportunities to engage airport tenants and discuss security topics in greater detail. Whenever possible, airports should invite frontline tenant workers to join these events to improve their security knowledge and encourage their engagement with the security of the airport.

Security roadshows are typically short presentations focused on a single security topic, such as access responsibilities or de-escalation practices for unruly individuals. The roadshows are additional training opportunities for tenant workers and should be presented multiple times to ensure participation from all shifts and tenants.

TENANT FEEDBACK

Surveys enable the airport to gain a clearer understanding of how tenant workers feel about the airport security posture. Surveys can gather participant feedback with a limited time commitment for each participant. The anonymous nature of the surveys also gives participants the freedom to speak truthfully without fear of consequence.

One effective type of survey question ask the respondent to specify their level of agreement with a statement, from low to high, with a neutral option in the middle. This type of survey is called a Likert scale and can be used to measure a variety of sentiments (e.g., agreement, satisfaction, frequency, desirability) while providing the participant with degrees of opinion. Each sentiment is assigned a numerical value (i.e., "I strongly agree" is assigned the number 7), which allows the airport to objectively measure their tenants' opinions and perceptions. The data from the surveys can be used to determine how certain security initiatives have impacted the airport's security culture. This information can be compared to the airport's key performance indicators to determine where the airport should focus more attention.

Stakeholder forums allow for continuous and open dialogue regarding security programs, procedures, and technologies that can be applied at a tenant facility to mitigate the potential for security incidents and violations. The forums gather several stakeholders into a shared space, and a host leads discussions by asking questions to elicit feedback. The stakeholders can interact with each other and share concerns or suggestions. These forums provide valuable information regarding the airport's security program but require more effort than other methods. The forum will take more time than a feedback survey and will

require a leader to manage the group and guide the discussion. Participants may also feel less free to speak as there is less anonymity in the group. Regular stakeholder forums can help the airport gauge the progress of certain security initiatives.

INCENTIVE PROGRAMS

Incentive programs are reward-based initiatives designed to encourage tenant employees to participate in the airport's security programs. Employees who challenge correctly or perform desirable security tasks, such as reporting or correctly answering quiz questions, are rewarded with prizes.

Many airports reward participants with gift cards or vouchers to airport concessionaires; however, this is not possible for all airports because many local governments prohibit any form of monetary payment as an incentive. Some airports create raffles or reward participants with small items like challenge coins or branded merchandise. Collectible items, such as challenge coins, are highly desirable, and airports report high participation from employees attempting to complete collections. This is a good option if monetary rewards are prohibited, but they can be costly for airports without extra funds in the security budget.

For airports with a limited budget, rewards such as a parking space or public recognition can be used to incentivize participation in security initiatives.

ENGAGEMENT METRICS

Collecting engagement metrics will allow the airport to gauge the impact of programs and initiatives on the airport's security posture, and compare performance over time. Strategic data collection would enable the airport to determine how engaged airport tenants are in the airport's security efforts and highlight areas in need of attention. The metrics of success will be determined by the individual airport but may include:

- Number of citations
- Number of successful badge challenges
- Number of incentives rewarded
- Percentage of tenant training complete
- Percentage of successful log audits
- Stakeholder feedback scores

Once the airport has defined its metrics, data will need to be collected periodically and compared to past performance to determine the level of change. Data can be collected through a variety of methods, and the airport can leverage existing data collection processes, such as training logs and security violation lists.

2.7.6 Training

Airports should leverage initial, recurrent, and supplemental training to enable behavior changes, and reinforce and promote an enhanced security posture.

The most effective training program is composed of initial and recurrent training paired with special training events and reinforcement measures, such as newsletters and quizzing. Repetition of key security messages will promote security awareness and knowledge retention.

Initial Training: The airport's SIDA and AOA training are often an employee's first introduction to the airport's security positions, so this training should be thorough and memorable. Security training provided at the beginning of a new badge holder's tenure directly influences the airport's security

culture and posture. It is common for airports to require additional security training beyond what is federally required. The airport may require this additional training as part of its rules and regulations or as a city/county requirement.

Recurrent Training: Many airports require annual or biannual recurrent training for their badged population. This is typically performed in conjunction with badge renewal. Recurrent training is important to refamiliarize badge holders with their security responsibilities and update them on any changes to the security program. Recurrent training can consist of the same training courses or modules used in the initial training, or it may consist of modified courses and quizzes.

Supplemental Training: Often these trainings and presentations are tailored for certain badged populations, such as presentations on vendor goods inspections. Many airports use special training events to reiterate security requirements and responsibilities to tenant workers. Airports may consider adding the following topics to their training program or presenting them during special training events:

- Insider threat awareness
- Reporting protocols
- Active shooter
- Workplace violence
- Security information-sharing requirements
- Cybersecurity

Training requirements should be based on the tenant worker's security responsibilities

Retraining: Many airports require retraining as an administrative penalty for breaking an airport security rule. In a tiered penalty system, retraining is often included at all levels up to badge revocation. The individual may retake the entire security training course or only specific topics related to the broken security rule.

Training Administration: Initial and recurrent security training is most often provided via computer-based applications. Computer-based training requires a high initial investment in the equipment and training modules, which may need periodic updating.

Instructor-led training is also common. Participation during instructor-led training allows for better information retention, as participants can ask questions for clarification. Some training courses provide opportunities to role-play security scenarios. Instructor-led training will require a qualified trainer.

Special trainings may be administered and taught by airport personnel, local law enforcement, or federal and local partners. It is common for airport police to present on specific security trends or security awareness. TSA will provide situational awareness training to airport workers upon request as part of their "If You See Something, Say Something®" program. Local security partners, such as fusion centers, may also be willing to provide training on specific topics to airport tenants.

SECTION 3: ASSESSING AND ENFORCING TENANT SECURITY PERFORMANCE

Effective implementation of security measures is evaluated through an airport and tenant's quality control program. This program usually comprises several related activities, including assessments, audits and inspections, and tests, each with a different purpose and method of delivery.

Interviews with airports and tenants indicated that the degree to which each activity is undertaken differs from one location to the next. Actions to rectify identified shortfalls also vary based on who is conducting the activity (e.g., self-evaluation or TSA), the scope of the activity (e.g., localized test versus system-wide audit), and the level of noncompliance.

Quality control measures ensure that the tenants are complying with policies, principles, standards, procedures, and methodologies as well as legal, regulatory, and contractual requirements. Developing formal processes to implement these measures provides the airport with documentation that may assist when penalties are issued.

It is important to emphasize that these activities reflect the extent to which an entity complies with existing requirements; they do not comment on the effectiveness of those requirements to counter a new, emerging, or resurging threat. Vulnerability assessments add the necessary analytical component to determine whether existing requirements need to be adjusted to prevent a threat from being carried out.

Tenant employees are reminded of their security responsibilities every time they are inspected, audited, tested, or assessed, so these measures should be performed regularly. Inspections, audits, and tests may be conducted more frequently because they typically do not require substantial time commitments. Vulnerability assessments demand longer time commitments and are therefore carried out less frequently, often annually.

3.1 Vulnerability Assessments

Comprehensive vulnerability assessments allow the airport to identify deficiencies, vulnerabilities, and security risks in the security operations, employee training, or facility design. The information collected during the assessment can be used to identify and prioritize security enhancement projects. Vulnerability assessments may be performed on an as-needed basis to help identify the root cause of recent security trends.

The optimal way to ensure effective mitigation measures is by establishing and maintaining a vulnerability assessment regimen. Unlike audits or inspections that confirm measures are in place, assessments include analysis that looks at the efficacy of the measures to determine whether they meet the intended objective. These assessments may be performed by an external entity (e.g., TSA), the airport, or the security point of contact for the tenant. These assessments focus on current threat information relevant to the airport and are tailored as necessary to reflect changes in the threat picture.

From the largest Category X to the smallest Category IV, airport security depends on the understanding, implementation, and sustainment of vulnerability mitigation measures that counter threats. These measures must focus on preventing a threat from being executed, regardless of whether the perpetrator's motivation is criminal (e.g., theft), ideological/political (e.g., terrorism), disruptive (e.g., vandalism), or some other inspiration. In all cases, the focus is on ensuring security levels are sufficient to detect, deter, or prevent the perpetrator from carrying out the action.

The airports that indicated vulnerability assessments were conducted stated that the initiatives were partnerships with other organizations such as TSA, FBI, or CISA.

Depending on the type of assessment being conducted, the operational areas, facilities, and operations themselves may be included. For example, where a tenant facility is near or part of an airport perimeter, a vulnerability assessment may include those facilities and tenant operational processes, or tenant areas may need to be accessed. This would include inspection and evaluation of physical items like barriers, fencing, walls, and structures forming the perimeter. It would also likely involve assessment of access control measures at gates and doors. In addition to assessing the physical security measures in those tenant areas, an inspection and review of related security practices would be conducted. As part of internal review and response to vulnerability assessments, it is not uncommon for airports to review findings and conclusions with key stakeholders, including tenants, and for recommendations to include tenant improvements.

One interviewed airport stated that joint vulnerability assessments are conducted annually with TSA and the FBI, and a Drone Vulnerability Assessment was recently completed. That airport now has an assigned FBI agent. To address insider threat concerns, a robust "If You See Something, Say Something®" program is in place. However, this airport does not have a dedicated risk manager or risk management department.

Designating an airport risk manager would be highly beneficial in ensuring vulnerability assessment results are implemented appropriately for the airport's circumstances and unique characteristics. A risk manager is an individual who has the knowledge and expertise necessary to understand the nuances of the threat-vulnerability consequence matrix and how it applies to the airport. Some airports hire a consultant to perform the vulnerability assessment, which is more costly but provides an outside perspective by a security expert. The consultant can offer recommendations with the findings and help the airport identify and prioritize security projects.

The Vulnerability Assessment Guide in Figure 2 is a non-comprehensive list of topics and questions that can be used when assessing the effectiveness of security measures. These points focus on a tenant whose facility constitutes part of the airport's perimeter, but the principles can be applied to any tenant or third-party controlled site.

Figure 2. Vulnerability Assessment Guide

Vulnerability Assessment Components

1. General information
2. Perimeter aspects
3. Facility security characteristics
4. Access mechanisms
5. Personnel
6. Designation of secure areas

Vulnerability Assessment Guide

Tenant/Third-Party Controlled Facility on Airport Perimeter

The following questions are a non-comprehensive list of considerations when assessing the effectiveness of security measures implemented by a tenant whose facility constitutes part of the airport's perimeter.

General

- Who has primary responsibility for access control security around the tenant facility?
- Does the airport have access to tenant security documentation?
- Does the tenant participate in meetings during which threat information is disseminated?
  - If no, how is the tenant made aware of changes in threats?

Perimeter Aspects

- How is the facility secured on the public side?
- What physical barriers are in place between the public side and the secure (airport) side?
  - Do any natural or artificial features exist that would enable a perpetrator to breach the barrier (e.g., parked vehicles, trees, construction objects)?
  - How often is maintenance performed to ensure the physical barriers remain clear (e.g., ground clearing, removal of objects)?
- Does the perimeter line controlled by the tenant include any fencing?
  - If yes:
    - Is the fencing at least 8 feet high?
    - Is it topped with barbed wire or some type of razor-taped wire?
    - Is the bottom of the fence either buried in the ground or firmly affixed to a concrete base or sill?
    - Is the material highly difficult to cut?
- Is a CCTV system in use?
  - If yes:
    - Does the airport have a policy on the use of CCTV cameras and equipment at tenant facilities?
    - Does the tenant have written protocols regarding use, management, monitoring, recording, duplication, data storage, release, and general access to the CCTV system?
    - Is the system monitored in real time?
      - If yes:
        - Who has access to the system feed?
        - What protocols are in place to respond to an intruder?
    - Are procedures in place to enable sharing CCTV data with the airport?
- Is an intruder detection system in use?
  - If yes:
    - Is the system monitored 24/7?
    - Who has access to the system feed?
    - What protocols are in place to respond to an intruder?
- Is perimeter lighting spaced close enough that no dark spots exist where an intruder could hide undetected?
  - How often are inspections of the security lighting system performed to ensure lights are replaced before their luminosity decreases or they burn out?
- Is the tenant responsible for patrols?
  - If yes:
    - How frequent are the patrols?
    - How are the patrols performed (e.g., on foot, vehicular)
    - What response protocols are in place if an issue is detected?
- Is the tenant responsible for any gates?
  - If yes:
    - Is the gate constructed of material at least as robust as the fencing?
    - How is the gate opened (e.g., key, badge)? *See Access Mechanisms below for more questions pertaining to access mechanisms.*

Facility Security

- How is access from the public side into the facility controlled?
- Are openings in the building such as windows and ventilation ducts securely locked or fitted with grills, bars, or other entrance-preventing devices?

- Are doors to secure areas equipped with audible alarms?
- Are entrances and exits monitored with CCTV?
  - If yes:
    - Is the CCTV feed monitored in real time?
    - Who has access to the system feed?
    - What protocols are in place to respond to an intruder?
- Who performs security patrols of the facility (e.g., airport, LEOs, contract staff)?
- Who performs audits and inspections of the facility?
- Who monitors the access portals?

Access Mechanisms

- Who owns the ACS?
  - If tenant:
    - Does the airport have access to the control logs?
    - How often is the access media audited?
- How is access to the secure (airport) side obtained?
  - If a card reader/badge system is used:
    - Are the badges issued by the airport or the tenant?
      - If issued locally, does the tenant have strict control and accounting procedures for badge issuance?
    - Is multifactor authentication or two-factor badge authentication in use?
    - How is badge-sharing prevented?
    - What procedures are in place if a badge is stolen or the holder is no longer employed?
  - If keys are used:
    - Are specific procedures in place for the issuance, usage, and protection of keys?
    - Are keys only issued to those individuals with a proven need to independently access the space?
    - Are keys numbered or registered to prevent duplication?
    - How often is the lock-and-key inventory audited?
    - What steps are taken in the event of employee departure or key loss?
  - How is piggybacking/tailgating prevented?

Personnel

- Are visitors, vendors, and other non-employee personnel vetted prior to accessing the facility?
- Are all non-employees escorted while in the facility?
- Are non-employees prevented from accessing the airport side unless properly authorized by the airport?
- Are badges clearly coded (e.g., colors, stripes) to indicate the areas to which the badge holder is authorized access?
- Is a robust challenge protocol in place to ensure unauthorized personnel are not allowed to access or remain in secure areas?
- Does the tenant have a policy against employees sharing badges, access codes, keys, or otherwise circumventing the ACS?

Designation of Secure Areas

- Are restricted areas within the tenant facility well marked with signage?
- Are access points from the facility to the airport side well marked with signage?

3.2 Inspections, Audits, and Tests

INSPECTION ACTIVITY

Inspections are narrowly focused comparisons of what is occurring versus predetermined criteria at a single point in time. Internally driven inspections identify local and systemic issues that can be addressed before they become extensive. Violations identified during inspections conducted by external bodies such as TSA can result in hefty fines.

Many airports conduct daily inspections. The airport perimeter was highlighted as being checked every day, and frequent inspections were performed on access control mechanisms, both automated and lock-and-key. Badge challenges were also a frequent activity. Some airports inspect all employees and any items entering restricted areas, and several airports conduct random inspections of employees, usually in partnership with TSA. Below is sample language in one airport's rules and regulations that permit the inspection of any individual and their property when entering one of the designated restricted areas.

> AOA - Right to Search: The Permittee agrees that its vehicles, cargo, goods and other personal property are subject to being searched when attempting to enter or leave and while on the secured Area/AOA/SIDA. The Permittee further agrees that it shall not authorize any employee or agent to enter the secured Area/AOA/SIDA unless and until such employee or agent has executed a written consent-to-search form acceptable to the Department of Airport (DOA). Persons not executing such consent-to-search form shall not be employed by the Permittee of the Airport, in any job requiring access to the secured Area/AOA/SIDA.

Note that the airport requires individuals authorized to access the restricted area to sign a consent-to-search form. Some airports include language in the badge application allowing search of person and property, such as in the example below. The applicant must sign the agreement or forfeit the right to an airport badge allowing access to the restricted areas.

> I understand and acknowledge that by accepting an Airport ID badge I am giving my consent for search by [the Airport's] employees, contract employees authorized by the [Airport], and/or TSA personnel of both my person and property whenever entering, being within, or leaving a secure or sterile area of the airport to ensure I have a valid Airport ID badge and am not carrying any prohibited items. Further, I understand and acknowledge that my refusal to comply with this consent search may result in my Airport ID badge being confiscated and my access to secure and/or sterile areas of the airport being denied. By initialing here, I certify I have read and understood this statement.

Inspections of badges and keys, in addition to audits, were reported by several airports. One airport uses a centralized and automated key- and lock-control system that ensures the airport tenants fully understand their responsibilities with respect to access control security. Airport field security inspectors visit each tenant and conduct a full audit of their key control logs and practices. The findings are recorded in an automated form, and are compiled and maintained in a centralized database. The field report form includes fields for entry of a range of data relating to a tenant's lock and key control programs, including the hardware (locks and keys themselves) as well as operational control and record-keeping practices. This automated report system is a good practice for airports looking to enhance their inspection and audit systems.

Several airports employ a contractor to perform perimeter patrols and inspections at access control points. Security responsibilities and job functions for contract security are typically described in the contract with the service provider and a set of post orders that describe the officers' scope of work. Post

orders may be maintained by the contractor's on-site manager or posted at locations where the officers will be stationed. Airports may require certain certifications for officers stationed on property, such as permit to carry a firearm, and evidence that all officers have completed required trainings, such as SIDA and AOA training. The sample language below is from an airport's EAA requiring the use of contract security and a semi-annual review of the post orders.

> [Tenant] will accomplish access control at each access point to the [Tenant] Exclusive Security Areas by:
>
> Maintaining properly staffed security posts or computer-assisted access control points or both at each [Tenant] vehicle and pedestrian gate used to enter the [Tenant] Security Areas. [Tenant] will review security post orders semi-annually and will make those orders available for inspection with the [Airport] or TSA security inspectors.

A major cargo company that operates from a Category X airport provided a tenant's perspective on quality control procedures. Inspection practices included airport examination of physical security items, including locks, fencing, setback signage, and building walk-throughs. The tenant stated that inspections and audits were performed by both TSA and airport personnel, with the airport activity being more frequent.

AUDIT ACTIVITY

Audits are an evaluation of adherence to requirements over time and often involve a review of a series of inspection results. They focus on procedural and systemic compliance. Ideally, audits are conducted by an external entity to remove any bias in the evaluation.

Audits are common at airports to identify discrepancies in data logs. Airport badge logs may be the most commonly audited due to the regulations surrounding lost and missing badges. Another common data log airports utilize tracks doors at tenant facilities with access to restricted areas (see Section 3.3).

Airports may also audit access control logs to identify unusual movements throughout the campus. Several airports with an automated ACS indicated they follow TSA-specified procedures for auditing media related to unescorted access. Where tenant facilities are part of an airport's automated ACS, the audit can be conducted using airport records. However, some tenants interviewed for this project indicated that their facilities are secured by an automatic ACS installed by their corporate security department and permissions for access are granted through a centralized system that is operated by corporate management. When evaluating the vulnerability of such a system, the assessors should determine the extent of the corporate security office's expertise in security parameters and ensure the corporate security policies and measures are adapted as needed to address any unique circumstances at the tenant's location.

Key logs may be audited for vehicle gates or pedestrian doors secured with a lock-and-key system to ensure no keys are missing. All airports stated they audit key control programs, some through random inspections culminating in comprehensive annual audits.

Audits may also compare blueprints and design documents to the facility to determine whether the tenant has made security enhancements that do not comply with the airport rules or lease agreement.

TESTING ACTIVITY

Airport security and law enforcement often test tenant employees to ensure they are complying with airport security requirements. Overt or covert tests are simulations of an attempt to commit an unlawful

act. They typically focus on access controls, protection of aircraft, implementation of inspections, and other means by which a bad actor may carry out a threat.

Testing methods should be tailored to the tenant's security responsibilities. For example, security may attempt to piggyback through an access-controlled door or purposefully hide or obscure their airport badge. Test failures provide an opportunity to retrain staff, and management should consider a review of operating procedures and training standards. Some airports give rewards for correctly completing the test, which encourages further participation in the security measures.

3.3 Supporting Documentation

Several airports shared materials they developed to facilitate the conduct of quality control activities.

As part of the leasing process at one airport, tenant facilities are required to create a door chart outlining all access portals within the facility. The chart indicates the type of lock or ACS used to secure the portal and the identity of each person issued a key or access control card. In addition to the door chart, tenants are required to create a schematic of the tenant space identifying the location of all access portals.

At another airport, each tenant facility is required to create a tenant Facility Access Plan (FAP), which is submitted to the airport security department. These plans are marked and maintained as SSI, but they are not included as exhibits in the ASP. The FAP includes:

- Designation of facility contact personnel (24/7 contact in the event of an emergency)
- Definition of critical terms utilized in the FAP
- Assignment of responsibility to notify the airport of security events or incidents
- Assignment of responsibilities for preventing unauthorized access to SIDA/AOA areas
- Requirements for employee training/conduct
- Requirements for employee badging and escort
- Requirements for key control
- Requirements for cipher lock control
- Requirements for facility-automated ACS
- Requirements for record keeping and audit with respect to all ACS utilized

An example of a FAP is included as Appendix E.

Tenants governed by the FAP are required to complete an appendix identifying all facility doors and gates and the access control measures used to secure those doors and gates, as shown in Table 1. These measures are subject to inspection and audit by the airport security department. Those inspections are conducted at least annually. Airport security personnel also conduct unscheduled spot inspections.

Table 1. Example of a Door Log

Door Number/ Description	Location	Monitoring	Security Control
Door 1/Pedestrian	Main entrance to building	CCTV/ receptionist	Tenant's access card
Gate 1/Vehicle	Gate with access to AOA on west side of building	Stationed security officer	Airport ACS

One Category X airport's Comprehensive Cargo Security Plan (CCSPP) requires that the tenant manage the escort of unbadged visitors, unbadged employees, and flight crews. These requirements include the maintenance of logs for visitors. Those logs need to document the visitors' names and the type and number of the ID used to establish the identity of the visitor. Additionally, the logs must document the date and time of entry and exit of the visitor and the name and airport badge number of the escort. Logs are required to be maintained for a period of three years, and the airport must be notified of their destruction.

3.4 Corrective Actions

Airports remediate noncompliance through formal corrective action programs. These vary greatly based on the individual airport's state and local laws and security culture. In general, the corrective action program is described in the airport's rules and regulations or an ordinance.

The airport's corrective action program should be carefully documented and reviewed by the airport's legal department. In many cases, the airport's governing body and local governments will need to approve the program and the penalties to be assigned.

When deficiencies in security or noncompliance are identified in a tenant's facility, the airport needs to take prompt corrective actions as quickly as possible. In some cases, the finding requires immediate action, such as repairing an access door that does not lock. In other cases, remediation may take some time, such as retraining. The corrective action program should define any timeframes for completing remediating actions.

Some airports utilize a workflow management system to issue and track citations. This helps the airport ensure citations are addressed and corrective actions are taken. It can also help the airport identify trends and patterns in violations that can be used to enhance quality control measures and tenant training programs.

For more information on establishing and enforcing corrective action programs, please refer to PARAS 0019: *Employee/Vendor Physical Inspection Program Guidance* and PARAS 0020: *Strategies for Effective Airport Identification Media Accountability and Control*.

3.4.1 Monetary and Non-Monetary Penalties

Airports can use either monetary or non-monetary penalties for noncompliance. Many airports must receive permission to issue fines from their governing body, such as city councils, county boards, or the state's Department of Transportation. Fines may be levied against the individual who committed the offense, against the employer of the individual, or both, depending on the airport's program. Issuing monetary penalties to individual airport workers is generally effective at deterring repeat violations. The feasibility of implementing a monetary penalty system must be discussed with the airport's owner, legal department, and local governments.

Monetary penalty systems will require the airport to create collection methods and procedures. This may include the purchase of a payment system but must also include written policies outlining steps to be taken to collect the fine and the penalties for non-payment.

Many airports are prohibited from issuing fines as they can be burdensome to working populations. Instead, the airport can use non-monetary penalties, such as retraining, shorter badge renewal periods, or suspending or revoking access privileges. In many cases, non-monetary penalties impose a burden on the airport to enforce (e.g., teaching retraining courses), so airports developing non-monetary systems

need to ensure there are enough resources to conduct the program. Many airports with monetary penalties also implement retraining and badge suspensions.

In some cases, the airport can use the rules and regulations or local ordinances to pass on fines issued to the airport as a result of a tenant employee security violation. Below is sample language from an airport's rules and regulations to support the transfer of penalties to another party. Note that the rule is supported by a local ordinance to compel compliance.

> Any monetary civil penalty or fee charged to the airport as the result of any action or inaction by any person or entity that violates a federal, state, or local law, or regulation shall, at the discretion of the director, be paid by the person or entity responsible for the violation.

3.4.2 Tiered and Point-Based Systems

Many corrective action programs use a tiered system of violations with increasingly more severe penalties for repeated or additional violations. Typically, the violations accumulate for a certain period of time and reset at the end of that period, often coinciding with the badge renewal process. Some airports consider violations across the worker's entire history at the airport. Some airports only assign the next tier for repeat offenses.

The systems vary from airport to airport, but many have commonalities. Airports can use the following table as a starting point to create their own tiered system based on the most common penalties from other airports.

Table 2. Common Penalties for Tiered Systems

Tier	Badge Suspension Period	Retraining Required?	Monetary Penalty
Tier 1 (First Offense)	24–72 hours	Yes	$25–$200
Tier 2	48–168 hours	Yes, as well as individual's supervisor/manager	$100–$500
Tier 3	Revoked	——	$250–$1000

Below is an example of a tiered violations program written into the airport's rules and regulations. It also sets a time frame within which the offenses accrue before resetting.

> The aviation general manager may, in the manager's discretion, suspend or revoke the Airside Operating Permit, for a definite or indefinite period, or impose fines arising out of any violation to any [City] ordinance. The company will be responsible for any monetary fees assessed by the aviation general manager. The aviation general manager is authorized to impose progressive disciplinary measures for violations of any city ordinance, which shall consist of the following:
>
> (1) First Offense: The company may be assessed a $250 fine.
>
> (2) Second Offense: The company may be assessed a $500 fine within twelve (12) months of the first offense.
>
> (3) Third Offense: The company may be assessed a $1000 fine within twelve (12) months of the first offense.

> (4) Suspension: The company's Airside Operating Permit may be suspended by the aviation general manager.
>
> (5) Revocation: Any company violating any city ordinance shall be subject to revocation of its Airside Operating Permit.

Some airports assign a point value to each type of violation, like a traffic point system. Accruing a pre-defined number of points within a specific period of time results in monetary and/or non-monetary fines. More serious offenses are typically assigned a higher point value. After the specified period is complete, points are reset to zero, or the airport may choose to track the number of points across the worker's history at the airport.

APPENDIX A. SECURITY SURVEILLANCE SYSTEM POLICIES

CCTV Security Surveillance System Policies and Guidelines

1. ***Introduction***
   - This Directive will serve to provide the policies and procedures to be adhered to by all DOA personnel, vendors, concessionaires, contractors, businesses, airlines, or any other persons or entities who have access to [NAME] Airport's CCTV Security Surveillance System. CCTV is used to enhance security, safety, and quality of life by integrating the best practices of "virtual policing" with state-of-the-art technology.
   - The Security Division will be the regulatory entity regarding [NAME] Airport's CCTV Security Surveillance System. The Division will be responsible for CCTV to include the installation and use of cameras; use and operations of VMS; placement, use, and operations of associated workstations; approval of who will have access of any type to the CCTV Security Surveillance System, the preservation of selected video footage; the viewing of the video footage; and the preparation of CDs or other digital media and to allow viewing of selected video.

2. ***Installation of Cameras and Recording Systems***
3. ***Use of [NAME] Airport's VMS and Related CCTV Surveillance System***
   - Examples of legitimate safety and security purposes for CCTV monitoring include but are not limited to:
     - Protection of individuals, property, and buildings
     - Confirmation of alarms or events
     - Patrol of public areas
     - Monitor aircraft movement
     - Investigation of incidents at the TSA checkpoints
     - Investigation of criminal activity
     - Emergency/incident response
     - Investigation of smoke, fire, or flooding
     - Monitoring security K-9 activity
     - Security training

4. ***Selected Video Preservation Policy and Procedures***

> *(1)* This Operating Directive will serve to provide the policies and procedures for Security Division Personnel to adhere to regarding the preservation of selected video footage, the viewing of the video footage, and the preparation of CDs or other digital media; to allow viewing of selected video (collectively referred to as "CD"). It is intended to facilitate the preservation of selected video footage which may depict information relevant to reported emergencies, criminal activities, property damage, sick or injured persons, or similar incidents, provided that the Security Division receives timely notice of said incidents.

APPENDIX B. EXAMPLE CYBERSECURITY POLICY FOR TENANTS

Cybersecurity Policy Requirements

Applicable as of the Effective Date and may change from time to time in the City's sole discretion.

- *Automatic Screen lock in 15 minutes of inactivity on the workstation that use a password to unlock the workstation screen.*
- *Users should have unique login that requires a strong password that must be changed on a routine basis.*
    - *Passwords best practices policies:*
        - *Password must be at least thirteen (13) characters and include at least three of the following types of characters: upper case, lower case, number, and special character.*
        - *New passwords must not have been used in the past 10 passwords.*
          Passwords must be changed every 90 days and have a minimum age of two (2) days.
        - *After six unsuccessful attempts, your account will be locked for 2 hours or until an administrator enables the account.*
- *No Default Passwords for user or administrator accounts.*
- *No guest accounts.*
- *Role Base Access – Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.*
- *Antivirus installed and updated routinely.*
- *Firewall installed.*
- *Use Data Encryption when workstation used outside the more secure corporate network environment.*
- *Two-Factor Authentication for users accessing workstation.*
- *Operating system patching to occur on a monthly basis or as required.*

APPENDIX C. CONSTRUCTION GUIDELINES FOR TENANTS

Tenant Construction Guidelines

Table of Contents

Below is the section on temporary barriers extracted from the Construction Guidelines:

3.2.4 **Temporary Barriers**: Temporary Interior and Exterior construction wall and/or barrier shall be constructed per DOA/[redacted] requirements as follows:

- No plastic "fillable" barriers shall be permitted on the Aircraft Operations Area (AOA).
- All interior construction requires a temporary barrier.
- Temporary barriers shall create a dust barrier and meet one of three conditions: 1) Extend to ceiling/structure above, 2) Extend to a height that shall not allow visibility of work site, 3) Provide a top enclosure to isolate the work site.
- All barriers shall be constructed of a standard stud wall with finished drywall, painted, painted and/or graphics, cove base and trim.
- All barriers shall be maintained in good condition throughout the entire project.
- Barriers shall not expose non-construction personnel to pinch points, slips, trips, falls, or cut hazards.
- Barriers shall be installed on a plywood/hardboard base per DOA/[redacted] requirements to prevent floor damage.
- Access doors to the construction areas shall be self-closing, metal type and secured using a Best or equivalent seven-pin type cored locking device operator using green, orange, sand or other construction core as required by the DOA.
- Following the project completion, all finishes (project related or adjacent to the project) shall be restored to a DOA acceptable condition.

APPENDIX D. TENANT IMPROVEMENT MANUAL

TABLE OF CONTENTS

Revisions Are Indicated By Gray Shading

2

PART 8. EXHIBITS

APPENDIX E. FACILITY ACCESS PLAN

Facility Access Control Contact (FACC)

The FACC shall serve as the Tenant primary and immediate contact for all security related activities and communications with the [redacted] and the Transportation Security Administration (TSA) and is available 24 hours a day, seven (7) days a week.

The FACC will immediately notify [redacted] Operations of any lost or stolen keys, or access media to access points providing unrestricted access to the SIDA/AOA.

The FACC will report unserviceable locks on access points providing unrestricted access to the SIDA/AOA.

The FACC shall review with sufficient frequency all security related functions to ensure effectiveness and compliance with this program and will on a periodic and appropriate basis conduct, or ensure that a review be made of the following:

- All persons provided tenant access control media (i.e., keys, cipher codes, proximity cards) to the facility that allows access to the SIDA/AOA must be issued a valid [redacted] SIDA (Blue, Red, or Green) Airport ID.
- Proper operation of Facility Access Control systems, measures and procedures pertaining to SIDA/AOA.
- Storage and distribution of Facility Access media to ensure only authorized persons have unrestricted access to the SIDA/AOA.

The FACC will make immediate notification to the [redacted] Airport Security Coordinator of any instance of non-compliance with this Facility Access Control Plan.

The Facility Access Control Contact or his/her designee, when notified or becomes aware of an incident, suspicious activity or threat information that could affect the security of [redacted] or US Civil Aviation must notify [redacted] Airport Operations as soon as practical. Incidents, suspicious activities, and threat information may include, but are not limited to incidents of interference with flight crew, specific or non-specific bomb threats, any information relating to the possible surveillance of an aircraft or airport facility that could indicate a potential threat to civil aviation.

The following information, as it is available and to the extent not legally prohibited, shall include in this report:

1. The name of the reporting individual and call back number
2. A description of the threat/incident/suspicious activity.
3. The names and other biographical data, as available, of individuals involved in the threat, incident, or activity.
4. The source of any threat information.

Facility Access Control Overview

Individuals without a valid [redacted] ID are not allowed to be left alone, in tenant facility areas with unrestricted access points to the SIDA/AOA.

Tenants are required to train their employees to, report unauthorized or suspicious individuals, activities, or items in the SIDA/AOA, and secure the following access points:

- Tenant Doors and Gates providing unrestricted access to the SIDA/AOA
  - These doors are secured by the tenant through the use of a lock and key system, cipher lock or a FSCAS approved by the [redacted].
  - Locks corresponding to unaccounted keys and/or locks that malfunction will immediately be re-cored by tenant.
  - During tenant business hours, these doors are monitored by employees with valid [redacted] ID to the SIDA/AOA to ensure no unauthorized access and/or alarmed to control unauthorized use and access to the SIDA/AOA.
  - When not in use, these doors are secured by the tenant.
- Vehicle Overhead Doors and Gates
  - These doors are secured by the tenant through use of a lock and key system, cipher lock, or a FSCAS approved by the [redacted]
  - These doors are either kept closed and secured or monitored by employees with valid [redacted] ID to the SIDA/AOA when open and in use.

Facility Key System (FKS)

Facility Access Control Contacts (FACCs) are to control their lock and key systems, which allow unrestricted access to the SIDA/AOA, by conforming to the following minimum criteria.

- The FACC will ensure key holders whose keys have been lost or stolen report the loss or theft to [redacted] Airport Public Safety Office immediately.
- The Tenant will replace or re-core or replace all locks with unrestricted access to the SIDA/AOA whenever a single key is reported lost, stolen or otherwise unaccounted.
- FACCs are responsible for notifying [redacted] Airport Public Safety or Airport Operations regarding unserviceable locks on access points providing unrestricted access to the SIDA/AOA.
- The FACC will ensure the return of all keys issued by the tenant when an individual no longer needs unescorted access to the SIDA/AOA. Keys providing access to airport SIDA/AOA will only be issued to individuals issued a valid airport ID for SIDA/AOA.
- The FACC will ensure that control numbers and/or letters that are key holder specific are stamped/written on each key, and logged by date, key number/letter and issued key holder. No other identifier is used on the keys.
- The FACC will audit keys to access points providing unrestricted access to the SIDA/AOA at least once annually. A record of the audit must be maintained for at least twelve (12) calendar months including date of audit and name of the person conducting audit.
- The FACC will ensure employees report any lost or stolen keys immediately to the FACC.
- The FACC will maintain un-issued keys in a secure area with access limited to designated key custodians who have an airport approved badge for the SIDA/AOA.
- The FACC will maintain records of all keys issued including total keys maintained for each lock, key holder name, key serial number, issue date, return date, or date lost.
- [redacted] monitors tenant lock and key control programs by auditing record keeping, at least once annually, and auditing access points.

Facility Security Computer Access System (FSCAS)

Facility Access Control Contacts are required to control their Facility Security Computer Access System (FSCAS), which allow unrestricted access to the SIDA/AOA, by conforming to the following minimum criteria.

- Require the return of all access control media issued by the tenant when an individual no longer needs unescorted access to the SIDA/AOA.
- Facility access control media providing unrestricted access to airport SIDA/AOA will only be issued to individuals issued a valid airport ID for SIDA/AOA.
- The FACC will ensure access control media has a unique individual serial number.
- The FACC will audit tenant access media to access points providing unrestricted to the SIDA/AOA at least once annually. A record of the audit must be maintained for at least twelve (12) calendar months including date of audit and name of the person conducting audit.
- The FACC will require employees to report any lost or stolen access media and deactivate access media immediately.
- The FACC will maintain un-issued access media in a secure area with access limited to authorized [redacted] ID badged individuals.
- The FACC will maintain records of all access media issued including total access media maintained for each lock with unrestricted access to the SIDA/AOA. Records must include access media holder name, access media serial number, issue date, return date or date lost.
- [redacted] monitors FSCAS programs by auditing record keeping, at least once annually, and auditing access points and the FSCAS.

Tenant Security Combination / Cipher Locks

Facility Access Control Contacts are required to control their doors or gates, which allow unrestricted access to the SIDA/AOA, and are secured by a cipher lock by conforming to the following minimum criteria.

- Ensure cipher lock combinations and codes are provided only to [redacted] ID badge holders with authorized unescorted access to the SIDA/AOA.
- Immediately change lock combinations and cipher lock codes when the combination/code has become compromised or when a person no longer requires unescorted access.
- Unserviceable locks will be immediately reported to the FACC.
- Maintain a record of the date of last combination/code change, the names and [redacted] ID badge numbers of individuals issued the combination/code for each access point providing unrestricted access to the SIDA/AOA.
- Train individuals issued the cipher code/combination to not share the code/combination.
- [redacted] monitors Cipher Lock programs by reviewing record keeping, at least once annually, and observing access points.

Facility Access Doors & Gates

PLEASE PROVIDE A MAP OF THE FACILITY.

Describe where your SIDA Area is located. List of Facility Doors leading to SIDA/AOA:

SIDA/AOA Door #	Type	Location	Lock Type/ Control Type

FOR PUBLIC SAFTEY & SECURITY DEPARTMENT	
ASC Inspector:	Initial Inspection Date:
Title:	Date Approved:
TSA Approval:	Date Approved: