SAFE SKIES

PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0054

January 2025

Optimizing Compliance with Airport Security Rules and Regulations

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Scott Houston, Principal Investigator
Lee Kair
The Chertoff Group
Washington, DC

Gloria Bender
Jessica Gafford
Andy Entrekin
TransSolutions, LLC
Fort Worth, Texas

Michele Freadman
M. Freadman Consulting, LLC
Attleboro, Massachusetts

Kim Dickie
KPD Consulting, LLC
Powell Butte, Oregon

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 0054 PROJECT PANEL

Tracy Fuller *Allied Universal*

Mark Inzana *Denver International Airport*

Nikola Vucicevic *John F. Kennedy International Airport*

Jeanne Olivier *Port Authority of New York and New Jersey (Retired)*

Martina Benedikovicova *Charlotte Douglas International Airport*

Jason McBride *Memphis International Airport*

Doug O'Mara *Global Elite Group*

Jordan Biegler *Hartsfield-Jackson Atlanta International Airport*

Jeff Swan *Quad Cities International Airport*

Aaron Deery *Lee County Port Authority*

Abedoon Jamal *San Francisco International Airport*

AUTHOR ACKNOWLEDGMENTS

The PARAS 0054 Research Team would like to thank the organizations and individuals who graciously volunteered to participate in interviews and gave permission to showcase their unique practices. This research is successful only because of their assistance.

The authors would also like to thank the Project Panel for their guidance and feedback during the research, which helped shape the direction of the final document. Our thanks are also extended to National Safe Skies Alliance for facilitating the research and providing guidance.

CONTENTS

TABLES & FIGURES

SUMMARY

Optimizing compliance with airport security rules and regulations requires a comprehensive and systematic approach that balances security requirements with operational needs. As demonstrated throughout this guidance, successful optimization relies on several key elements:

- Well-designed and regularly updated security rules and regulations that clearly communicate requirements and consequences
- Proactive compliance measures that emphasize prevention and encourage positive security behaviors
- Effective methods to identify noncompliance through inspections, audits, and systematic monitoring
- Fair and consistent enforcement strategies that combine accountability with education
- Strong stakeholder engagement and communication to build a culture of security compliance
- Integration of lessons learned from safety programs to enhance security management

Airports can implement these strategies through scalable solutions that require minimal to moderate investment while delivering significant benefits. When properly executed, these approaches can help airports:

- Reduce security incidents and regulatory findings
- Lower administrative costs associated with managing violations
- Improve stakeholder relationships and voluntary compliance
- Create more efficient and effective security operations
- Build a stronger, more resilient security culture

As airports continue to face evolving security challenges and regulatory requirements, the ability to maintain optimal compliance becomes increasingly critical. The strategies and solutions presented in this guidance provide airports with practical methods to enhance their security compliance programs while supporting their broader operational objectives. Through careful implementation of these approaches, airports can work toward creating a more secure, efficient, and compliance-focused operating environment that benefits all stakeholders in the airport community.

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
AI	Artificial Intelligence
AOC	Airport Operations Center
ASB	Airport Security Bulletin
ASC	Airport Security Coordinator
ASM	Airport Security Manager
ASP	Airport Security Program
AWS	Aviation Worker Screening
BEES	Building Effective EUG Security
BOI	Boise Airport
Cat	Category
CEO	Chief Executive Officer
CLT	Charlotte/Douglas International Airport
COU	Counseling Violation
DEN	Denver International Airport
EAA	Exclusive Area Agreement
EUG	Eugene Airport
FBO	Fixed Base Operator
GA	General Aviation
HAWKS	Helping Airport Workers Know Security
IAD	Dulles International Airport
IDMS	Identity Management System
ISO	International Organization for Standardization
KPI	Key Performance Indicator
MWAA	Metropolitan Washington Airports Authority

NA	National Amendment
NOV	Notice of Violation
ONT	Ontario International Airport
OSHA	Occupational Safety and Health Administration
O&I	Orders and Instructions
PDX	Portland International Airport
PGD	Punta Gorda Airport
RCA	Root Cause Analysis
SAT	San Antonio International Airport
SeMS	Security Management System
SFO	San Francisco International Airport
SMS	Safety Management System
TUS	Tucson International Airport

SECTION 1: INTRODUCTION

Airport security rules and regulations form the foundation of an airport's security program by establishing clear requirements and standards that protect the traveling public, airport workers, airlines, tenants, and critical infrastructure. As airports face evolving security threats, changing regulatory requirements, and operational challenges, the need for effective compliance with these rules and regulations becomes increasingly important.

This document provides airports with practical, scalable strategies to optimize compliance through well-designed requirements, proactive measures, stakeholder engagement, and appropriate enforcement actions. The guidance focuses on:

- Developing and updating airport security rules and regulations
- Implementing proactive compliance measures
- Establishing methods to identify noncompliance
- Creating effective violation, fine, and penalty structures
- Applying lessons learned from safety programs

The guidance presented here can be scaled and adapted for airports regardless of their size, governance structure, or operational complexity.

1.1 Research Method and Approach

This guidance is based on interviews and data collected from twenty-two airports of varying sizes and governance structures, as well as an extensive review of literature, publicly available airport security rules and regulations, and security compliance guidance and training materials shared with the Research Team. The research identified effective practices through these interviews and document reviews. When describing common practices or trends, this document refers specifically to observations from this research sample and literature review unless otherwise noted.

1.2 Understanding the Need for Optimized Security Compliance

Effective compliance with airport security rules and regulations is fundamental to maintaining safe and secure airport operations. Beyond meeting regulatory requirements, optimized compliance programs help airports build a strong security culture, reduce vulnerabilities, and improve operational efficiency. These programs represent a strategic investment that supports both security and business objectives.

BENEFITS OF OPTIMIZED COMPLIANCE

Airports with effective, well-designed security rules and regulations that support a security culture of compliance can realize significant operational and strategic benefits. A well-designed compliance program typically reduces security incidents and violations, leading to fewer TSA findings and lower administrative costs. These airports often experience more efficient security operations through better resource allocation and reduced time spent on corrective actions. Strong compliance programs also foster improved stakeholder relationships, as clear communication and consistent enforcement build trust and encourage voluntary compliance. Perhaps most importantly, optimized compliance supports a proactive security culture where potential issues are identified and addressed before they become serious problems, enhancing the airport's overall security posture.

Strategic advantages include:

- Enhanced ability to adapt quickly to new security requirements and threats
- Reduced costs associated with violations and remedial actions
- Improved operational efficiency through standardized processes
- Stronger relationships with regulatory authorities
- Greater stakeholder trust and cooperation
- More effective use of security resources
- Increased employee engagement in security practices

CHALLENGES OF INEFFECTIVE SECURITY COMPLIANCE PROGRAMS

Airports facing challenges with their security rules, regulations, and compliance programs may experience significant impacts to their operations, security posture, and regulatory standing:

Security Risks – The most immediate concern for airports with ineffective security compliance programs is increased vulnerability to security breaches and incidents. Without consistent enforcement and clear procedures, airports often experience higher rates of security violations and gaps in security awareness. This weakness in the security framework can lead to delayed or inadequate responses to emerging threats and vulnerabilities, potentially compromising the overall security of the airport.

Regulatory Challenges – Airports with less effective security compliance programs could face increased TSA enforcement actions, including more frequent inspections and higher numbers of security findings that require correction and result in civil penalties. These airports may also face greater difficulty adapting to new regulatory requirements.

Operational Impacts – The financial and operational burden of ineffective compliance management can be significant. Airports face increased administrative costs from managing violations, implementing corrective actions, and conducting remedial training. Security personnel and resources are often used inefficiently as they respond to preventable incidents rather than focusing on proactive measures. These operational inefficiencies can ripple through various airport departments, affecting overall performance and creating unnecessary complexity in security management. The time and resources required to address compliance issues can become substantial, creating a continuous cycle of reactive corrections rather than proactive compliance.

Stakeholder Issues – Ineffective security rules, regulations, and compliance programs ultimately strain relationships with airport stakeholders. Inadequate communication of security requirements can lead to confusion and resistance among tenants and badge holders. Without strong stakeholder buy in, airports may find it challenging to maintain a robust security culture, further compromising their ability to implement effective security measures. This breakdown in stakeholder relations can create long-term challenges in implementing new security initiatives and maintaining consistent standards across the airport community.

1.3 Using This Document

The guidance is organized into five main sections that address key aspects of security compliance:

Section 2: Developing and Updating Airport Security Rules and Regulations – This section covers the creation, review, and communication of security requirements

Section 3: Proactive Compliance Measures – This section discusses strategies to prevent violations and enhance security awareness

Section 4: Methods to Identify Noncompliance – This section details various inspection and audit approaches

Section 5: Violation, Fine, and Penalty Structures – This section provides frameworks for appropriate enforcement actions

Section 6: Lessons Learned from Safety Programs – This section explores how safety program principles can enhance security compliance

Throughout these sections, real-world examples and proven practices from airports demonstrate how these concepts have been implemented successfully. The document emphasizes programmatic, innovative, and behavioral approaches that can be implemented with minimal to moderate investment, focusing on solutions connected to quality assurance principles.

Airport operators can use this document as a comprehensive resource to evaluate their current compliance programs and identify areas for improvement. The guidance supports airports in selecting and implementing appropriate strategies for their specific operating environment while developing more effective security rules and regulations. Through application of these concepts, airports can build stronger security awareness and culture, enhance stakeholder engagement and communication, and create sustainable compliance solutions that align with their operational needs and capabilities.

SECTION 2: DEVELOPING AND UPDATING AIRPORT SECURITY RULES AND REGULATIONS

Effective policy development and implementation is critical to a successful and effective compliance program. Integrating compliance into daily operations, business processes, and organizational culture—through written policies and procedures, training and education, communication of standards, active oversight, and proactive measures—supports the airport's efforts to improve compliance with security rules and regulations.

2.1 Reviewing Security Rules and Regulations

Continuous assessment of airport security rules and regulations is necessary to identify areas in need of improvement, and to ensure alignment with the evolving legal, regulatory, threat, and societal/workforce landscape. Periodic reviews of the rules and regulations can ensure they are sustainable, timely, and applicable with current internal and external factors, conditions, and laws.

Among the airports studied, the review process is typically performed annually with updates every two years, or as needed. Several airports interviewed conduct the review less frequently (every three to five years) or when a significant regulatory or procedure change triggers necessary revisions. Revisions of airport regulations are often driven regulatory and legal changes, emerging threats and vulnerabilities, compliance performance/violation trends, behavioral incidents, and enforcement gaps. Establishing a standardized time frame and consistent process to revise airport rules and regulations can ensure that the regulations respond to the current operating environment and compliance posture and trends.

The airport security department is the most suited to performing the initial review of the security rules and regulations. These individuals are more informed about the current security violation trends and where the rules and regulations may be deficient. They are also more aware and knowledgeable of the regulatory requirements, both current and anticipated. Secondary reviews often include other airport departments, the airport director, airport police, and the airport's legal counsel.

The primary goal of the review is to identify unintended gaps and loopholes that may impair enforcement action; for example, describing consequences of piggybacking for the individual who held the door but not the one who failed to swipe their badge. Many airports in this study reported having identified gaps regarding inappropriate conduct and behavior of airport workers during the badging process or while on airport property.

The research showed a trend in airport operators incorporating security standards that encompass inappropriate badge holder behavior and conduct at the airport, such as criminal acts or swearing at individuals performing security activities, coworkers, or passengers. Incorporating behavior standards into airport rules and regulations is a method to address and enforce the number of rising incidents of improper conduct by badge holders that affect the safety, security, and operations of the airport.

> Charlotte/Douglas International Airport (CLT) has promulgated provisions in their CLT Security Standards regarding employees who behave inappropriately or are convicted of crimes on airport property. The regulation "Confiscation of Badge" authorizes the airport to permanently revoke the airport badge and all access privileges of any badge holder who engages in inappropriate conduct on airport premises or is convicted of a misdemeanor or felony committed on airport property.
>
> CLT's Security Standards state that every airport user, employee, and subcontractor plays a vital role in ensuring CLT provides and maintains a safe and secure environment. These provisions are designed to ensure that the appropriate legal authority exists for the airport to impose penalties for these specific violations.

> *“(6.2.7.b.)* ***Penalty for Inappropriate Conduct on Airport Premises.***
>
> *“CLT reserves the right to restrict access privileges and confiscate Badges of Badge holders who engage in inappropriate conduct, which includes but is not limited to using offensive or threatening language and/or gestures; refusing to cooperate with law enforcement, CLT staff, TSA, or other individuals charged with implementing the provisions of the ASP [airport security program], or other rules and regulations of CLT; tampering or interfering with the Airport's access control system; interrupting or disrupting airport operations, or damaging airport property. Note: Disseminating or releasing, without authorization, either security sensitive information (“SSI”) as defined in 49 CFR Part 1520, or other information that would not have otherwise been known or observable to the general public that has the potential to impede an investigation or adversely impact operations may be considered inappropriate conduct, depending on the totality of the circumstances.*
>
> *“(6.2.7.c.)* ***Confiscation of Badge for Conviction of Crimes Committed on Airport Property***
>
> *“Confiscation of Badge for Conviction of Crimes Committed on Airport Property. CLT will permanently revoke the Badge and all access privileges of any Badge holder who is convicted of a misdemeanor or felony committed on airport property.”*

———

San Francisco International Airport (SFO) issued rules and regulations to establish behavior that is prohibited for airport badge holders at the airport. An excerpt of the language is below.

> *“(ASB 24-01)* ***Unacceptable Behavior at the Airport.*** *All Airport ID Badge holders shall conduct themselves under the guiding principles of SFO's Core Values. Unacceptable behavior including, but not limited to, verbal or physical assaults, ignoring lawful and reasonable directions by authorized personnel, yelling, and/or profanity by Airport ID Badge holders towards passengers, other badge holders, or anyone at the Airport will not be tolerated. The Airport reserves the right to impose all applicable enforcement actions against any person(s) who violate this bulletin, including against any employer or other authorized signatory of such person(s), which may include, the issuance of citations to such employer or authorized signatory, and/or badge revocation as warranted.”*

———

The Metropolitan Washington Airports Authority (MWAA) airport regulations empower the Airport Security Manager (ASM) of each airport to establish rules and standards (“Orders and Instructions” [O&I]) governing the security of the respective airport. MWAA has published O&I that authorize the ASM to suspend or revoke a badge for inappropriate behavior. The language is presented below.

> *“(10.B.2.iv.)* ***Interference with the operation of Reagan National or Dulles International.*** *The Airport Security Manager may suspend or revoke a person’s ID Badge for serious or repeated, inappropriate behavior, whether criminal or not, that significantly interferes with the efficient and orderly operation of Reagan National or Dulles International (for example, stealing from passengers’ luggage, shoplifting, aggressive confrontations with passengers or co-workers).”*

———

San Antonio International Airport (SAT) added the following provision to its airport security rules and regulations to address the growing number of incidents of improper conduct by badge holders.

> *“(Sec. 3-23)* ***Improper conduct.*** *No person shall engage in any improper conduct while on airport property. Improper conduct includes, without limitation, using profane or vulgar language; committing a felony or a misdemeanor; unlawfully possessing a firearm or other weapon; fighting, defecating, or urinating in public; gambling or participating in other games of chance where money is involved; failing to cooperate with any airport official in the performance of his or her official duties; willfully assaulting or committing battery upon any person; threatening the safety of any person; recklessly or intentionally destroying property owned by any person; or acting in a manner intended or that is reasonably likely to cause physical injury to any person.”*

2.2 Revising or Developing Security Rules and Regulations

When developing and updating security regulations, airports must balance maintaining robust security standards with ensuring that changes do not lead to excessive complexity or administration by the airport, or unfair burdens on tenants and badge holders. Airport security regulations should not only enhance security and reduce risk, but also foster a secure, fair, and efficiently managed airport environment that supports collaborative engagement in building a strong security culture.

Regulations are developed or revised in response to a gap in enforcement measures in existing regulations, spikes in a specific type of security violation, the promulgation of federal security requirements, and associated penalties for noncompliance.

In 2023, TSA issued National Amendment (NA)-23-02 Aviation Worker Screening, which requires specified aviation worker screening (AWS) notice and signage to inform aviation workers of the screening requirements and penalties for noncompliance with the airport's AWS policy, including confiscation and revocation of their badge and/or revocation of unescorted access authority. TSA also requires airports to include a "Screening Notice" in SIDA badge applications that advises that any employee holding a credential granting access to a SIDA may be screened at any time while gaining access to, working in, or leaving a SIDA. As a result of these TSA requirements, some airports issued new or revised regulations to ensure compliance and impose penalties for noncompliance with the NA.

CLT issued a security screening regulation specific to aviation workers in their Security Standards that defines who must be screened, screening protocols, and consequences. An excerpt is presented below.

> ***"4.2.1 Who Must be Screened***
>
> *Aviation workers possessing airport-issued identification (ID) media and their Escorts are subject to screening/inspection for unauthorized weapons, explosives, and incendiaries. Noncompliance with the airport operator's aviation worker screening policy could result in penalties, which may include confiscation of their airport operator issued ID media and/or revocation of unescorted access authority.*
>
> *"In addition, all persons desiring to enter the Secured Area, AOA, SIDA, or Sterile Area are subject to, and consent to, security screening, questioning, inspection, and search of their persons and accessible property as required by law and must comply with the system, measures, or procedures being applied to control access as defined in these rules. This includes Badge holders and those under escort. Screening and searches may be conducted randomly by the TSA or other appointed authority at any time a person is attempting to access or while in restricted areas. Compliance with inspections while at an access point or within the restricted area is mandatory. Inspections can include a search of your person, your outer coat and jacket, your accessible property, and of your Badge. […]*
>
> *"Note: Individuals are considered submitted to screening upon getting in line to or attempting to enter the restricted area and may not leave once they have entered the line until screening is complete."*

Additional indications that an airport's security rules and regulations need enhancement may include the absence of an internal quality control process or system, poor audit outcomes, a punitive culture towards failures, and an overreliance on external checks by TSA and other regulatory agencies without proper follow up.

Often, the revision process begins with the security department or security manager developing proposed language to address regulatory or procedure changes. Some airports participating in this research authorize specific roles or positions to create new rules, regulations, and/or ordinances; this responsibility is often granted to the airport director and their designated representatives through city, county, or state laws and ordinances.

Dade County, Florida ordinances contain language that allows airport directors to issue operational directives and penalties, including fines, for noncompliance with those directives.

> ***"(25-1.2) Applicability of rules and regulations; Operational Directives.***
> *"The Department, through its Director, may from time to time cause to be issued Operational Directives applicable to any Airport. If any such Operational Directive contains a requirement that fees or charges be paid for any operation on or use of an Airport as defined in the Operational Directive, such fees and charges shall be established in accordance with the provisions of subsection 25-1.2(a) hereof (Ord. No. 88-37, § 2, 5-3-88; Ord. No. 95-41, §§ 36, 37, 3-7-95)"*

Changes in policy should reasonably reflect shifts in security risk or operations, and remain current with the airports' operating, legal, and regulatory environment. Updates to security standards should be approached judiciously and carefully, focusing on measures that substantially decrease security risks. Careful drafting will ensure that new language does not create unintended loopholes or gaps that may impair future enforcement of these security provisions. Precise language that can be clearly communicated and understood by the affected populations will avoid policy misunderstandings that contribute to security deficiencies and violations.

Use of a Security Regulation Update Log maintained by the Airport Security Coordinator (ASC) or their representative can help capture relevant revisions proposed or needed throughout the year. The log should contain fields to note the relevant section of the rules and regulation, explain why changes are needed (reference a case/Notice of Violation [NOV] number if necessary), and provide a rough draft of the language revisions. The airport community can propose changes throughout the year; once logged, there is little risk of the suggestion being lost or missed during the revision process. The log can be maintained in a simple spreadsheet, document, or other application already in place at the airport.

Many interviewed airport operators review language published by other airports of comparable size, governance, or in the same state. This provides foundational language to build on and modify to reflect local conditions. This may be especially beneficial to smaller airports with limited resources, such as in-house legal counsel.

When Portland International Airport (PDX) needs to update their security rules and regulations to address a gap, the security manager will review the rules and regulations of other airports published online. Using other airports' language as a reference saves the security manager time during the legal review process, as the language has already been vetted by another airport's legal department.

When a revision is necessary to comply with federal, state, or local law, most airports participating in this research stated that they will modify the regulatory language to fit the airport's rules and regulations format. Requirements outlined in SSI materials (e.g., ASP, NAs, Security Directives [SD]) are scrubbed of the sensitive information before incorporation. Well-drafted regulation language should ensure that the airport stakeholders can clearly understand how to comply, and should not contain unintended gaps or loopholes. Among the airports surveyed, it is common practice to collaborate with TSA to ensure the drafted language accurately reflects the requirements in federal regulations.

Many of the airports interviewed have rules and regulations that exceed TSA requirements, with specific provisions to reduce risk and maintain order for their unique operation. This may include conditions governing social media activity related to incidents or operations occurring at the airport that may impact safety, security, and operations. Local TSA representatives (e.g., the FSD) may be asked to review the drafted language to ensure it does not conflict with any federal requirements.

During the development stage, input is requested from various internal stakeholders, including code enforcers, compliance specialists, security, operations, airport law enforcement, and legal. Some airports interviewed during this research have multiple departments review the proposed language. A rules and regulations committee composed of relevant airport department representatives (e.g., legal, facilities maintenance, tenant operations, airfield operations) can provide a more comprehensive review of the regulations and provide recommended changes from multiple perspectives.

The proposed changes are then submitted for final review and approval to legal and airport executives. Some airports will need approval from the owner of the airport, such as the airport board of directors, county commission, or city attorney's office. The legal department typically has the final review before publication.

2.3 Legal and Governance Impact

Airports face numerous challenges related to state and local ordinances, which often impact the enforcement of security rules and regulations. These challenges arise primarily due to the complex interplay between different layers of regulations, including federal, state, and local laws.

Airports operate under various governance structures, which significantly influence how security rules and regulations are implemented and enforced. Some airports are organized as special districts, which grant certain autonomous powers to enforce their rules and regulations, similar to local ordinances, with significant independence from city or state government oversight. Some airports' security regulations are enacted as local ordinances and changes are required to follow the same lengthy approval processes. Some airports have the legal authority to criminally prosecute specific airport rule violations.

MWAA is empowered through its interstate compact and Virginia law to adopt or amend regulations for Washington Dulles International Airport (IAD) and Ronald Reagan Washington National Airport. The regulations carry the "force and effect of law," which allows MWAA to file criminal charges for certain rule violations.

> *"**§ 1.9. Force and Effect of Law; General Penalty for Violation.** (Res. No. 94-4, 1-5-94) These Regulations have the force and effect of law. Unless otherwise specified, the violation of any of them shall be a Class 4 misdemeanor, a matter within the jurisdiction of the state courts of the political subdivision where the violation occurred and with the same punishment as Class 4 misdemeanors under the Code of Virginia."*

Another airport has included language in its rules and regulations authorizing the airport to criminally charge badge holders for certain violations. The anonymized language is presented below.

> *"Any person who knowingly uses the access control media of another may be criminally charged with Unauthorized Use of Property, [relevant section in the state code], a misdemeanor of the fourth degree, punishable by up to thirty (30) days in jail and/or a fine of up to $250.00, in addition to any penalty established by these Rules and Regulations.*
>
> *"[Authority] issued identification and other access control media are the property of the [Authority] and must be returned upon revocation, suspension, termination of employment, or upon request of [Authority] personnel. Any person who fails or refuses to return an [Authority] Issued Identification, or other Access Control Media, may be denied future issuance of [Authority] issued identification or access control media and/or charged with theft pursuant to [relevant section in the state code]."*

Many states have codes or ordinances that recognize the authority of the airport's governing body, airport director, and their authorized representatives to issue and enforce rules and regulations. Airports can define and establish the responsibilities and authority of the ASM and ASC as representatives of the airport director in the rules and regulations to support the position's authority.

One airport authority has a board resolution that grants authority to the President and Chief Executive Officer (CEO) to amend the rules and regulations during critical or exigent circumstances. This resolution greatly accelerates the organization's capability and process to perform revisions. The language reads:

> *"Written directives, special notices, or memoranda of an operational nature may be issued by the President & CEO or designee under the authority of these Rules and Regulations and shall have the full force and effect as these Rules and Regulations."*

Airport security rules and regulations often reference specific requirements outlined in the ASP, such as access control violations or lost or unaccounted for airport ID media. However, changing the airport's ASP can be time consuming and cumbersome. Amending an ASP usually requires navigating internal review processes, including discussions with legal counsel, lengthy TSA regulatory procedures, and approval from governing bodies (e.g., city council or airport authority), which can delay the implementation of security updates.

The enforcement of local airport security rules and regulations also falls outside the direct purview of federal agencies, although they often address offenses covered by federal regulations or the ASP. This can lead to situations in which both airport and TSA authorities pursue separate actions against violators for the same offenses, complicating the legal landscape. Furthermore, enforcing security rules and regulations and assessing monetary penalties typically require the basic or essential elements of due process, often involving formal notice, an opportunity to be heard, an impartial decision maker, the right to present evidence, a written decision, appeal rights, and reasonable timeframes. These elements of due process, while essential for fairness, add a layer of complexity to airport enforcement efforts, and often require significant time to properly execute.

Some interviewed airports are subject to influence from state-run aviation agency regulations and policies, which guide the creation and enforcement of airport security regulations. These airports enforce and issue penalties for security violations pursuant to state laws and authorities. These examples illustrate the varied and complex nature of airport governance, which requires airports to navigate a maze of regulatory frameworks while striving to maintain effective security measures and compliance by airport stakeholders.

A small, non-US airport, managed through a government concession, is legally allowed to press criminal charges for certain airport security violations based on the results of an investigation. This has served as a significant deterrent factor for individuals who may be tempted to knowingly breach aviation security rules and regulations.

2.4 Stakeholder Communication and Engagement

Effective communication and collaboration with airport stakeholders are crucial to optimizing compliance with airport security rules and regulations. High turnover in tenant and concessionaire employees can make it difficult to institute security knowledge; more new and inexperienced badge holders may lead to more security violations as they learn their job and the airport's rules simultaneously. Airports that engage in frequent, clear, and consistent outreach and communication about their security rules and regulations, including recent updates and proposed changes, have experienced increased trust, improved relationships, and enhanced compliance from airport tenants, workers, and stakeholders.

Airports that have strong relationships with their stakeholder communities often make use of multiple outreach and communication strategies and techniques. There are various communication and engagement methods for sharing important information to ensure employees are aware of and understand the airport's security rules and regulations. Regardless of the specific strategies and techniques implemented, stakeholder communication and engagement efforts must be inclusive and consistent to build and sustain compliance over time.

2.4.1 Communicating with Stakeholders

When communicating changes to security rules and regulations, and other significant security initiatives and updates, it is especially important for airports to be clear about the specific changes and the legal and financial consequences for noncompliance, including loss of badging privileges for tenants, concessions, sponsors, etc., or access privileges or fines for badge holders. Special emphasis placed on clarity and conciseness can ensure changes to security rules and regulations are accessible and easy to understand. Airport security officials should clearly communicate and specify:

- What is changing
- What is staying the same
- Why the change is necessary
- Specific requirements airport workers and stakeholders must follow to comply with the new security requirements
- Consequences for noncompliance

Airports participating in this research generally communicate with their stakeholders through in-person meetings and printed or digital publications.

2.4.1.1 Security Meetings and Working Groups

Security meetings and security working groups with airport stakeholders are the primary or preferred method for communicating updates and issues related to security rules and regulations at many of the airports interviewed for this research. Both strategies provide airport stakeholders access to airport security decision makers and an opportunity to voice concerns with specific issues related to security rules and regulations and enforcement. These forums enhance communication and build trust for airport stakeholders, which support accountability and improve compliance with security rules and regulations.

Among the airports studied, security meetings are typically held at regular intervals (e.g., daily, weekly, monthly, bi-monthly, or quarterly), and attendees may include airport security personnel, law enforcement, federal partners, airport attorneys, airline managers, tenant managers, service provider managers, vendors, and other stakeholders. Tabletop exercises can also be used to reinforce the airport's security rules and regulations. The purpose of these security meetings may include:

- Review of recent security incidents
- Reporting and analysis of security violations, including trends in type of violation, location, company, root cause, etc.
- Introduction of proposed or new security policies, requirements, initiatives, or operational changes
- Discussion of security risks, concerns, and solutions
- Identifying areas for improvement
- Acknowledging accomplishments of airport workers
- Inviting feedback from the broader airport community

Stakeholder security meetings can take a number of forms, but the information sharing and opportunity for stakeholders to express concerns and ask questions about security policies and requirements supports a sense of shared responsibility in complying with airport security rules and regulations. Many airport operators participating in this research divide the meeting into two components: the first part of the meeting invites any stakeholder to participate, and the second part of the meeting is restricted to stakeholders with a "need to know." Attendees who do not meet this criteria are not allowed to attend to ensure that more sensitive security topics can be discussed. This format encourages tenant and concessionaire managers to participate in the meeting.

Leadership visibility and participation are crucial to enhance compliance with security rules and regulations and foster a strong security culture at airports. Leaders are encouraged to engage directly with the airport community and participate in daily operations, training events, and security forums. This top-down leadership approach demonstrates a commitment to security and communicates to all personnel that maintaining a robust security culture is a collective responsibility and high priority.

The research found that many ASMs participate in regularly scheduled discussions or forums with other security managers around the United States. Association and committee forums are a valuable resource to gain experience, knowledge, and background on conditions, rationale, legal issues, etc. affecting peer airports that can be applied when revising security regulations. Security conferences hosted by industry associations are another excellent opportunity for ASMs to exchange experiences and solutions, and to interact with TSA leadership.

A number of airports in this study have established formal security working groups to communicate new requirements, update security messaging, discuss security issues, solicit feedback from stakeholders, and support the airport's security culture. Working groups can serve as platforms for sharing effective security practices and innovative solutions. These groups may meet regularly (e.g., quarterly) or on an as-needed basis to discuss a particular security concern. Security working groups typically include senior representatives from the airport, law enforcement, and security subject matter experts. The regular meeting agendas often include law enforcement, subject matter experts, and FBI briefings for airport stakeholders and community leaders.

MWAA has created a collaborative problem-solving forum that engages their community to discuss and examine specific security issues or solve a security concern. Recent topics studied by the Airport Security Working Group have included a review of a Joint Vulnerability Assessment, insider threat concerns, and badge compliance.

The Airport Security Working Group is led by the ASM and consists of TSA representatives, airport law enforcement, airport operations and maintenance representatives, and many of the airline and ground handling company managers. Other participants are recruited by the ASM for each meeting based on the area of focus.

It may be beneficial to participate in regularly scheduled, population-specific security meetings to discuss security topics that only concern Authorized Signatories, Exclusive Area Agreement (EAA) holders, or a tenant or concessionaire population. Several airports interviewed meet with the authorized signatories to discuss changes to security processes, especially those concerning the badging process. This practice can be extended to other populations and topics, such as discussing changes to regulations around serving and selling alcohol with restaurant, lounge, and duty-free concessionaire managers, or meeting with contract security supervisors to address questions relating to contractor compliance duties under the airport's aviation worker screening plan.

2.4.1.2 Security Bulletins, Newsletters, and Marketing Materials

In addition to in-person discussions, several airports interviewed publish security awareness newsletters, bulletins, posters, mobile applications, and other marketing materials to disseminate important information and educate airport stakeholders on new security rules and regulations or changes to enforcement policy, or to improve compliance with specific measures.

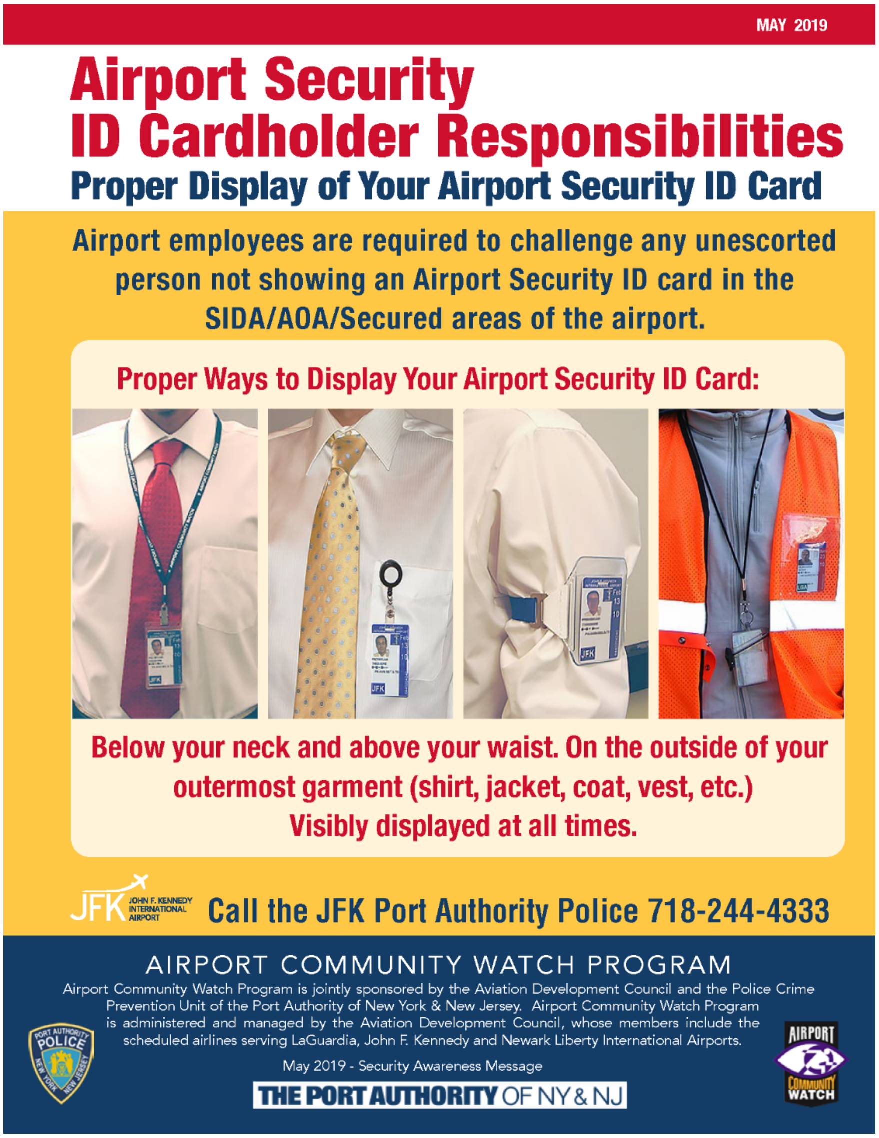
Regularly disseminated newsletters and bulletins keep the airport community current on security information, new policies, programs, initiatives, and other important security-related announcements. Airports also use newsletters and bulletins to incorporate ideas and suggestions submitted by airport stakeholders, such as TSA announcing awards and acknowledging the accomplishments of airport workers who demonstrate an exceptional commitment to the security of the airport and compliance with rules and regulations.

The research found that airport security awareness newsletters are typically distributed on a regular basis (often monthly or quarterly). They include articles written by airport staff or submitted by members of the airport community that discuss special security needs, apprise readers of proposed or upcoming policy changes, reinforce security requirements, and inform of upcoming security initiatives and events. Some airports interviewed focus on a specific security theme or topic for each newsletter based on procedural changes, compliance issues, or operational changes.

Security bulletins are typically shorter in length than newsletters—often just one page—and include articles on new or proposed changes to airport security requirements, guidance and best practices for compliance, and other information on airport security programs and initiatives. Bulletins are typically posted in airport breakrooms, at access points, employee buses, and other areas where airport employees and tenants congregate.

The research found that airports also use posters, signs, booklets, handouts, fliers, or cards to increase messaging on airport rules and regulations. Airport security officials may post security marketing materials throughout public and airport secure areas, such as employee access control points, to provide employees with a visual reminder of security requirements and enforcement policies. The poster in Figure 2-1 from John F. Kennedy International Airport highlights the proper display of an airport badge and provides the phone number to the Port Authority of New York and New Jersey police to report instances of noncompliance.

Figure 2-1. Informational Poster



MAY 2019

Airport Security
ID Cardholder Responsibilities

Proper Display of Your Airport Security ID Card

Airport employees are required to challenge any unescorted person not showing an Airport Security ID card in the SIDA/AOA/Secured areas of the airport.

Proper Ways to Display Your Airport Security ID Card:

Below your neck and above your waist. On the outside of your outermost garment (shirt, jacket, coat, vest, etc.)
Visibly displayed at all times.

JFK JOHN F. KENNEDY INTERNATIONAL AIRPORT Call the JFK Port Authority Police 718-244-4333

AIRPORT COMMUNITY WATCH PROGRAM

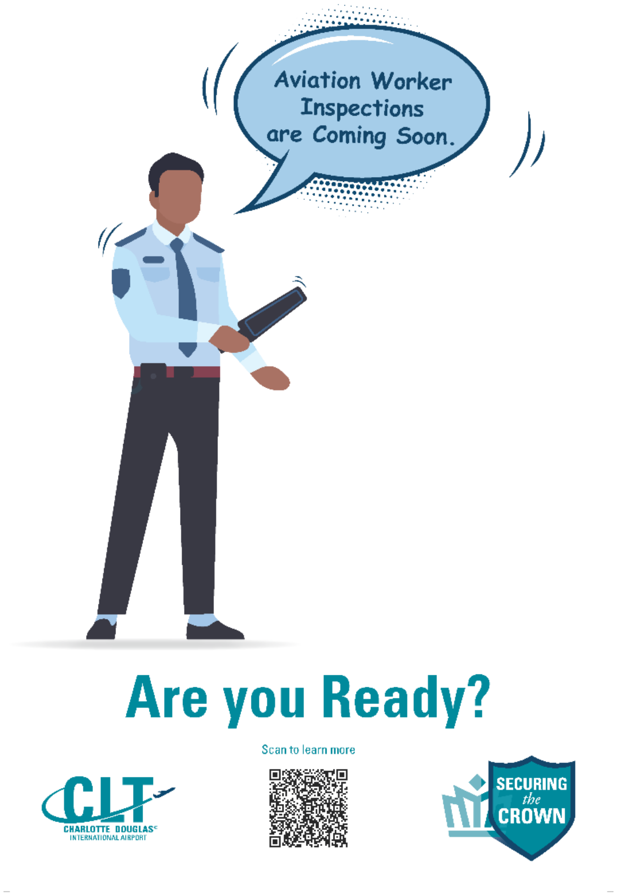
Airport Community Watch Program is jointly sponsored by the Aviation Development Council and the Police Crime Prevention Unit of the Port Authority of New York & New Jersey. Airport Community Watch Program is administered and managed by the Aviation Development Council, whose members include the scheduled airlines serving LaGuardia, John F. Kennedy and Newark Liberty International Airports.

May 2019 - Security Awareness Message

THE PORT AUTHORITY OF NY & NJ

Some airports provide pocket-sized, printed security booklets or handouts during the badging process for airport employees and tenant employees to carry for quick reference. Adding QR codes to posters, handouts, and badges also enables airport stakeholders to quickly refer to the airport rules and regulations or other important security information (Figure 2-2).

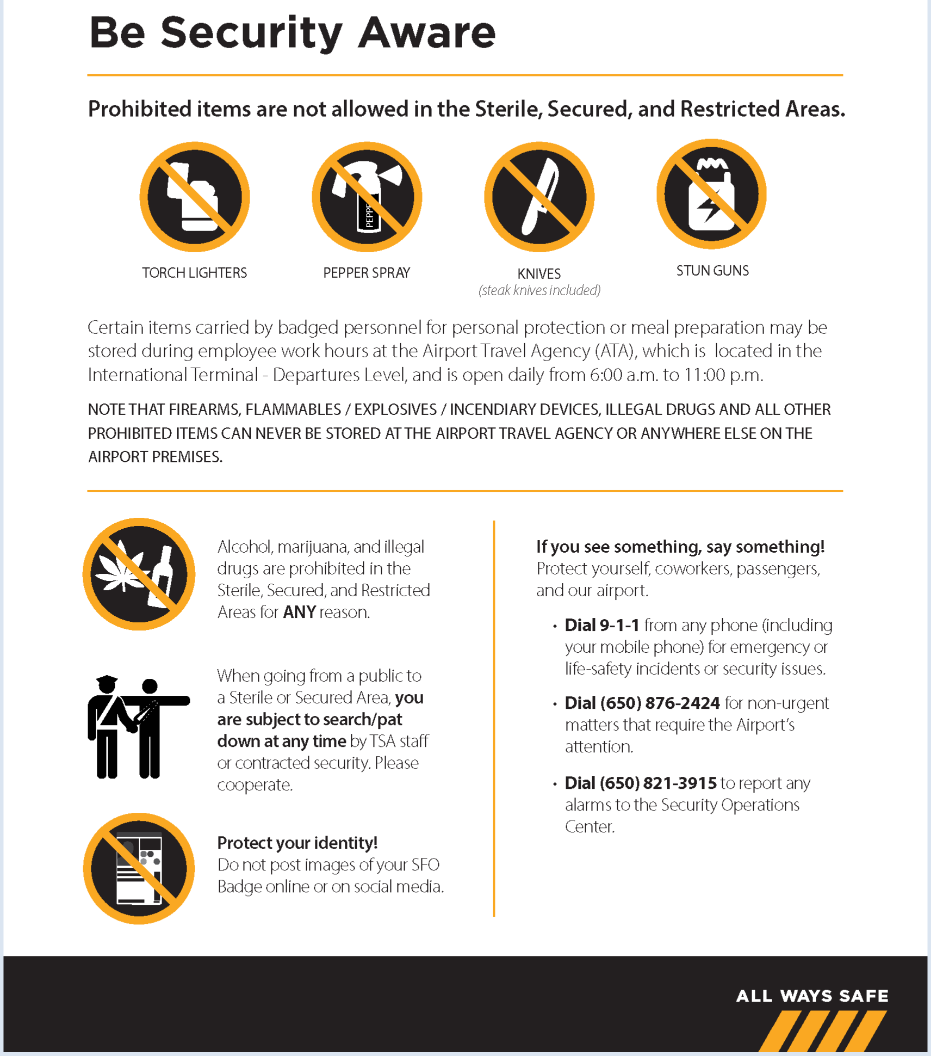
Figure 2-2. Flyer with QR Code


Aviation Worker Inspections are Coming Soon.
Are you Ready?
Scan to learn more
CLT CHARLOTTE DOUGLAS INTERNATIONAL AIRPORT
SECURING the CROWN

Security awareness newsletters, bulletins, and marketing materials can be distributed to airport employees and authorized signatories of tenants, lessees, agencies, and other organizations at an airport. The authorized signatory often serves as the primary point of contact for the airport to convey security-related matters and updates to airport security rules and regulations, and distribute security newsletters, bulletins, mobile applications, and other security messaging material.

SFO has created a Safety and Security Promotions Working Group to communicate and support the airport's security culture. The Working Group is tasked with creating campaign materials on specific security topics that are posted throughout the airport or given to airport workers. Figure 2-3 presents an example of a poster developed by the Working Group and posted on access-controlled doors.

Figure 2-3. Security Poster



Be Security Aware

Prohibited items are not allowed in the Sterile, Secured, and Restricted Areas.

TORCH LIGHTERS
PEPPER SPRAY
KNIVES
(steak knives included)
STUN GUNS

Certain items carried by badged personnel for personal protection or meal preparation may be stored during employee work hours at the Airport Travel Agency (ATA), which is located in the International Terminal - Departures Level, and is open daily from 6:00 a.m. to 11:00 p.m.

NOTE THAT FIREARMS, FLAMMABLES / EXPLOSIVES / INCENDIARY DEVICES, ILLEGAL DRUGS AND ALL OTHER PROHIBITED ITEMS CAN NEVER BE STORED AT THE AIRPORT TRAVEL AGENCY OR ANYWHERE ELSE ON THE AIRPORT PREMISES.

Alcohol, marijuana, and illegal drugs are prohibited in the Sterile, Secured, and Restricted Areas for **ANY** reason.

When going from a public to a Sterile or Secured Area, **you are subject to search/pat down at any time** by TSA staff or contracted security. Please cooperate.

Protect your identity!
Do not post images of your SFO Badge online or on social media.

If you see something, say something!
Protect yourself, coworkers, passengers, and our airport.

- **Dial 9-1-1** from any phone (including your mobile phone) for emergency or life-safety incidents or security issues.
- **Dial (650) 876-2424** for non-urgent matters that require the Airport's attention.
- **Dial (650) 821-3915** to report any alarms to the Security Operations Center.

The thirty-member interdisciplinary Working Group consists of airport team members from security, safety, compliance, facilities, and marketing who collaborate to update the security campaign messages and graphics each month, including changing posters on access doors to promote awareness of new topics and campaigns, such as prohibited items. This is an excellent example of innovation, collaboration, and creativity in promoting compliance with airport security regulations.

Most security messaging materials are distributed electronically through emails to the authorized signatories, who are expected to distribute the information to their badge holders. Some airports in this study use their mass notification systems to send messages about major security requirement updates to every badge holder enrolled during the initial badging process. The alert may be sent via text and/or email.

2.4.2 Fostering a Culture of Compliance

Security awareness and knowledge about rules and regulations can fade over time without recurrent training, knowledge checks, and other methods to ensure continued vigilance, commitment, and necessary knowledge levels. Additionally, institutional knowledge fades with high employee turnover. Airports participating in this study use a variety of techniques to maintain a high level of commitment and vigilance over time, such as rotating security notices posted at access points, delivering regular security compliance updates to tenant organizations, or rewarding correct and compliant security activities (e.g., conducting badge challenges, reporting security incidents).

Effective stakeholder engagement can be accomplished using multiple channels and is a powerful tool to deter complacency, build a committed workforce, and strengthen security culture. Many airports interviewed during this research have discovered complacency is a common root cause of security deficiencies and is directly related to compliance. The ability of an organization to deter noncompliance is reflected in the organization's compliance performance.

Continuous improvement and innovative practices that incorporate ideas suggested by stakeholders can help ensure that the airport community not only meets current regulations but is also prepared for future changes. MWAA's Airport Security Working Group (see Section 2.4.1.1 Security Meetings and Security Working Groups) is an excellent example of an airport engaging the community to examine and solve security issues and concerns.

The terminology used in developing airport security rules and regulations varies by airport and is tailored to the airport's specific culture, environment, and legal authority. Among the airports surveyed, it is common practice for airport security rules and regulations to contain unique provisions that optimize compliance by imbuing collective responsibility.

Some airports interviewed during this research designate each air carrier, licensee, tenant, vendor, contractor, or city/county department or division requiring access to the Secured or Sterile Area, and/or any other controlled areas as a "Participant in the ASP." This status imparts and imbues specific security responsibilities to participants, and each participant must remain in good standing in order to retain airport security privileges (e.g., access to secure areas).

This approach has served as an effective strategy to build collective responsibility amongst the participating organizations and entities, and the responsibilities and penalties for noncompliance are clearly prescribed. Example language is presented below.

> *"Each air carrier, licensee, tenant, vendor, or contractor requiring Security Badges shall become a "Participant" in the Airport Rules and Regulations, the ASP, and remain in good standing to retain airport privileges."*
>
> *"Each air carrier, licensee, tenant, vendor, contractor, or [City/County] department and/or division requiring access to the Secured Area, Sterile Area, and/or any other Controlled Areas shall become a "Participant" in the ASP, and remain in good standing in order to retain Airport Security privileges."*

These strategies help build a security culture intended for all members of the airport community to feel a shared responsibility for the security of the airport, as opposed to being a set of regulations set forth by others with which they must comply. Feedback loops with stakeholders support this shared responsibility by demonstrating that stakeholder participation is important to the growth and security of the airport. Instilling a sense of security ownership in the airport community will improve compliance.

2.4.3 Collaborative Problem Solving

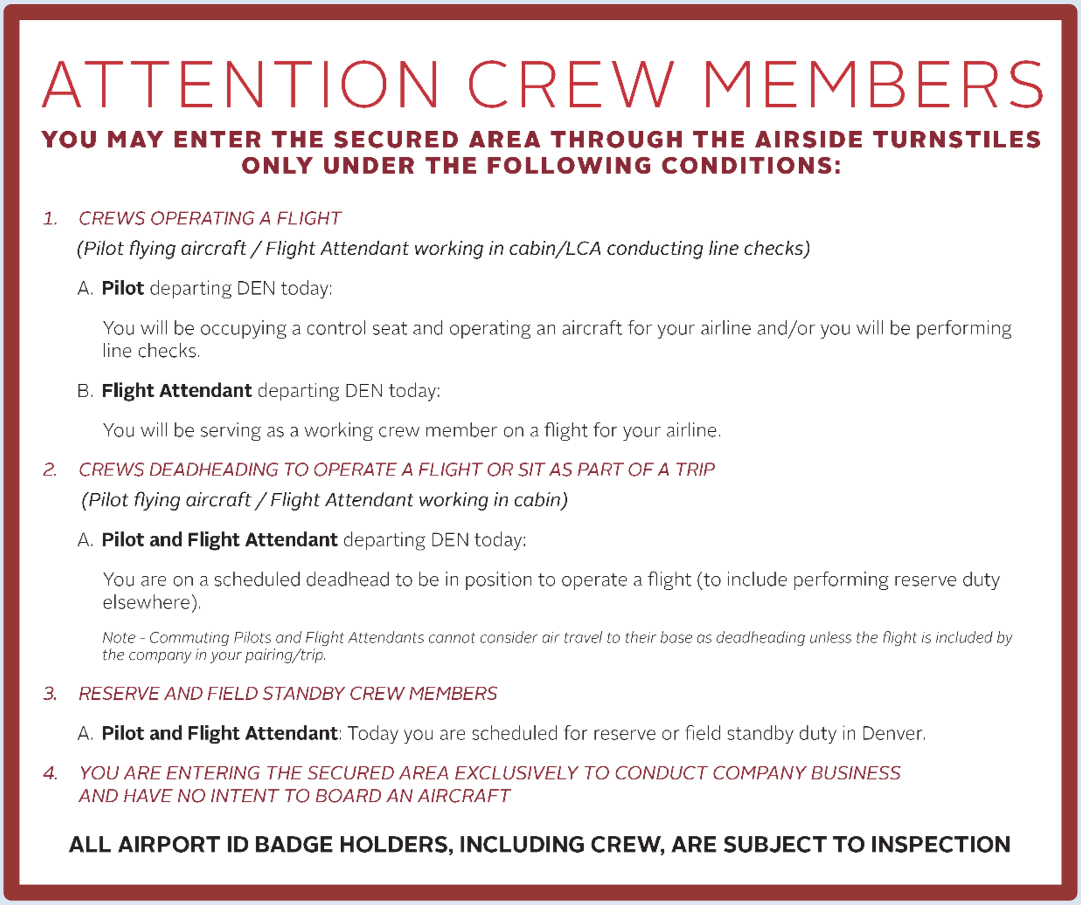
Airports can encourage collaborative problem solving by emphasizing local resolution strategies, leadership engagement, and community-wide security culture initiatives. It is in the best interests of all airport stakeholders to work together in resolving disputes about the application of airport security rules and regulations before the rules are implemented to improve compliance. Enlisting the participation of airport stakeholders and business partners can result in innovative and effective solutions to security issues and build unity of purpose.

Denver International Airport (DEN) discovered a rising trend in the number of crew members caught using the airport's employee access portals for personal travel, rather than utilizing a Known Crew Member portal. Airport security partnered with the chief pilot groups to develop a flyer (Figure 2-5) using crew member terminology to explain what travel was approved through airport-staffed employee screening portals.

In addition, the airport operator worked with airlines to explain and help them understand these rules, especially the expectation of wearing uniforms when on duty. The flyer was posted in the airside employee parking area, and some airlines displayed the flyer in their flight operations areas.

This strategy was effective because it used crew member vocabulary to describe the rules and clarified confusion between the crew members and the airport, and the responsible party took ownership of the initiative and corrective action needs. The flyer is an excellent example of collaborative problem solving that resulted in improved compliance and understanding for all.

Figure 2-4. Crew Member Travel Flyer



ATTENTION CREW MEMBERS

YOU MAY ENTER THE SECURED AREA THROUGH THE AIRSIDE TURNSTILES ONLY UNDER THE FOLLOWING CONDITIONS:

1. *CREWS OPERATING A FLIGHT*

   (Pilot flying aircraft / Flight Attendant working in cabin/LCA conducting line checks)

   A. **Pilot** departing DEN today:

   You will be occupying a control seat and operating an aircraft for your airline and/or you will be performing line checks.

   B. **Flight Attendant** departing DEN today:

   You will be serving as a working crew member on a flight for your airline.

2. *CREWS DEADHEADING TO OPERATE A FLIGHT OR SIT AS PART OF A TRIP*

   (Pilot flying aircraft / Flight Attendant working in cabin)

   A. **Pilot and Flight Attendant** departing DEN today:

   You are on a scheduled deadhead to be in position to operate a flight (to include performing reserve duty elsewhere).

   Note - Commuting Pilots and Flight Attendants cannot consider air travel to their base as deadheading unless the flight is included by the company in your pairing/trip.

3. *RESERVE AND FIELD STANDBY CREW MEMBERS*

   A. **Pilot and Flight Attendant**: Today you are scheduled for reserve or field standby duty in Denver.

4. *YOU ARE ENTERING THE SECURED AREA EXCLUSIVELY TO CONDUCT COMPANY BUSINESS AND HAVE NO INTENT TO BOARD AN AIRCRAFT*

ALL AIRPORT ID BADGE HOLDERS, INCLUDING CREW, ARE SUBJECT TO INSPECTION

Using collaborative problem-solving approaches can ensure broad stakeholder engagement and enhance compliance with airport security policies. Security protocols are greatly improved by including a wide range of stakeholders, from frontline staff to executives and legal advisors, in the development of security programs. Highlighting the importance of active participation, ongoing feedback, and targeted communication strategies will help cultivate a proactive and informed security culture.

2.5 Publishing Security Rules and Regulations

The process of approving and publishing airport rules and regulations is unique to every airport. The airport's governing structure, legal counsel, and security culture are just a few of the factors that impact how updates and revisions are reviewed, accepted, and ultimately published to the airport community.

Periods for public comment allow stakeholders the opportunity to provide feedback on the updates before they are formally published and put into effect. The comment period varies but is generally at least thirty days. For many airports participating in this research, this is the only opportunity the community of stakeholders will have to comment before publication.

SFO has a unique approach to ensuring airport stakeholders have an opportunity to provide feedback on new or revised rules and regulations. Throughout the year, the airport releases Airport Security Bulletins (ASB) drafted by the airport security department and attorneys and approved by airport executives and city attorneys.

The ASBs are typically issued with an expiration date of December 31 of the year they were issued and hold the same weight as an airport rule. Every October, the airport conducts a comprehensive review and update to the Airport Rules and Regulations, and at this time all ASBs issued during the year are incorporated into the Rules and Regulations document, as well as other changes that are requested by airport staff. The Airport Rules and Regulations document is redlined with the added ASB language and other proposed changes, and airport tenants comment any feedback or potential issues in the language. During this period, the airport hosts a "Page Turn Meeting" in which tenants, concessionaires, airlines, and service providers meet virtually to review and approve each page of the redlined copy. Sixty to seventy stakeholders are included in the process and are encouraged to bring up concerns or offer feedback on the ASB.

The city attorney makes final revisions to the redlined version and the document is sent to the airport commission for final approval. Once approved by the commission, the updated Airport Rules and Regulations are put into effect on January 1 of the following year, just after the ASBs expire on December 31.

Using this method has effectively promoted community awareness and knowledge of security requirements.

Some security rules and regulations are included in the badge application, mostly regarding disqualifying offenses, badge-holder responsibilities, and inappropriate conduct during the badging process. The badge applicant is required to read and sign their acknowledgement of the rules and regulations before submitting their application.

Among the airports surveyed, it is common practice, particularly for smaller airports, to print copies of their rules and regulations to be handed out during the initial badging process and the renewal process to ensure each badge holder possesses a copy for reference. This may be cumbersome for airports with a large badged population, and undesirable for airports committed to paperless processes. Additionally, reprinting to capture updates to the document can be costly and may result in several versions among the stakeholders.

Eugene Airport (EUG) provides physical copies of the airport's security rules and regulations to each tenant. When the document is updated, security personnel deliver the updated pages, both in person and electronically. This ensures that each tenant has received and is aware of the updates. This also provides the tenants with the opportunity to ask questions or clarify their understanding of their responsibilities.

Most airports participating in this research post their rules and regulations on their website. This provides all airport stakeholders with a readily available copy and eliminates the need to print hundreds or thousands of copies to hand out to badge holders. Including a link to the airport's rules and regulations can be a quick means to reference relevant sections when issuing notices of violation or responding to questions about the rules and regulations. Adding a QR code to airport-issued badges and posters that leads to the published document would enable badge holders to quickly refer to the rules and regulations.

The research found that many airport rules and regulations are published on the airport’s website as a PDF file. When the document is updated with new language, the version on the website is replaced. Since it is difficult to tell which sections have been updated in the new version, a good practice is to highlight changes and updates at the beginning of the document to help readers quickly jump to the updated sections. An example of a revision table that can be included at the beginning of the document is presented in Table 2-1.

Table 2-1. Example of a Revision Table

Date of Revision	Section	Pages	Revision

Some airports whose rules and regulations are codified in state or municipal ordinances have their airport rules and regulations posted to interactive websites (e.g., https://library.municode.com/ and https://codelibrary.amlegal.com/), which automatically track changes and version histories. These sites also support quick references, with links to each section in the table of contents.

SECTION 3: PROACTIVE COMPLIANCE MEASURES

Proactive approaches to compliance with airport security rules and regulations are critical to prevent regulatory issues and enhance the overall security of an airport. A proactive compliance program not only helps in adhering to regulatory and administrative requirements but also supports a security-aware culture that can effectively adapt and respond to evolving security needs and airport operations. A proactive approach is essential for organizations aiming to maintain high standards of compliance and integrity which, ultimately, leads to better operational outcomes and reduced security risk.

Additionally, a proactive compliance program provides a significant return on investment by avoiding administrative costs associated with corrective actions required when noncompliance issues are identified. Early identification and resolution of issues reduces the potential costs to the airport, tenant, and individuals.

The research identified several proactive approaches to security compliance. At the core of these efforts is the clear documentation and publication of security rules, regulations, and policies. These guidelines cover crucial operational aspects, such as the management of airport ID media, access control protocols, worker screening procedures, incident reporting mechanisms, and standards of acceptable conduct. By establishing and communicating these measures, airports ensure that all badge holders are fully aware of their roles and responsibilities within the security framework. This approach not only clarifies expectations but also underscores the potential consequences of noncompliance.

Flexible badging policies can be used to manage issuance periods, temporary badges, and visitor access. This supports access control requirements, lowers unaccounted for badges, and can be leveraged as a non-monetary consequence for noncompliance.

Robust and comprehensive training programs ensure badge holders are informed of the regulatory requirements as well as the airport's specific enforcement policies and procedures. This includes initial training required to obtain a badge, recurrent training when the badge is renewed, periodic and topical training to stay abreast of information and trends, on-the-spot and supplemental training for knowledge retention, and mandatory training as a result of noncompliance.

Incentive programs leverage rewards and recognition to highlight positive security contributions by airport workers. These are an effective mechanism to reinforce compliance, build community engagement, and support a proactive compliance posture.

Investigation, root cause analysis, data collection, and reporting can provide insight into noncompliance trends that can be used to develop proactive interventions and solutions. Addressing security issues based on these efforts, and developing necessary solutions, can prevent future recurrence.

Additional information on proactive compliance strategies can be found in PARAS 0049: *Creating and Maintaining a Strong Security Culture at Airports*.[1]

3.1 Badge Policies

Reduced renewal periods for airport badges can be used to improve accountability for tenants whose employees show repeated incidents of noncompliance. Requiring these tenants and their employees to

[1] **PARAS 0049:** https://www.sskies.org/images/uploads/subpage/PARAS_0049.AirportSecurityCulture_.FinalReport_.pdf

perform more frequent renewals (e.g., every six months or annually) may require them to also retake training more frequently, which can help improve knowledge retention.

Some airports interviewed during this research reduce the badge renewal period as a penalty imposed on tenant companies to encourage accountability on the part of the managers, supervisors, and authorized signatories. More frequent badge renewals require more time and effort on the part of the tenants, which should motivate them to improve compliance in their employees or badge management.

Many airports participating in this research require badge renewals every two years based on prior TSA requirements, although some require annual renewals for the entire badge population or specific tenant populations, such as concessionaires with high turnover. Once a trend in noncompliance from employees of a single company has been identified, the airport operator may reduce the company's badge renewal period. For tenants renewing every two years, the airport operator may require annual badge renewals until accountability improves. Reduction to a six-month renewal period may be used for tenants with especially egregious noncompliance, or those already required to renew annually. As the tenant demonstrates they can maintain the required level of accountability and compliance, these periods can be gradually increased to the standard renewal period.

A Port Authority–operated Category (Cat) I airport identified trends in noncompliance for its Sterile Area concessionaire badges. To help improve compliance, the airport required this population to renew their badges every two months for the first year. When the tenants proved they could comply with these requirements, the renewal period was extended to six months for the second year. After two years, the concessionaire population was allowed to return to the airport's practice of a one-year renewal period.

In many ways, using flexible badge renewal policies can be a burden on the airport. More frequent renewals require the badging office to perform more badging activities and tasks, which can further strain these busy operations. This strategy will also require careful management and tracking of the renewal schedules, which will be unique to each tenant. However, if the airport operator determines the badging office can manage the additional work, adjusting the badge renewal periods can send a clear message to tenants that noncompliance will not be tolerated.

Airports choosing to adjust badge renewal periods to improve compliance will need strong support from airport leadership. This strategy will increase processing costs for the tenant and may trigger resistance. Creating policies or rules that outline these policies, or including them in contracts and leases, can support the airport's legal standing.

Some airports interviewed during this research identified noncompliance with their temporary and visitor badge programs. These badges are usually issued daily, with a limited number of badges that can be issued a day, and with badges that are typically only authorized for set number of visits to the airport (e.g., thirty visits) or a limited period of time (e.g., two weeks). Airport tenants may abuse the program by using temporary badges for their employees waiting to be issued an airport badge, or those who have had a badge suspended. Internal databases that track this information can be valuable for identifying potential misuse of the temporary badge program. Use of the TSA's Secure Flight Program to vet individuals applying for a visitor's pass can also reinforce the integrity of the program and ensure high levels of security.

SFO's Visitor Pass badges have embedded chips that allow the badges to be swiped at badge readers similarly to an airport badge. Access for those under escort is only permitted at access points that are attended, such as passenger screening checkpoints or vehicle access points. While the badges have no access authority, visitors under escort are required to swipe their badge prior to entering the access portal. This transaction creates a record of the portals the visitor accessed, which tracks the visitor's movements and can help identify unusual behavior.

Visitors are permitted to be escorted through access-controlled portals a limited number of times. Once that limit is reached, the visitor must apply for an Airport ID badge for continued access to the airport restricted areas. Additionally, if the Visitor Pass badge is not returned when required, the card can be automatically deactivated. This action will send an alert to the security department if the badge is subsequently swiped at an access portal badge reader.

Violations of escort policies are a common challenge at many airports interviewed during this research. Typically, badge holders found to be in violation of escorting requirements will have their escort privileges revoked or suspended for a period of time.

Ontario International Airport (ONT) in California has improved their visitor pass program through two strategies. First, visitors are required to wear their visitor badge on their body in accordance with airport badge policies (i.e., above the waist, on outer garments, etc.). Second, the badge does not say "Visitor," but "Escort Required." This provides a visual indicator to other airport badge holders that the individual must be accompanied by someone with escort privileges. If the individual is found in the secure areas without an escort, badge holders are required to challenge the individual and call airport police.

Contractors are often issued badges to access secure areas of the airport to complete construction projects. This population often has shorter badge expiration periods, which helps control and manage the accountability of the authorized signatory who may have very little experience in the role. Among the airports surveyed, it is also common to set the badge expiration dates to the contract's expected completion date. This ensures that no badges remain active beyond the required period.

IAD has a section in its O&I that discuss the badge issuance periods for a variety of populations. Typically, badges are issued for a twelve-month period with the expiration date set to the badge holder's birthday. Other circumstances that may change the expiration date are included in the excerpt below.

> *"7.B. Some ID Badges may be set to expire prior to the individual's birthdate. ID Badges may expire on a date other than an individual's birthdate, under any of the following circumstances:*
>
> *(1) ID Badges for Contractor employees will expire on either the contract completion date or the birthdate of the employee, whichever is earlier.*
>
> *(2) If the badge holder has AOA driving privileges, the ID Badge may be issued to expire at the same time as the expiration of the individual's state driver's license.*
>
> *(3) Expiration dates of badges of those who are not citizens or permanent residents will not exceed dates of work permits, visas, or the immigration form under which the badge holder is covered.*
>
> *(4) ID Badge holders who have been issued a Customs Seal by CBP may have their expiration date set to the expiration of the Customs Seal.*
>
> *(5) For ID Badge holders who have been arrested and/or charged with a criminal offense which may be a disqualifier for unescorted access to the Security Controlled Areas and for which a final disposition is still pending; the ID Badge may be issued to expire one calendar day after the next scheduled court hearing."*

More information on alternative badging policies can be found in PARAS 0020: *Strategies for Effective Airport Identification Media Accountability and Control*.[2]

3.2 Stakeholder Training

Effective security training at airports blends practical knowledge with technical understanding to ensure compliance with security policies, rules, and regulations that cover a broad range of required topics. However, implementing a comprehensive security training program is not without challenges. The research found that airports often face issues such as information overload, which can overwhelm trainees and new employees; and resource constraints, which can limit the frequency and quality of training sessions. These challenges can be mitigated with streamlined training content, use of technology for efficient delivery, and use of outreach campaigns to supplement formal training.

The strategic impact of training programs extends beyond mere regulatory compliance. These programs play a vital role in proactively managing and mitigating potential security risks, thereby ensuring a secure and compliant operational environment. Adopting proactive and adaptive training strategies that address both immediate and evolving security needs will equip personnel with the knowledge necessary to effectively tackle challenges in a dynamic security landscape.

The continuous reinforcement of security protocols ensures that all personnel are equipped to uphold security standards effectively amidst the dynamic, and often challenging, airport environment.

A crucial element of successful training programs is fostering a culture of security that promotes continuous learning and testing. This involves recurrent training and knowledge checks for all personnel, including badge holders, authorized signatories, security and operations personnel, and other airport staff. Such initiatives must be supported by airport leadership and be well-adapted to the specific needs and contexts of the airport environment.

A city-owned Cat I airport has tasked their compliance team with dedicated community outreach to foster collaboration and promote security knowledge in the community. The outreach includes impromptu and informal quizzes and tests of airport worker security knowledge, as well as security training for new badge holders, and retraining to address spikes in violations or adverse trends at specific companies.

Tailoring approaches to security training can ensure that all personnel, especially those with security responsibilities, understand and can effectively implement security measures. Many airports interviewed for this study are transitioning from more generic security training videos and modules to courses and videos that more accurately represent their airport environment. This typically includes videos and images taken on site that show the various boundary lines, terminal layouts, and other particulars unique to the airport.

The research identified a trend among participating airports to develop targeted training courses for tenants that discuss highly specific security practices, such as piggybacking, tailgating, and vehicle searches for concessionaires. These are often required for certain populations in addition to the training required to obtain a badge. Flexible and responsive training modules that can be quickly modified allow the airport to assign courses on an as-needed basis, such as in response to a violation, new requirements, or findings from security audits and inspections.

[2] **PARAS 0020:** https://www.sskies.org/images/uploads/subpage/PARAS_0020.IDMediaAccountabilityControl__.FinalReport__.pdf

ONT has developed a series of flexible, add-on training modules to support compliance across thousands of airport badge holders. When it is determined that the badge holders need training on a new requirement, or remedial training to address an individual violation or trend in a certain violation type, the security department creates a short information packet with questions about the topic. This is then uploaded with the other airport training modules and assigned to badge holders as necessary. The process can be completed quickly, is available for any future incidents, and provides an effective means of demonstrating immediate corrective actions for the TSA.

Participating airports commonly conduct initial training using computer-based learning modules or in-person training sessions. Computer-based training can be useful for airports with many badge holders, as it allows the individual to take the training as needed or by appointment. Many airports in this study are moving to remote, online training for recurrent training requirements. Airports desiring to move their training online will require the approval of their TSA FSD.

Live, in-person training sessions are valued for their direct interaction and support for immediate feedback. While this format is more engaging and often more effective than computer-based formats, it can be difficult to schedule enough sessions to accommodate large numbers of badge holders. Interactive training sessions, such as role-playing exercises, with badge holders can reinforce procedure adherence and response tactics. This can be useful for building confidence to conduct procedures that require badge holders to step out of their comfort zone, such as badge challenges that require confronting another individual on security rules.

Tucson International Airport (TUS) developed a comprehensive approach to deploying its new aviation worker screening program. The badged population had many questions about the updated procedures, and the airport wanted to gain buy-in from all stakeholders before the new program was implemented.

To do this, the airport operator hosted demonstrations of the screening process using the equipment that would be deployed, and explained the new requirements to the airport stakeholders. Questions about the process were answered in detail. The stakeholders appreciated the demonstration, and the airport gained much greater buy-in from the badged population.

On-the-spot training and/or counseling is typically performed by those authorized to issue NOVs (e.g., security or operations personnel, compliance personnel, police) when a violation of an airport rule or regulation is observed. The counseling is tailored to the individual violator and the specific violation, focusing on what they did incorrectly and what they should have done to remain in compliance. This offers greater personalization compared to retaking the generic security training and aims to address the root cause of the violation directly and immediately. An NOV may be issued in addition to the training, or the individual may be issued a warning.

A Cat I airport has developed a peer training approach to help spread awareness of security requirements. Individuals who have been issued a violation will prepare a 5–10-minute presentation on the security rule they violated as part of their mitigation plan. The individual presents the information to their coworkers during the company's safety meeting. This creates accountability for the individual and refreshes the training for their coworkers. There are instances where the individual's manager has them present to all three shifts to maximize the information sharing.

A significant challenge in security training is the quick decline of knowledge, especially technical knowledge, which can diminish within a month of training. To combat this, airports can implement retraining programs to continuously assess and increase critical knowledge levels of the workforce before the knowledge effectively "expires." This is a proactive method way to identify and repair knowledge gaps before they become a security finding. Ensuring continuous reinforcement of critical knowledge translates to higher compliance levels and reduced operational risk. Science has shown that information is better retained when training sessions are repeated multiple times over a span of time, and when the knowledge checks are tailored to an individual's personal knowledge level versus a generic approach that uses the same content for everyone.

One potential option is to reduce the badge issuance period, which would require badge holders to retake security training more frequently. The research found that many airport operators utilize their regularly scheduled security meetings to share information and remind stakeholders of the security rules and responsibilities. Random quizzing of badge holders with counseling training can also create awareness for badge holders without the potential consequence of an NOV.

An Airport Authority–owned Cat I airport created an Airport Security and Safety Briefing checklist to provide awareness of the airport's rules and regulations (see Appendix A). The checklist covers key topics related to compliance with security and safety requirements, such as access portal security, violation reporting, and prohibited items. Managers are required to maintain a copy and review it with any new employees, as well as all employees returning from leave, to help remind them of security requirements as they step back into their role at the airport.

Artificial intelligence (AI) and cognitive science–driven knowledge retention apps are also becoming popular at airports to improve security awareness and knowledge preservation among airport stakeholders. The application is customized with airport-specific, on-demand training content designed to reinforce the airport's security requirements. It uses AI, machine learning, and predictive analytics to track each individual's personal rate of forgetting and provide knowledge checks of information that may have been forgotten. The stakeholders are periodically assigned quizzes on various security requirements, and the app provides light-touch knowledge checks that serve as instant refresher training for incorrect answers.

3.3 Incentive and Reward Programs

Incentive programs at airports can help improve security compliance and cultivate a positive security culture by leveraging both internal and external motivators to encourage desirable behaviors among airport stakeholders. These programs often involve recognizing stakeholders who actively participate in security measures, such as successfully passing a badge challenge test or reporting a violation. The airport operator will reward these stakeholders with a challenge coin, gift certificate, or other form of reinforcement that rewards compliance with airport security rules and regulations. These forms of acknowledgment can also provide motivation and positive reinforcement for airport employees to maintain knowledge of and comply with airport security practices.

The research identified various forms of recognition and rewards, including monetary and non-monetary incentives for exemplary actions in security situations.

PDX created the Helping Airport Workers Know Security (HAWKS) program to promote security awareness in its badged population. Badge holders who pass a challenge play or exceed expectations in advancing airport security are presented with a recognition certificate and entered into a monthly drawing for a $50 Visa gift card.

However, some airports are prohibited from gifting monetary rewards based on the governing jurisdiction's rules and laws. Creative, non-monetary rewards can also motivate airport stakeholders to be more security aware. Challenge coins are especially popular due to their limited quantity and collectability. Typically, the coins are stamped with the airport's name, year printed, and the program's name, and are given to airport stakeholders who report security concerns or correctly perform a badge challenge. The coins will require a small investment to print but can avoid concerns over monetary rewards. Other potential non-monetary rewards include:

- Public recognition at award ceremonies, on recognition boards throughout the airport, or in airport security newletters
- Preferred parking spaces for a limited time frame (e.g., one month, one quarter, etc.)
- Airport- or program-branded giveaways, such as pens, clothing, candy, and lapel pins

EUG has developed the Building Effective EUG Security (BEES) program (Figure 3-1) to improve security awareness and engagement across the airport community. The program includes training opportunities for airport stakeholders and a reward system for stakeholders who demonstrate security awareness. The operations department gives away EUG and BEES branded items (e.g., small pins and candy) to stakeholders observed performing badge challenges, reporting security concerns, and other security activities.

In 2020, EUG was recognized by TSA as the top airport among Cat II–IV airports for its leadership, dedication to employee empowerment, and collaboration with stakeholders. The BEES program was an important factor in this recognition.

Figure 3-1. EUG BEES

Presenting certificates at a public award ceremony can recognize airport stakeholders who have demonstrated exemplary dedication to airport security while also promoting the incentive program. These ceremonies can be lavish events held annually as a reward to the entire community, or they can be more subdued ceremonies held more frequently, and an accompanying news brief or article can be issued for the public. Regardless of the size of the ceremony, recognizing the stakeholder publicly for their success provides validation of the security program and encourages other stakeholders to participate.

Each year, SFO’s Safety and Security Promotions Group hosts the Annual Safety and Security Awards ceremony to recognize stakeholders who have contributed to the security of the airport. The All Ways Secure Excellence Award recognizes stakeholders for the development of a program, initiative, idea, or suggestion that improves security through compliance with the ASP and the airport’s rules and regulations, promoting and encouraging “If You See Something, Say Something” campaign, or proper badge display and challenge procedures. Stakeholders are rewarded with a trophy for their efforts.

3.4 Determining Root Cause

Effective root cause analysis (RCA) is crucial in airport security to systematically address and mitigate potential vulnerabilities and noncompliance. RCA helps identify the fundamental reasons behind security failures, which is essential to prevent future occurrences. This analysis is not tied to a single methodology, but rather incorporates various techniques suited to the complexity and nature of the issue. RCA is a continuous process that requires revisiting and refining solutions as new information becomes available, or as the operational environment changes.

For airports, RCA involves a series of steps starting with acknowledging whether the issue at hand is simple, complicated, or complex, as each demands a different level of RCA engagement. Simple problems may have basic fixes without extensive RCA, while complex problems may demand a thorough exploration of intricate cause-effect relationships that are dynamic and often unpredictable.

Boise Airport (BOI) has found great success in engaging with individuals who violate airport security rules to understand why they chose to perform the action (or inaction) that led to the violation. This discussion of the individual's rationale for committing the violation can help to identify the root cause of the incident as well as provide an opportunity for counseling training on the appropriate response.

The effectiveness of RCA is enhanced through collaborative efforts involving numerous stakeholders and systems. The RCA process should include diverse perspectives to ensure comprehensive analysis. Examining various interconnected elements—such as policies, processes, and stakeholder behaviors—should be the focus.

Airport operators participating in this research frequently include RCA findings in their mitigation strategies to ensure solutions address the identified root causes effectively. This may involve revising operational procedures, enhancing training programs, evaluating staffing resources, or adjusting security measures. The goal is to develop sustainable solutions that prevent the recurrence of the problem.

A Port Authority–operated Cat I airport conducts deeper analyses of root causes during the hearing process for repeat security violations. The hearings have revealed that security violations at the airport are most often attributed to inattention, carelessness, or misunderstanding. This is compounded by the challenges of high turnover worker populations, especially in management and low-wage positions.

The approaches to RCA reflect diverse strategies for understanding and mitigating the underlying causes of security violations. Some airports in this study prioritize RCA with a focus on direct interactions to understand individual actions, while others rely on system-wide evaluations or data analysis. Each method aims to identify the root causes in order to facilitate more effective and targeted measures to prevent future incidents. In some cases, an RCA will reveal a malfunction in a physical security measure, such as a faulty locking mechanism on an access door, although the most common causes are complacency and inattention.

TUS experiences strong winds that can blow open access doors that are not securely shut. The airport determined this was the cause of the rising trend in unsecured access door violations; airport stakeholders were not ensuring the doors were completely closed and secured before walking away, and the wind would push the door open. The airport operator added signage to the doors to remind the airport workers that they must push/pull the door every time to ensure it closes to avoid an NOV. Incidents significantly reduced after the signage was posted.

Security, operations, or compliance teams are often responsible for conducting RCAs to assess and evaluate existing processes that may be contributing to security violations. These individuals should be trained in the methods to conduct a proper RCA investigation that includes considerations for human factors that perpetuate noncompliance. Additional information on conducting RCAs at airports can be found in PARAS 0027: *Guidance for Root Cause Analysis in Aviation Security*.[3]

[3] **PARAS 0027:** https://www.sskies.org/images/uploads/subpage/PARAS_0027__RootCauseAnalysis_FinalReport.pdf

SECTION 4: METHODS TO IDENTIFY NONCOMPLIANCE

Once security rules and regulations are in place, airport officials must determine how they will identify and deter noncompliance. The research identified various methods and activities to identify noncompliance with security rules and regulations, such as dedicated compliance teams, reporting mechanisms, compliance inspections, and audits.

4.1 Compliance Teams

Personnel dedicated to compliance activities have the potential to completely change the airport's security culture, lessen administrative burdens, and reduce the number of violations and incidents. Several interviewed airports have dedicated teams of specialized staff, such as security operations specialists, security assessment teams, or audit teams who are focused solely on compliance and investigation of security incidents. Others assign personnel from operations and/or security to conduct inspections and audits and enforce compliance. Providing compliance or security staff with sufficient authority, training, and resources to conduct and manage compliance activities helps embed security compliance into the airport's security culture.

An Airport Authority–owned Cat I airport provides an opportunity for their security technicians, who are typically responsible for monitoring CCTV, to conduct patrols and inspections in the field. This allows the technicians to engage airport stakeholders during their patrols and support compliance activities. Compliance activities include patrols of the baggage claim during peak periods of baggage theft, inspections of vendor merchandise, and airside escorting inspections.

Regular training and guidance should be provided to staff responsible for conducting compliance inspections and audits to ensure they are up to date with the latest security practices, rules, and regulatory requirements. They should also be trained to understand the context of observed behaviors or security incidents through significance of time, place, and the individuals involved. The compliance staff should also be trained to provide reports that are detailed and contextualized, and address the credibility of the information

With or without dedicated compliance personnel, it is essential to define clear roles for security directors, compliance managers, contract security, and administrators who conduct security compliance testing activities. Defining these roles and responsibilities in the security rules and regulations can support enforcement actions.

4.2 Security Incident Reports and Forms

Transparent mechanisms for capturing security events or incidents and reporting them to airport compliance or security staff can aid in the documentation and analysis of security data and enhance accuracy and timeliness. Effective reporting processes convey to airport stakeholders that compliance practices are adhered to and executed properly.

Developing standardized forms, templates, and checklists for inspections and audits can help document observed behaviors or statements clearly and concisely, thereby reducing biases and memory-related errors. These standardized tools help ensure consistency and comprehensiveness in reporting incidents and noncompliance.

A Cat IV airport developed a Security Infraction Form (Appendix B) to address repeat violations by airline employees who are new to the airline industry and airport environment. The form documents the person's name, badge number, employer, date of incident, and the number of infractions by the badge holder. The ASM completes the form with the offender to discuss what errors were made, why they were made, and corrective actions to prevent future infractions. The discussion may include a review of the CCTV footage of the incident. The offender then signs the form to acknowledge the violation and commit to compliance in the future.

The airport has found that this discussion and form provide a personal and targeted retraining session that is far more effective than reviewing the entire SIDA training course.

Many airports participating in this research have implemented solutions that allow airport stakeholders and passengers to report observed security concerns directly to the security department. These solutions are often mobile applications or telephone numbers that allow for anonymous reporting. Printing the direct number to the security, operations, police, or other point of contact on the airport-issued badge encourages badge holders to report security incidents quickly.

ONT developed a digital security and airfield enforcement program to more efficiently comply with and enforce ASP requirements and the airport's rules and regulations. The mobile reporting application allows airport officials to perform a variety of 49 CFR § 1542 compliance reporting needs. The program ensures prompt and effective corrective actions are implemented for instances of noncompliance with security requirements, prevents repeated offenses of the same or similar violations, and mitigates identified vulnerabilities.

The *citation module* allows airport officials to issue NOVs from their phone. Officials can quickly address the issue, enter the report, and return to their daily duties more quickly. The system automatically sends a notification of the violation to the badge holder, their authorized signatory, and airport officials. Additional information, such as photos, witness statements, and CCTV footage can be attached to the NOV record to capture all the information in a single location.

The online portal allows authorized signatories to perform the following tasks:

- Review the citation
- Review the associated corrective actions prescribed by the airport, to include a violation hearing, remedial training, shift briefing, or administrative fine
- Upload proof that prescribed corrective actions have been completed

The *incident module* provides a record of all law enforcement responses required by 49 CFR § 1542.221. This module effectively documents all security incidents involving non-badge-holders that are not otherwise documented using the NOV citation, including perimeter events, incidents occurring at the TSA screening checkpoint, and incidents involving requests from an aircraft operator (e.g., interference with a flight crew).

The system automatically sends a notification of the incident to airport officials and TSA. This notification provides awareness of incidents to all concerned, allows for a hot wash and RCA, and supports the development of a corrective action plan to mitigate future incidents.

The *inspection module* allows airport officials to document and manage required inspections such as perimeter patrols, concessionaire inspections, and vendor deliveries. The application has positioned ONT to rapidly develop an AWS scheduling tool, AWS inspection record, and automated end-of-day email notification to TSA to report daily activity.

The badge verification module allows security personnel to access the system using their phone to enter a badge number and validate active badges. This has improved efficiency and effectiveness in the verification process, especially at direct access points without legacy access control infrastructure, such as temporary construction gates.

The *reference module* allows ONT to efficiently share security information with airport stakeholders based upon assigned user groups, including security, operations, law enforcement, authorized signatories, and TSA.

Frequently shared items include security awareness briefings to all user groups, and TSA-approved notice of changed conditions affecting security for airport officials and TSA.

The system is also used to track and analyze potentially vulnerable areas. The system generates reports that can be used to support implementing changes to respond to NOV trends. The system's query manager supports a monthly report of all incidents and inspections provided to airport officials.

ONT has a high-level collaborative working relationship with TSA. TSA is able to access the system to acquire critical information needed for their reporting and applicable investigations, without having to engage the airport with associated records requests. This level of transparency is based upon established trust and ONT's understanding that airports and TSA have one collective mission: the safety and security of the traveling public and the airport community.

4.3 Airport Security Compliance Inspections

In general, an inspection is an examination of a specific process, policy, or facility to determine compliance with governing standards (e.g., federal or airport requirements). Inspections often use checklists, observations, and tests to determine if requirements are being met, but do not typically delve into the root cause of noncompliance. Inspections often result in a "yes" or "no" answer to questions of compliance.

Airport security inspection activities can be targeted or random. Targeted inspections may be in response to incidents, complaints, or emerging threats, or may target airport compliance and enforcement resources towards specific higher-risk violations or tenants. More frequent and in-depth inspections may be conducted for stakeholders with higher noncompliance rates; and fewer inspections may be conducted for those that are consistently compliant. Criteria such as past compliance history and the seriousness of documented violations can be used to determine the minimum frequency of inspection activities for tenants. Some airports surveyed conduct random tenant audits each quarter, including of general aviation (GA) and cargo tenants.

The research found that airports conduct inspections to ensure compliance with established security rules and regulations and to safeguard against potential vulnerabilities. Some inspection activities conducted by interviewed airports include:

- Testing response times to access door alarms
- Testing the access control system (ACS) with a deactivated badge
- Accessing construction sites with inappropriate or missing credentials
- Attempting to piggyback through an access door
- Checking concessionaire knife logs
- Testing door and gate locks
- Monitoring vendor goods inspections
- Quizzing stakeholders on security requirements
- Inspecting AOA fences for damage, regulated signage, clear zones, etc.
- Inspecting vehicles at access points
- Monitoring for vehicles left unattended on terminal roadways
- Monitoring for unattended baggage in public areas of a terminal
- Verifying tool accountability in Sterile Area construction sites

These inspection activities can be conducted in-person by visiting targeted areas around the airport. Airport stakeholders may be approached or observed at a distance to test their behaviors or knowledge. The airport operator can also monitor sensitive areas remotely with CCTV to assess the behavior of personnel entering and exiting secure areas to avoid influencing their actions directly. Video tracking analytics can automate the identification and notification of security violations, allowing for real-time analysis, enhanced situational awareness, and quick responses to security violations. Often, unplanned or random inspections are conducted while security staff are patrolling the airport property.

IAD commissioned a Security Electronic Data Inspection System to document the security inspections conducted by the airport's contract security guards and other authorized representatives performing security compliance functions. The system uses a mobile application to guide the individual through a variety of inspection types using a series of decision-tree questions that capture information through the specific process. There are mandatory selections and data entry requirements, as well as sections for free entry notes and capture of photographic evidence for each inspection type being conducted.

When used by the security guards, the guard first logs in and chooses the appropriate workflow for the activity to be performed (e.g., merchandise inspection, vehicle inspection). The application presents a series of questions that require the guard's response. Based on the response, the application guides the guard through the next steps and/or correct actions. For example, responding "yes" to "prohibited item discovered?" will display next steps to notify the appropriate authorities and secure the item.

Many of the guards appreciate the ease of use of this job aid, although there was a learning curve when it was first implemented. Through the use of the system, the airport has the ability to monitor and ensure that the guards are performing all required steps during inspections. The airport operator anticipates further system improvements, specifically to the reporting options to help identify trends and potential vulnerabilities.

Prompt and structured follow-up actions ensure that corrective measures are implemented in a timely manner, thereby minimizing the risk of security vulnerabilities. In some cases, a more in-depth audit will need to be conducted to identify issues or potential risks.

4.4 Airport Security Audits

Security audits offer an opportunity to highlight potential areas for improvement and facilitate changes within a regulated entity. Audits tend to be more complex and comprehensive than inspections, with the intention of reviewing entire systems, processes, or departments to identify systemic issues.

An audit can take many and multiple forms, such as data sampling, interviews, document reviews, and checklists. They may also be conducted by multiple teams or departments reviewing multiple data sources, policies, and other documentation. Often, data gathered during inspections is reviewed to understand the various factors surrounding the issue being audited. Airports participating in this study use audits of tenants and other regulated entities to ensure security compliance and accountability. Audits generally involve examining inspection results, records, or processes to determine compliance with airport security rules and regulations.

The scope of the audit should be clearly defined, with objectives that are conveyed to the stakeholders, such as a reducing unaccounted for airport badges or updating the list of issued parking permits. The audit assessment should maintain a comprehensive audit trail to ensure objectivity. When auditing a tenant facility (e.g., cargo or fixed-base operator [FBO]), the assessment should include a survey of physical security measures and practices to ensure they align with the security requirements in agreements, leases, and airport rules and regulations, as well as any recent operational changes or regulatory updates. Auditing tenant leases, EAAs, and other contractual documents can ensure their language aligns with compliance requirements.

Regardless of the scope of an audit, effective communication strategies—including training, outreach, and feedback loops—are vital to improve tenant compliance and recordkeeping. Engaging tenants to discuss audit findings and collaborate on necessary corrective actions, penalties, or other remedial measures can underscore the importance of security compliance and continuous improvement.

Technology can be leveraged to enhance audit efficiency and effectiveness. Utilizing various data sources, such as access control records and archived CCTV footage, allows the airport to identify discrepancies, validate initial audit findings, and enhance the effectiveness of the overall audit process. Airports can add audio capabilities at critical access portals to provide security with the ability to listen to discussions between aviation worker screening personnel and aviation workers being screened. This can provide additional evidence when conducting investigations of security violations.

BOI has recently implemented a new system to improve the badge auditing process and reduce the number of unaccounted for badges. Previously, the badge audits were a manual, time-consuming process that required the Trusted Agents to call each authorized signatory individually and continually follow up with them to complete the audit.

The new system allows the authorized signatories to complete the badge audits using a mobile application on their cell phones. The signatory must enter each individual's badge number and a number unique to each issued card. This validation process requires the authorized signatory to touch each badge to enter the numbers, providing an additional level of quality assurance and accountability from the signatory.

The tenants have embraced the new system as it allows them to perform the audit anywhere and at any time. The application has increased the efficiency of auditing security badges, greatly reduced the number of unaccounted for badges, and improved the performance of the badge auditing process for the airport and their community.

Audits can be conducted routinely for detailed analysis or as needed to address immediate issues or repeat noncompliance. More frequent audits may be conducted for tenants with repeat noncompliance or poor management practices. Conducting random follow-up checks can ensure continuous compliance and deter noncompliance. Some airports interviewed in this study conduct random tenant audits each quarter, especially for their GA and cargo tenants.

A Cat X airport has included the following language in their rules and regulations that requires tenants with access-controlled portals to conduct regular audits of the cipher lock program in their area.

> *With respect to any cipher lock in the leasehold or control of any tenant, the tenant shall: ensure all cipher locks are properly maintained and operational at all times; conduct audits of cipher lock operability at least once per month; change cipher code locks in conformance with the Airport's schedule at least once per year; ensure that all access points providing direct access to Restricted Areas are closed and secured when not in use; immediately report to the Airport's Security Operations Center any cipher lock that is not functioning properly or any cipher lock code change.*

An audit often results in a report that may contain compliance findings, recommended improvements or enhancements, and potential risk factors. Documenting the process and findings of the audit is essential to transform the insights gained into tangible improvements in security protocols and practices. Moreover, follow-up actions facilitate a continuous improvement process by engaging tenants and security personnel in discussions about the findings and gathering their feedback on compliance challenges, which helps to enhance their understanding of and compliance with security requirements. This iterative process not only reinforces the airport's commitment to maintaining security standards but also builds a culture of accountability and vigilance among all stakeholders involved in the airport's operations.

Additional information on conducting audits and inspections of airport tenants can be found in PARAS 0020: *Strategies for Effective Airport Identification Media Accountability and Control* and PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*.[4]

4.5 Tracking Trends and Metrics

The research found that airports are increasingly leveraging technology to track security management and compliance measures and to create dashboards for easy monitoring. The gathered data can be analyzed to identify trends in specific violation types, locations, companies, and other factors.

Among the airports studied, violations and incidents are frequently tracked using Excel workbooks with tables and graphs to reflect current challenges and issues. Compliance personnel enter information about an incident into the workbook, such as badge number, company name, incident type, etc. This data can be manipulated with pivot tables, graphs, charts, data queries, and data filters to identify common factors and rising trends. While simple, this method can provide significant clarity to the level of compliance within the airport community. This information can be converted into reports to be provided to airport executives for continuous updates.

> An Airport Authority–owned Cat I airport has developed an enhanced Excel workbook to support NOV issuance. Incident reports are entered into the workbook, which then automatically populates an NOV template with the appropriate information (e.g., date, badge holder name, incident description). The NOV can then be forwarded to the badge holder and authorized signatory for next steps.

Information management platforms are another tool several airports use for tracking trends and analyzing security incident and violation data. The platforms are often integrated with multiple data sources (e.g., ACS, CCTV), and may be included as a module in the airport's identity management system (IDMS), although standalone, off-the-shelf products are often used by airports. The system allows the airport operator to enter incident and violation information, and then analyze the data to make informed decisions quickly, identify compliance gaps, and implement corrective actions for stakeholder companies with repeat violations. If integrated into an IDMS, incidents and NOVs can be attached to individual badge holders and companies to help manage and organize the information.

Whether using Excel workbooks, IDMS modules, or standalone platforms, airports measure stakeholder compliance through various metrics and key performance indicators (KPI). The most common metrics tracked through these systems include:

- Number of violations and type
- Percentage of unaccounted for badges
- Response time to door alarms

Many airports in this study have expanded their tracking capabilities within these systems to monitor additional metrics, creating performance goals for each. This helps the airport understand the effectiveness of new compliance initiatives and areas in need of attention. These additional KPIs can include numbers of:

[4] **PARAS 0020:** https://www.sskies.org/images/uploads/subpage/PARAS_0020.IDMediaAccountabilityControl__.FinalReport__.pdf
PARAS 0025: https://www.sskies.org/images/uploads/subpage/PARAS_0025.SecurityComplianceTenantFacilities_.FinalReport_.pdf

- Perimeter checks
- Door alarm tests
- Badge challenges
- Tests performed on contract security
- Facility inspections (e.g., FBOs, exclusive areas)
- Airport workers screened
- Issued temporary badges and/or visitor passes
- Prohibited items found

SAT has developed 27 KPIs used to assess how well the airport stakeholders are complying with the airport's security rules and regulations. One KPI tracks the number of TSA findings compared to the number of airport findings. This metric is a leading indicator that helps the airport determine if more compliance activities are needed to proactively identify incidents of noncompliance before TSA does.

Airports may find it beneficial to track how long it takes to complete certain compliance tasks. Time-bound goals for tasks such as issuing NOVs, completing investigations, and other compliance activities can help identify processes needing improvement, increase accountability, and provide critical metrics to support quality assurance.

A small, non-US airport established a KPI goal for the security team to prepare Corrective Action Reports with the identified root cause, and review these reports with the individual who violated a security rule and their authorized signatory within three business days of the incident. This internal accountability measure prevents accumulation of tasks and paperwork, ensures prompt remedial action, avoids the potential for incidents to be missed or overlooked, and creates a more responsible and streamlined process.

SECTION 5: VIOLATION, FINE, AND PENALTY STRUCTURES

Compliance and enforcement strategies are most effective when there is clear communication of rules and consequences, ensuring that all involved understand the repercussions of security violations. Often, penalty structures are outlined in the airport's rules and regulations and contain language that allows an authorized airport representative to adjust penalties on a case-by-case basis.

Airports use a variety of penalty processes that are tailored to their specific operational needs and security culture. Many airports in this study employ strategies rooted in classic deterrence theory, which suggests that behavior is influenced by the certainty, severity, and swiftness of penalties. Airports must also navigate local legal and political landscapes, which can affect the feasibility of certain penalties. Some airports surveyed opt for monetary fines, while many are not permitted to use fines and instead use non-monetary penalties, such as mandatory retraining or suspension of badges and access privileges

The research found that airports tailor their approach to penalties to fit their operational needs and security culture, employing a mix of immediate penalties and longer-term corrective strategies to enhance overall security compliance and address the underlying causes of violations. The variety of approaches reflect each airport's commitment to maintaining strict compliance with airport rules and regulations, often with an emphasis on education, progressive discipline, and the potential for severe penalties for more serious infractions, to ensure that all personnel understand the importance of compliance and the consequences of violations.

The research found that many participating airports employ tiered violation systems, where penalties are based on the severity of the violation and repeated offenses. Each violation type is assigned a tier and associated penalty for first, second, and sometimes third offenses. Tier I offenses may include piggybacking or other lesser infractions, with penalties ranging from suspension of badge privileges for a few days to a week, mandatory retraining, and potentially a small fine. Tier II includes more serious offenses, such as failing to report an arrest or bringing a prohibited item through security, and often results in badge suspension for up to a month, mandatory retraining, meetings with supervisors to develop a mitigation plan, and larger fines. Tier III is typically reserved for the most egregious offenses, such as allowing another individual to use their airport badge, and often results in revocation or permanent suspension of badge privileges.

Implementing graduated penalties that increase with repeated noncompliance can be particularly effective. Each subsequent penalty is designed to be more burdensome than the last, increasing the incentive for compliance. This structure helps mitigate the risk of penalties being viewed merely as a cost of doing business. It also emphasizes the importance of continuous improvement and helps reduce repeated mistakes.

Tiered violation systems are often presented as a matrix that shows penalties for all tiers and repeated offenses, such as the example in Table 5-1.

Table 5-1. Example of a Tiered Violation Matrix

	Tier I *e.g., piggybacking, incorrect display of badge, failing to report an unattended door, forcing a door, violations of smoking policies*	**Tier II** *e.g., bypassing security screening, incorrect escorting procedures*	**Tier III** *e.g., use of another's badge, duplication of airport-issued badge*
1st Offense	Mandatory retraining within 10 days Badge suspension for 7 days Penalty up to $50	Mandatory retraining within 10 days Badge suspension for 30 days Penalty up to $100	Possible revocation of Airport Badge
2nd Offense (and any subsequent Tier II or III offenses)	Mandatory retraining within 10 days Badge suspension for 15 days Meeting with ASM and Supervisor to develop mitigation plan Penalty up to $100	Mandatory retraining within 10 days Badge suspension for 60 days Meeting with ASM and Supervisor to develop mitigation plan Supervisor must take mandatory retraining within 10 days Penalty up to $150	
3rd Offense (and any subsequent Tier II offenses)	Mandatory retraining within 10 days Badge suspension for 30 days Meeting with ASM and Supervisor to develop mitigation plan Supervisor must take mandatory retraining within 10 days Penalty up to $150	Possible revocation of Airport Badge	

Some airports interviewed during the research use point-based violation systems. Similar to driver's license point systems, violation types are assigned a category, and each category is assigned a point value, with more severe violations assigned more points than minor violations. Accumulating a certain number of points within the airport's violation period (e.g., twenty-four months) will result in graduated penalties and can ultimately result in a suspended or revoked badge.

Point-based systems are often presented in a point accumulation schedule, such as the example in Table 5-2.

Table 5-2. Example of a Point-Based System

4 Points	6 Points	9 Points	12 Points
Mandatory retraining within 10 days	Mandatory retraining within 10 days Seven-day badge suspension	Mandatory retraining within 10 days Fifteen-day badge suspension	Possible revocation of Airport Badge

Offense Category	Point Value
Security Badge: Failure to display badge correctly; failure to challenge individuals not wearing a badge; using a badge that is expired or reported lost or stolen	**1**
Reporting: Failure to report a security or safety incident; failure to disclose an arrest; failure to report a failed badge challenge	**2**
Compliance with Procedures: Bypassing security screening; failure to secure, inventory, log, or audit Sterile Area prohibited items; authorized signatory violations	**3**
Unauthorized Access: Tailgating through vehicle gates; piggybacking through access doors; improper escorting procedures; failure to secure access portal before departing	**6**
Unacceptable Behavior: Damaging airport property; inappropriate conduct during the badging process	**9**
Significant Offenses: Using another’s badge or loaning a badge to another; duplication of an airport-issued badge; driving on the AOA without a valid driver’s license	**12**

Implementing a complex penalty structure may place a significant administrative burden on airport operators, as they must manage the assessment and collection of fines, enforce monetary and non-monetary penalties, and handle appeals. Airport operators should publish a description of the penalty system to ensure that determination of appropriate penalties and management of appeals or compliance processes is fair, transparent, consistent, timely, and effective. This should also include which roles may issue an NOV.

5.1 Accountable Parties

Penalties can be imposed upon tenant companies, company managers or supervisors, or individual badge holders, with some airports finding success in targeting all three populations to ensure effective enforcement and comprehensive compliance. This approach not only promotes fairness, particularly towards lower-wage employees, but also encourages comprehensive security practices that recognize that many security breaches are symptomatic of systemic issues within tenant companies, such as inadequate training or cultural misalignments.

Among the airports surveyed that issue monetary penalties to individual badge holders, these fines tend to be smaller and may be covered by the employer. The individual may be required to take mandatory retraining aimed at improving the individual’s awareness of their security responsibilities, and their badge may be suspended for a specific time. Without an active badge, the individual is typically not permitted to enter the secure areas of the airport, even with an escort. This limits the individual to working in public areas, which may not be an option. Loss of income as a result of a suspended badge can be significant for many stakeholders. Understaffed tenants will be further impacted by the loss of an employee. Some airport operators interviewed take these factors into consideration when determining appropriate penalties.

One Cat IV airport has developed an informal process to notify their airline tenant supervisor that a badge will be suspended before issuing the NOV. The airport has developed a strong relationship with this tenant and is aware of the impact to staffing when an employee's badge is suspended. Advance notice enables the airline supervisor to begin organizing staffing adjustments as soon as possible.

Company supervisor or manager penalties target those responsible for a badge holders who have committed certain violations. In these instances, the airport expects the managers to spread awareness of security requirements and share security information with their badge holders. Penalties may include badge suspension, mandatory retraining, and monetary fines aimed at enhancing management practices.

Company-level penalties often include significant fines, and may require the tenant to develop a company-wide compliance action plan in response to significant noncompliance by employees or auditing failures. By holding companies responsible for their employees' violations, airports aim to foster a more security-conscious corporate culture among all stakeholders. It also aims to create widespread behavioral change across the airport community, addressing issues from the company level down to individual badge holders through shared accountability. Company-level monetary penalties may need to be significant enough that they cannot be dismissed as merely an unavoidable cost of doing business.

MWAA has included language in their O&I that outlines the airport's authority to suspend or revoke credentials at the company level.

> ***Interference with the Operation of Reagan National or Dulles International.*** *The Airport Security Manager or designee may suspend or revoke the entity's ability to request ID Badges for serious or repeated, inappropriate behavior, whether criminal or not, that significantly interferes with the efficient and orderly operation of Reagan National or Dulles International (for example, failure to properly ensure that employees are complying with this O&I, failure to properly ensure that employees are operating in a safe manner).*

Overall, a flexible penalty structure supports a strong security culture within the airport by holding all parties accountable and emphasizing continuous improvement in compliance with security rules and regulations.

5.1.1 Population-Specific Measures

Population-specific measures can enhance compliance with security rules and regulations by tailoring strategies to different groups within the airport community to ensure effective security management.

The research found that many airport rules and regulations include descriptions of an authorized signatory's role and responsibilities as they relate to badge issuance and accountability. The rules may also include penalties against signatories for failing to meet these responsibilities, such as failure to collect and return badges from former employees.

DEN has created a section in their rules and regulations that describes the signatory's role, necessary qualifications, expected knowledge, and required training, as well as potential consequences for failing to follow the procedures described. An excerpt from the section is presented below.

> *20.03-3 The Authorized Signatory is the primary point of contact for Airport Security, and is responsible for the authorization of all Fingerprinting and Badging Applications, applicant identity verification, active*

and inactive Airport ID badges, vehicle permits, access changes, access control reporting, driving privileges, violation notices, active badge certification reports, and security key user agreements. The Authorized Signatory is also responsible for maintaining current contact information for the company as well as any other business relating to Airport Security.

20.03-4 Each individual designated by a Participant as an Authorized Signatory must successfully complete the following requirements in order to initially qualify, and to maintain qualification, as an Authorized Signatory:

a) Attend an initial Authorized Signatory training class and annual recurrent Authorized Signatory training.

b) Maintain an active Airport ID badge.

c) Submit and maintain an active Authorized Signatory Designation form.

20.03-5 Every Authorized Signatory is required to know the policies and procedures as they apply to their company:

a) Denver Municipal Airport System Rules and Regulations

b) Personnel Identification Systems

c) Systems Background Check

d) Procedures Airport ID Badge Training

e) Active Badge Certification Report

f) Vehicle Permit Procedures

g) Driver Authorization Training

h) Security Key Procedures

i) Audit Procedures

j) Violation Notice Response

k) Cipher Code Procedures

l) Sponsorships Requirements, if applicable

An Authorized Signatory who fails to follow these procedures may have his or her Authorized Signatory privileges and/or Airport ID badge revoked or suspended.

Imposing structured fines and penalties on authorized signatories or their company can have a significant impact on business operations, thus motivating them to stay in compliance. Penalties may include suspending the authorized signatory’s—or even the company’s—ability to process credentials with the airport badging office.

MWAA has included language in its O&I that defines the ASM’s authority and describes the criteria by which it may suspend or revoke the ability of an individual or entity (e.g., tenants, contractors, vendors) to request airport badges.

(10.B.2) Suspension and Revocation

i. Immediate Suspension without Notice

In the event of a serious violation including, but not limited to, those resulting in an imminent substantial threat to public safety or deliberate impeding of the operation of the Airport, the entity’s ability to request ID Badges may be immediately suspended without prior notice. Furthermore, the Airport Manager or designee may immediately and without prior notice suspend any or all access of some or all badged employees under the entity.

ii. Grounds for Immediate Revocation or Suspension

Serious or Repeated Security Violations. The Airport Manager or designee may suspend or revoke the entity's ability to request ID Badges for serious or repeated violations of federal security regulations, the Reagan National ASP, the Dulles International ASP, or Authority Regulations, including O&Is, that protect security at Reagan National or Dulles International (for example, failure to return Airport ID Badges in a timely manner, failure to respond to audits in a timely manner, or failure of the company to comply with security procedures).

Safety Violations. The Airport Security Manager or designee may suspend or revoke the entity's ability to request ID Badges for serious violations Authority Regulations protecting safety at Dulles International (for example, failure to comply with OSHA [Occupational Safety and Health Administration] rules, failure to obey traffic rules on the AOA).

Interference with the Operation of Reagan National or Dulles International. The Airport Security Manager or designee may suspend or revoke the entity's ability to request ID Badges for serious or repeated, inappropriate behavior, whether criminal or not, that significantly interferes with the efficient and orderly operation of Reagan National or Dulles International (for example, failure to properly ensure that employees are complying with this O&I, failure to properly ensure that employees are operating in a safe manner).

Many airports surveyed in this research utilize third-party contract security to perform various security and compliance activities around the airport. Descriptions of the roles and responsibilities for security contractors are typically included in the airport's post orders and contract with the company. The duties often include security inspections of vehicles, merchandise, and aviation workers, as well as badge checks and airport patrols. The contractors are not typically permitted to issue violations but are required to report incidents to the airport's security team, airport operations center (AOC), or operations department. However, some airports participating in this research outline the responsibilities of the contracted security force in the rules and regulations which will ensure the airport community is aware of their role and job responsibilities.

IAD's O&I have a section that outlines the roles and responsibilities for AOC personnel that can also be "delegated to the authorized security contractor." This provides the airport with more latitude to assign compliance activities to either the operations personnel or contract security as needed.

(5.B.) Airport Operations Center Personnel

Personnel assigned to the AOC are responsible for enforcing compliance with TSAR [TSA Regulations], the ASP, Authority Regulations and Dulles International's policies and rules including O&Is. The Airport Operations Center Personnel have the responsibility to:

(1) Conduct security checks on all of Dulles International's property including perimeter fencing, roadways, and the properties providing direct access to security areas. This task may be delegated to an authorized security contractor.

(2) Conduct random tests of controlled access doors, check for the proper display of ID Badges, and test for employee challenge procedures in the Security Controlled Areas and to maintain security awareness during routine patrol of Airport property. This task may be delegated to an authorized security contractor.

(3) *Conduct random open and look searches of employees' property, and/or other individuals prior to entering sterile, secured or non-public areas in accordance with TSA requirements. This task may be delegated to an authorized security contractor.*

Among the interviewed airports that utilize contract security, it is common practice to track and monitor the activities of security guards to ensure they are completing their security tasks to the level required in the post orders. This quality assurance review is often performed through CCTV or stand-off observation. Noncompliance is typically addressed through counseling, training, or revocation of the guard's airport badge, depending on the severity of the violation and whether it is a repeated offense.

Overall, using targeted approaches to enhance security compliance and adapting security measures for various airport groups can improve the airport's security posture.

5.1.2 Lease and Contract Considerations

The research found that airports use tenant leases and contracts to support and ensure compliance with security rules and regulations that are tailored to specific populations (e.g., FBOs, construction contractors). These documents often include provisions with general language that reference broader federal regulations, the ASP, and/or the airport rules and regulations that require security compliance. This approach avoids the need to frequently amend leases when specific security requirements change. The lease or contract requires the tenant or contractor to comply with current requirements in federal and local regulations.

Analysis of airport lease agreements revealed several enforcement measures airports use to ensure compliance. These include financial penalties for noncompliance or even termination clauses for serious breaches. Among the airports studied, lease agreements often contain provisions that hold tenants financially responsible for TSA fines resulting from tenant security violations. Some participating airports also reported requiring tenants to cover the costs of remedial actions when security standards are not maintained on leased properties. Such measures are designed to make tenants active participants in maintaining airport security standards, thereby extending the enforcement capabilities of the airport beyond its own operations to include all tenant activities. Adding language in the lease that penalizes the tenant for noncompliance using large fines can encourage diligence and accountability.

An Airport Authority–run Cat I airport has included language in concessionaire leases that authorizes the airport to transfer TSA fines levied for a security violation caused by the concessionaire company. The company may also require reimbursement for costs associated with correcting the security notice. The anonymized language from the lease is presented below.

> *If [Authority] incurs any fines and/or penalties imposed by the FAA or the TSA or any expense in enforcing Applicable Laws, as a result of the acts or omissions of Concessionaire, Concessionaire agrees to pay and/or reimburse all such costs and expense. Concessionaire further agrees to rectify any security deficiency as may be determined as such by [Authority], the FAA, or the TSA. [Authority] reserves the right to take whatever action necessary to rectify any such security deficiency, in the event Concessionaire fails to remedy the same.*

———

A Port Authority also holds leaseholders responsible for any costs incurred as a result of failure to fulfill the conditions in their lease agreement.

> ***<u>Section ##</u>*** ***Additional Rent and Charges***
>
> *(a) If the Landlord is required or elects to pay any sum or sums or incurs any obligations or expense by reason of the failure, neglect or refusal of the Lessee to perform or fulfill any one or more of the conditions, covenants or agreements contained in this Agreement to be performed by Lessee or on behalf Lessee or as a result of an act or omission of the Lessee contrary to the said conditions, covenants and agreements, the Lessee agrees to pay the sum or sums so paid or the expense so incurred, including all interest, costs, damages and penalties, and the same may be added to any installment of rent thereafter due hereunder, and each and every part of the same shall be and become*

> *additional rent, recoverable by the Landlord in the same manner and with like remedies as if it were originally a part of the rent as set forth in this Section.*
>
> *(b) For all purposes under this Section and in any suit, action or proceeding of any kind between the parties hereto, any receipt showing any payment of a sum or sums by the Landlord for any work done or material furnished shall be prima facie evidence against the Lessee that the amount of such payment was necessary and appropriate. Should the Landlord elect to use its operating and maintenance staff in performing any work and to charge the Lessee with the cost of same, any time report of any employee of the Landlord showing hours of labor or work allocated to such work, or any stock requisition of the Landlord showing the issuance of materials actually used in the performance thereof, shall likewise be prima facie evidence against the Lessee that the amount of such charge was necessary and reasonable.*

US airports are in a continuous state of improvement and may have multiple, ongoing construction projects (e.g., terminal modernization, roadway, expansion, baggage system enhancements). In many cases, a single construction project may be staffed by construction workers from multiple subcontractors. To streamline the badging process and improve accountability, some airports interviewed during this research require the construction group to designate a single authorized signatory for all the companies under the contract. The language governing these rules is not typically contained in the airport's rules and regulations but may be included in the construction contract or in special rules for construction contractors.

Airports participating in this research frequently include language in the construction contract that allows for fines and penalties to be levied against the construction contractor for failure to meet or comply with airport security and safety rules and regulations. These are often large fines or a portion of the contract amount to compel good management practices and compliance. The contracts also typically include language that requires the contractor to reimburse the airport for any fines assigned to the airport due to a security failure of the contractor, their subcontractors, or their security contractor.

Language in Punta Gorda Airport's (PGD) construction contract includes language to protect the airport from TSA and FAA penalties by requiring the contractor to comply with all airport security requirements.

> *The Contractor shall reimburse the Airport for the full amount of any fines placed on them due to negligence on the part of the Contractor or their Subcontractors. […] It is the Contractor's responsibility to prevent any breach of security within his area of construction or any route of entry to area of construction. All personnel having unescorted access to any security restricted area shall wear valid airport and contractor identification badges on their outer garments in such areas at all times to permit ready recognition by Airport Security. […]*
>
> *"Failure to comply with these requirements will result in the employee being escorted off the AOA and fines may be imposed at the Contractor's expense.*

Service contracts with third-party security providers typically contain penalties that can be levied against the security company, ranging from financial penalties to termination of the contract. Some airports surveyed allow construction contractors to subcontract a security company to conduct the vehicle and person inspections required in the contracts. The subcontractor must also meet all airport security requirements.

The involvement of airport property management (i.e., the department responsible for lease negotiation, execution, and compliance) and legal counsel in drafting and amending tenant and concession leases is crucial due to the potential legal complexities and risk of litigation. Legal oversight can ensure that leases not only comply with current laws and regulations but also provide airports with the necessary tools to enforce security measures effectively and anticipate new security regulations issued after the lease is executed.

5.2 Monetary and Non-Monetary Corrective Actions

Corrective actions and penalties typically include non-pecuniary penalties, such as mandatory security retraining, development of a corrective action plan, temporary loss of badging privileges, and occasionally badge suspension and revocation. Some airports participating in this research also issue monetary penalties to discourage noncompliance and cover administrative costs in the violation process. However, not all airports are permitted to levy fines as penalties based on their governing structure and local laws. Balancing punitive measures with educational and corrective actions allows airports to foster an environment where corrective measures are continuously reinforced and adapted to changing circumstances and behaviors to ensure the security and integrity of airport operations.

The research found that citations are not typically issued at the time the violation is discovered, such as during an inspection. It is far more common for the authorized personnel to issue a verbal or warning NOV, record the incident details in a report, and submit to the personnel authorized to issue formal notices. The incident is investigated using CCTV footage or other forensic data and an NOV is then issued. If the incident was discovered by personnel monitoring CCTV footage, a report is generated and submitted to the authorized personnel who issue a formal NOV after investigation.

IAD takes a proactive approach to enforcement activities both at an individual level and at the entity level. Citations may be issued at the time of the violation if the incident was observed by personnel authorized to issue a citation, or they may be issued based on the results of an investigation and corroborating information.

If the violation is discovered during an investigation such as CCTV inspection or some other reporting measure, the violator’s badge is suspended until a citation is issued. Once a citation is issued, the badge remains in a suspended state until all of the consequences for the violation (e.g., retraining, monetary penalty, minimum suspension periods) are met. This approach ensures swift action, maintains strict control over access privileges, and deters future security breaches. The airport rules and regulations authorize these actions through the language below.

> *(5.H) Employees who fail to comply with any requirement or responsibility are subject to Dulles International’s progressive security violation enforcement process that includes confiscation of the employee’s ID Badge, security retraining, increasing monetary penalties, and a three violation limit before an individual loses the privilege of having an ID Badge. Any enforcement action taken by Dulles International is separate and apart from any enforcement action which may or may not be taken by TSA for the same incident of noncompliance.*

Entity-level investigations and violations are handled by the ASM or one of the Alternate ASCs, and involve a formally documented process such as Letter of Investigation, Warning Notice, and NOV. While some investigations are closed through a Warning Notice, others move into a formal NOV with monetary penalties and Corrective Action Plans required of the entity. Through IAD’s proactive enforcement posture, entity-level investigations may result in monetary penalties from as little as $200 to cases that have over $300,000 in monetary penalties assessed based on the severity and magnitude of the violations discovered.

Some airports interviewed in this research take an approach that involves informal enforcement actions and warnings that only rise to the level of formal enforcement actions and penalties with repeated violations. Relying solely on punishment can lead to temporary compliance, which may revert once enforcement pressure is reduced. No-fault policies can support this effort. For example, if an individual mistakenly triggers a door alarm, they must contact security or operations and stand by the door until the alarm is resolved; as long as they do this they will not be issued an NOV, but they may receive on-the-spot counseling.

ONT differentiates between minor infractions and more serious violations. Badge holders who trigger a nuisance alarm are issued a counseling violation (COU), which is similar to a warning, and given on-the-spot training. COUs do not require a violation hearing or a fine, although a record is made of the incident in the airport's violation tracking database, and the respective authorized signatory is sent a copy of the COU for situational awareness and to support stakeholder shift briefings.

Depending on the seriousness of the violation, or if the incident is a repeat offense, the airport can elevate the incident to an NOV, which would require a violation hearing, remedial training, potential administrative fines, and badge suspension or revocation.

The COU process allows for a documented progressive action program that tracks the offender's compliance history and the severity of the incident, which is considered prior to the determination of corrective actions. This model best demonstrates ONT's progressive action philosophy, which aligns with the violation structure contained in the airport's rules and regulations.

Continuous evaluation of penalties for violations can help the airport determine whether the measures are effectively reducing noncompliance. Adjustments may be necessary based on tenant feedback and observed changes in behavior. A responsive approach allows airports to adapt their strategies to achieve the best results.

Proper documentation is crucial for supporting the enforcement of penalties. This includes detailed records of training sessions, interactions regarding rules and responsibilities, and logs of violations with relevant details. Such documentation will help justify penalties when they are challenged and ensure transparency and fairness in enforcement practices.

5.2.1 Non-Monetary Penalties

For airports that lack the authority to issue monetary penalties, or where the issuance of fines is overly burdensome or not feasible, a variety of non-monetary penalties can be used to enforce compliance, such as temporary badge suspensions, mandatory retraining, or shortening badge renewal periods for airport workers or tenants. The issuance of non-monetary penalties should aim to educate and guide towards proper behavior, including training and clear communication of expectations, rather than punishment.

Non-monetary penalties are usually easier to implement and adjust than monetary penalties, especially in jurisdictions where levying fines is limited by local laws or involves complex administrative procedures. The flexibility of non-monetary penalties allows airports to swiftly adapt their enforcement strategies to emerging challenges and compliance trends. Including language that allows the airport to adjust penalties based on mitigating and aggravating circumstances can support this flexibility.

PDX has included language in its airport rules and regulations that allows the ASC and Violation Panel to adjust penalties for a violation based on the circumstances of the incident and the individual's history of violations.

> ***(17.5) Badge holder Penalties*** *The "Enforcement Matrix," is a guideline to be used by the Aviation Security Department and the Airside Operations Department for issuing penalties for substantiated Security Violations. Although the Enforcement Matrix will generally be followed in most cases, the penalties given for some Security Violations may vary from the Enforcement Matrix, depending on the nature of each specific Security Violation, the timing of its occurrence and if, in the reasonable opinion of the ASC or of the Airside Operations Department, a variation from the Enforcement Matrix is warranted by the findings of the Security Violation investigation. All penalties imposed are in addition to any other rights or remedies available to the Port.*

It should be noted that implementing non-monetary penalties also requires additional administrative effort, such as conducting additional training sessions, managing additional meetings with tenants, and reviewing corrective action plans. These measures may require increased support from airport leadership and, potentially, additional resources to effectively administer and enforce.

Airports can issue non-monetary penalties to stakeholder companies with high rates of noncompliance, such as limiting the privileges of authorized signatories to request new badges or requiring the development of a corrective action plan by the violator and/or the violator's employer. These measures encourage companies to adopt better management practices. Airports may also need to increase the severity of penalties or vary the timing and focus of enforcement efforts to keep individuals and companies vigilant and motivated to comply.

PDX has included language in the airport rules and regulations that allows for the suspension or revocation of a tenant company's ability to request new badges and/or the suspension of badges for all the tenant's employees. There is also language that permits the ASC to waive this penalty.

> ***(17.2) Suspension or Revocation of an Employer's Access Privileges***
> *Upon either suspension or revocation of an employee's access privileges, the Port may deactivate and/or confiscate any or all PDX Security Badges held by the affected employer, including the PDX Security Badges of all employees, contractors and agents whose access privileges were authorized by that employer. All affected Badge holders must immediately surrender any PDX Security Badge authorized by the employer to the Security Badging Office or Port Police and, if a Badge holder is within Restricted Areas at the Airport, leave the Restricted Areas. The Port may also cancel the affected employer's ability to request the issuance of PDX Security Badges, unless waived by the ASC.*

5.2.2 Monetary Penalties and Fines

When developing a monetary penalty system, airport operators must consider whether they have the authority to enforce and levy monetary penalties and collect the fines. The ability of an airport to impose or alter monetary penalties may be limited by state and local laws.

Airport operators should seek to ensure that enforcement penalties are proportionate to the severity of the violation and the context of the violator's actions. Monetary penalties and fines should be designed to not only deter the badge holder involved from repeating the misconduct but also to serve as a warning to others to promote a culture of compliance across all airport workers.

SAT has created a list of monetary penalties that badge holders can incur for violating or failing to comply with security rules and regulations.

> ***Security access and control charges.***
> *(a) The aviation department shall implement the charges airport identification media at [Airport] set forth below. These rates shall remain in effect unless amended by action of the city council as may be necessary from time to time. The following charges are inclusive of sales tax payable to the state: […]*
>
> *(4) Unaccountable airport identification (ID) media (lost, stolen or non-returned): $150.00.*
>
> *"Employers will be assessed and are responsible for paying the above fee for any unaccountable airport identification media for which they are designated sponsor in the system. In the event that an airport identification media, which has been previously reported as unaccountable, is returned to the airport badging office within thirty (30) days after such airport identification media was deemed unaccountable. The city shall refund the employer one hundred dollars ($100.00) if the employer has paid the one hundred fifty dollar ($150.00) fee.*

Employers are encouraged to return the airport identification media even after the thirty (30) days.

(5) Badge and ID missed appointment fee: $25.00

"The following constitutes a missed appointment:

a. Arriving fifteen (15) minutes after scheduled appointment.

b. Failure to arrive at the scheduled date or time of appointment.

c. Failure to present all required documents for scheduled appointments. […]

"Applicants or authorized signatories must notify the badge and ID office […] of cancellations twenty-four (24) hours prior to the date and time of the scheduled appointment.

(6) Airport identification media reactivation fee after security violation[5]:

First offense: $25.00

Second offense: $50.00

Third offense: $75.00

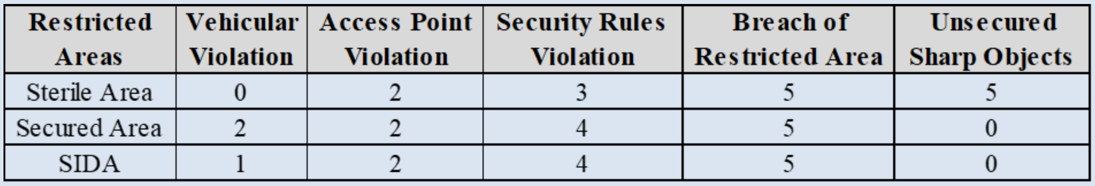
Fourth offense—Airport identification media issuance/reactivation will be denied. […]

(8) Progressive security enforcement fee: Ten dollars ($10.00) × frequency × severity factor as described in section […].

The airport has also published the formula used to determine the progressive security enforcement fee incurred after being issued an NOV.

> ***Progressive security enforcement fee.*** *The progressive security enforcement fee shall be determined by multiplying the frequency and severity of the security violation, by a ten-dollar ($10.00) baseline charge (i.e., fee = $10.00 × frequency × severity factor). The severity factor is determined by the location and the type of the offense. [Airport] has three (3) designated restricted areas: the sterile area (inside the terminals but beyond the TSA security checkpoint), the secured area (outside the terminals near the commercial aircraft), and the security identification display area (SIDA, the entire AOA). The types of security violations are grouped into five (5) major categories: vehicular violations, access point violations, security rule violations, breaches of the restricted area, and unsecured sharp objects. The table below indicates the severity factor by location to be applied in the formula.*

Severity Factor by Location



Restricted Areas	Vehicular Violation	Access Point Violation	Security Rules Violation	Breach of Restricted Area	Unsecured Sharp Objects
Sterile Area	0	2	3	5	5
Secured Area	2	2	4	5	0
SIDA	1	2	4	5	0

The size of fines should be carefully considered and discussed with legal counsel. Large monetary penalties for significant security violations may lead to pushback from the airport community, underscoring the need for robust outreach and education strategies to clarify airport priorities, responsibilities, and the repercussions of noncompliance.

Conversely, small fines may create a mindset that paying the fine is an easier option for the organization than complying with rules.

[5] Note: media issuance/reactivation can be denied after the first offense depending on the severity of the violation.

Where possible, the levy of fines should be flexible based on aggravating or mitigating circumstances. This is often enabled in the rules and regulations by using language that provides the airport with discretion to reduce or eliminate fines based on the specific circumstances of each violation, or to hold the tenant company responsible for repeat or severe violations.

SFO's rules and regulations contain language that allows levying of fines against a violator's employer. This enforcement mechanism is designed to place more accountability on the tenant company or contractor for the actions of their employees.

> ***(14.2) General and Administrative Fines*** *Any person or business entity violating or otherwise engaging in prohibited conduct under these Rules and Regulations may be subject to general and/or administrative fines as provided under this Rule 14. If the violator is an individual employee or agent of an Airport tenant or contractor, the fine may be assessed against the employer/tenant or contractor at the Airport's discretion.*

The effective management of monetary penalties in airports requires a balance between deterrence, flexibility, education, and accountability for individuals and tenant companies. The strategies range from punitive fines to encouraging compliance through mandatory retraining, with varying degrees of discretion in the application of these penalties.

5.3 Security Violation Hearing Process

Security violation hearing officers and panels adjudicate legal responsibility of the party issued an NOV (respondent), or offer the respondent an opportunity to present and/or appeal their case before a hearing officer or panel.

Depending on the rules and regulations and authority granted, hearing officers and panels may adjust penalties based on mitigating and aggravating circumstances. These hearings can be mandatory for all or select violations. In addition to the statements from the respondent, the hearing process may also include statements from the respondent's employer and the ASC.

Some hearings require the respondent to appear in person at a scheduled date and time before the hearing officer, panel, or similar body, which may be composed of airport and/or city representatives. The hearing officer or panel will review the facts of the case; elements of the applicable security rules and laws; testimony of the respondent and witnesses; written statements; and evidence including CCTV, ACS, and records to determine responsibility of the respondent and to dispense appropriate consequences.

This body often has the authority to amend the violation, reduce the amount of statutory fines, assign a monetary penalty appropriate for the violation, and/or assign non-monetary penalties such as mandatory security retraining. Airport legal counsel, security and/or operations personnel, the ASC, and the Airport Director may participate in the hearing process in some capacity, in accordance with the governing laws of the administrative hearing and appeal process.

A Cat I airport has detailed the authority review procedures in the airport rules and regulations, including the steps required to answer the NOV charge, penalties for failing to appear before the Hearing Committee, and actions the Hearing Committee is authorized to take to eliminate, mitigate, or modify the violation penalties based on the explanation and mitigating facts presented.

> *If the Hearing Examiner/Committee determines that the explanation mitigates the fact that the person committed the infraction, the Hearing Examiner/Committee may eliminate or reduce the amount of the assessment or fine arising out of the infraction or order an alternate penalty.[…]*

The addition of other departments to the panel can help ensure that corrective measures are well-coordinated and tailored to each specific case, with a focus on resolution, compliance reinforcement, and consistent application of the penalty system.

Fort Lauderdale–Hollywood International Airport has an innovative security hearing process that leverages a collaborative, problem-solving model to address security violations. The airport solicits senior-level management representatives from the airport community, such as airline managers, service company managers, and other entities, to serve on the Monthly NOV Panel as disinterested parties. This body is charged with hearing all NOV appeals, and typically three cases are scheduled on the docket each month. The composition of the Monthly NOV hearing process incudes the three-member panel, the Assistant Director of Security who presents the county's position, and an attorney from the county legal department who observes the process to ensure that the proper procedures and due process are administered.

Panel members are provided with specific training to understand their role and responsibilities, and core knowledge needed to serve in this capacity. The panel excludes members of law enforcement and representatives of the violator's employer to avoid bias in the decision-making process. The cross-organization composition of the panel not only provides an impartial judgement on the case but also serves to educate members of the airport community on the security requirements for all airport badge holders. Participating in the NOV appeal hearing process, listening to the facts of the case, and determining responsibility heightens the security compliance and commitment of the airport community.

SECTION 6: LESSONS LEARNED FROM SAFETY PROGRAMS

Some airport operators participating in this research have incorporated lessons from safety programs into the development and enforcement of their security rules and regulations. A collaborative problem-solving approach that emphasizes transparency and engagement, and uses root cause analysis to examine and address violations of security regulatory standards, supports a more proactive and engaged compliance program.

The FAA has developed their Compliance Program[6] approach and Just Culture Initiative[7] to promote the use of on-the-spot corrections, counseling, and additional training designed to reinforce compliance with safety regulations and address underlying causes of deviations. Recognizing that a non-punitive approach to resolving noncompliance can lead to better security outcomes, FAA encourages airports to self-disclose safety violations.

The FAA has also integrated Risk-Based Decision Making into its strategic initiatives, using data to proactively identify and address safety risks before they lead to incidents or accidents.

Airports can incorporate lessons from safety approaches by encouraging open and non-punitive information sharing and mutual cooperation through self-disclosure and correction of security issues. Lessons learned from the FAA's Compliance Program and Safety Management System (SMS) can be adapted to the security realm to support a more responsive, responsible, and flexible operating environment in which proactive measures and continuous engagement lead to sustained compliance and security enhancement.

PGD has integrated the SMS structure into investigations performed on security violations. The safety and security manager conducts interviews with all parties involved, investigates the incident using RCA methods, and generates the violation report. If a root cause is determined, the manager provides this information and feedback on any other findings to all parties involved in the incident as part of a feedback loop to ensure effective communication. The airport requests a mitigation plan and proposed actions to correct the security violation and prevent future incidents of a similar nature. The safety and security manager reviews and approves the plan, provides additional direction as needed, and establishes a timeframe for implementation.

The Security Management System (SeMS) approach incorporates many lessons from its SMS counterpart. SMS provides a framework and principles that can be modeled to integrate security into business operations and the organization's culture, build and reinforce quality assurance processes, and implement mechanisms to continuously assess and manage risk in a systematic, proactive, and precise process. See PARAS 0009: *Guidance for Security Management Systems (SeMS)* for more information on establishing and maintaining an SeMS.[8]

[6] https://www.faa.gov/about/initiatives/cp
[7] https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/air/transformation/csp/initiatives/initiative_3
[8] **PARAS 009:** https://www.sskies.org/images/uploads/subpage/PARAS_0049.AirportSecurityCulture_.FinalReport_.pdf

REFERENCES

ANSER. (2021). *Guidance for Root Cause Analysis in Aviation Security* (PARAS 0027). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0027__RootCauseAnalysis_FinalReport.pdf.

Arup. (2018). *Guidance for Security Management Systems (SeMS)* (PARAS 0009). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0009SeMS_Guidance-Final.pdf

Barich. (2017). *Enhancing Communication & Collaboration Among Airport Stakeholders* (PARAS 0003). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0003.C2Guidebook.FinalReport.pdf.

Cadmus Group. (2023). *Creating and Maintaining a Strong Security Culture at Airports* (PARAS 0049). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0023_ExitLaneStrategiesTech_FinalReport.pdf.

Duncan, Caroline. (2024). "Communicating New Policies and Procedures Sample: 7 Tips and Sample Email." DeskAlerts. https://www.alert-software.com/blog/company-policies-effective-communication.

Duncan, Caroline. (2022). "Ensure Compliance With Bank Policies and Procedures". DeskAlerts. https://www.alert-software.com/blog/ensure-compliance-with-bank-policies-and-procedures.

Federal Aviation Administration. (2022). *The FAA's Compliance Program*. Safety Analysis & Promotion Division.

Hyperproof. (2022). "The Journey to Compliance: Why You Should Start Now (and How to Get Started)." https://hyperproof.io/resource/compliance-journey/.

Hyperproof. "The Compliance Maturity Spectrum." https://hyperproof.io/compliance-maturity-spectrum/.

Faith Group. (2017). *Employee Inspections Synthesis Report* (PARAS 0006). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0006.Employee_Inspections.FinalReport.pdf.

Kusserow, Richard. (2020). "Compliance Program Maturity Models." Journal of Health Care Compliance. September-October 2020.

LAM LHA. (2019). *Strategies for Effective Airport Identification Media Accountability and Control* (PARAS 0020). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0020.IDMediaAccountabilityControl__.FinalReport__.pdf.

MISO. *Compliance Maturity Model – Process Level*. https://assets.corporatecompliance.org/Portals/1/PDF/Resources/past_handouts/Utilities-Energy-Compliance-Ethics/2013/Tuesday/TGS3handout.pdf.

National Air Transportation Association. (2009). *Airport Sponsors Guide to Minimum Standards & Airport Rules and Regulations.*

Salus Solutions. (2021). *Insider Threat Mitigation at Airports* (PARAS 0026). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0026_InsiderThreatMitigation.FinalReport_.pdf.

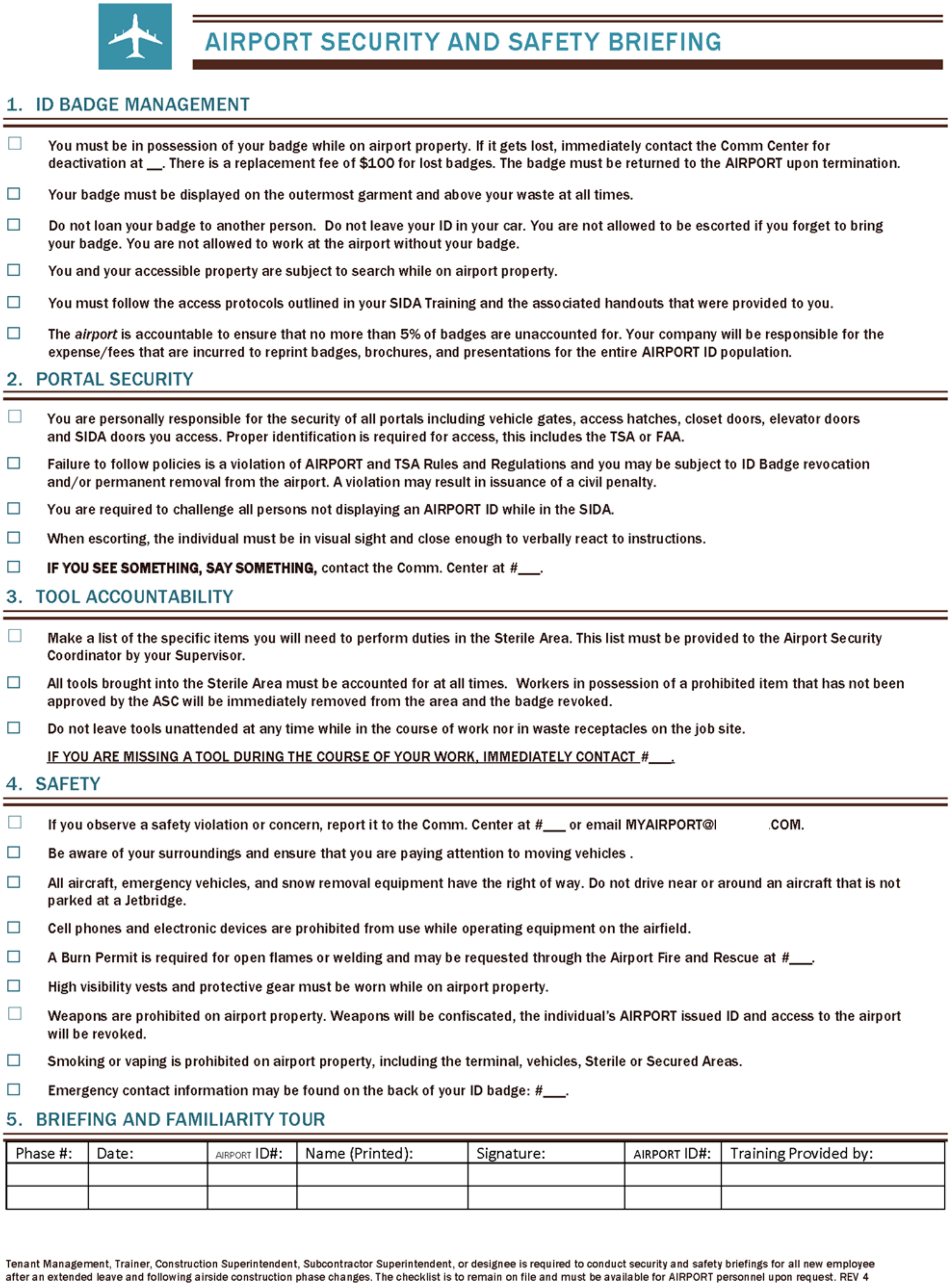
Transportation Security Administration. (2022). *TSA Action Plan Program*.

TransSolutions. (2020). *Employee/Vendor Physical Inspection Program Guidance* (PARAS 0019). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0019.EmployeeVendorPhysicalInspectionPrograms__.FinalReport__.pdf.

Zhang, Tianjian. (2018). "Knowledge Expiration in Security Awareness Training". Annual ADFSL Conference on Digital Forensics, Security and Law. https://commons.erau.edu/adfsl/2018/presentations/2.

Zoufal, Donald. (2021). *Security Regulatory Compliance at Tenant Facilities* (PARAS 0025). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0025.SecurityComplianceTenantFacilities_.FinalReport_.pdf.

APPENDIX A: SAMPLE AIRPORT SECURITY AND SAFETY BRIEFING CHECKLIST



AIRPORT SECURITY AND SAFETY BRIEFING

1. ID BADGE MANAGEMENT

□ You must be in possession of your badge while on airport property. If it gets lost, immediately contact the Comm Center for deactivation at __. There is a replacement fee of $100 for lost badges. The badge must be returned to the AIRPORT upon termination.

□ Your badge must be displayed on the outermost garment and above your waste at all times.

□ Do not loan your badge to another person. Do not leave your ID in your car. You are not allowed to be escorted if you forget to bring your badge. You are not allowed to work at the airport without your badge.

□ You and your accessible property are subject to search while on airport property.

□ You must follow the access protocols outlined in your SIDA Training and the associated handouts that were provided to you.

□ The *airport* is accountable to ensure that no more than 5% of badges are unaccounted for. Your company will be responsible for the expense/fees that are incurred to reprint badges, brochures, and presentations for the entire AIRPORT ID population.

2. PORTAL SECURITY

□ You are personally responsible for the security of all portals including vehicle gates, access hatches, closet doors, elevator doors and SIDA doors you access. Proper identification is required for access, this includes the TSA or FAA.

□ Failure to follow policies is a violation of AIRPORT and TSA Rules and Regulations and you may be subject to ID Badge revocation and/or permanent removal from the airport. A violation may result in issuance of a civil penalty.

□ You are required to challenge all persons not displaying an AIRPORT ID while in the SIDA.

□ When escorting, the individual must be in visual sight and close enough to verbally react to instructions.

□ **IF YOU SEE SOMETHING, SAY SOMETHING,** contact the Comm. Center at #___.

3. TOOL ACCOUNTABILITY

□ Make a list of the specific items you will need to perform duties in the Sterile Area. This list must be provided to the Airport Security Coordinator by your Supervisor.

□ All tools brought into the Sterile Area must be accounted for at all times. Workers in possession of a prohibited item that has not been approved by the ASC will be immediately removed from the area and the badge revoked.

□ Do not leave tools unattended at any time while in the course of work nor in waste receptacles on the job site.

IF YOU ARE MISSING A TOOL DURING THE COURSE OF YOUR WORK, IMMEDIATELY CONTACT #___.

4. SAFETY

□ If you observe a safety violation or concern, report it to the Comm. Center at #___ or email MYAIRPORT@I .COM.

□ Be aware of your surroundings and ensure that you are paying attention to moving vehicles .

□ All aircraft, emergency vehicles, and snow removal equipment have the right of way. Do not drive near or around an aircraft that is not parked at a Jetbridge.

□ Cell phones and electronic devices are prohibited from use while operating equipment on the airfield.

□ A Burn Permit is required for open flames or welding and may be requested through the Airport Fire and Rescue at #___.

□ High visibility vests and protective gear must be worn while on airport property.

□ Weapons are prohibited on airport property. Weapons will be confiscated, the individual's AIRPORT issued ID and access to the airport will be revoked.

□ Smoking or vaping is prohibited on airport property, including the terminal, vehicles, Sterile or Secured Areas.

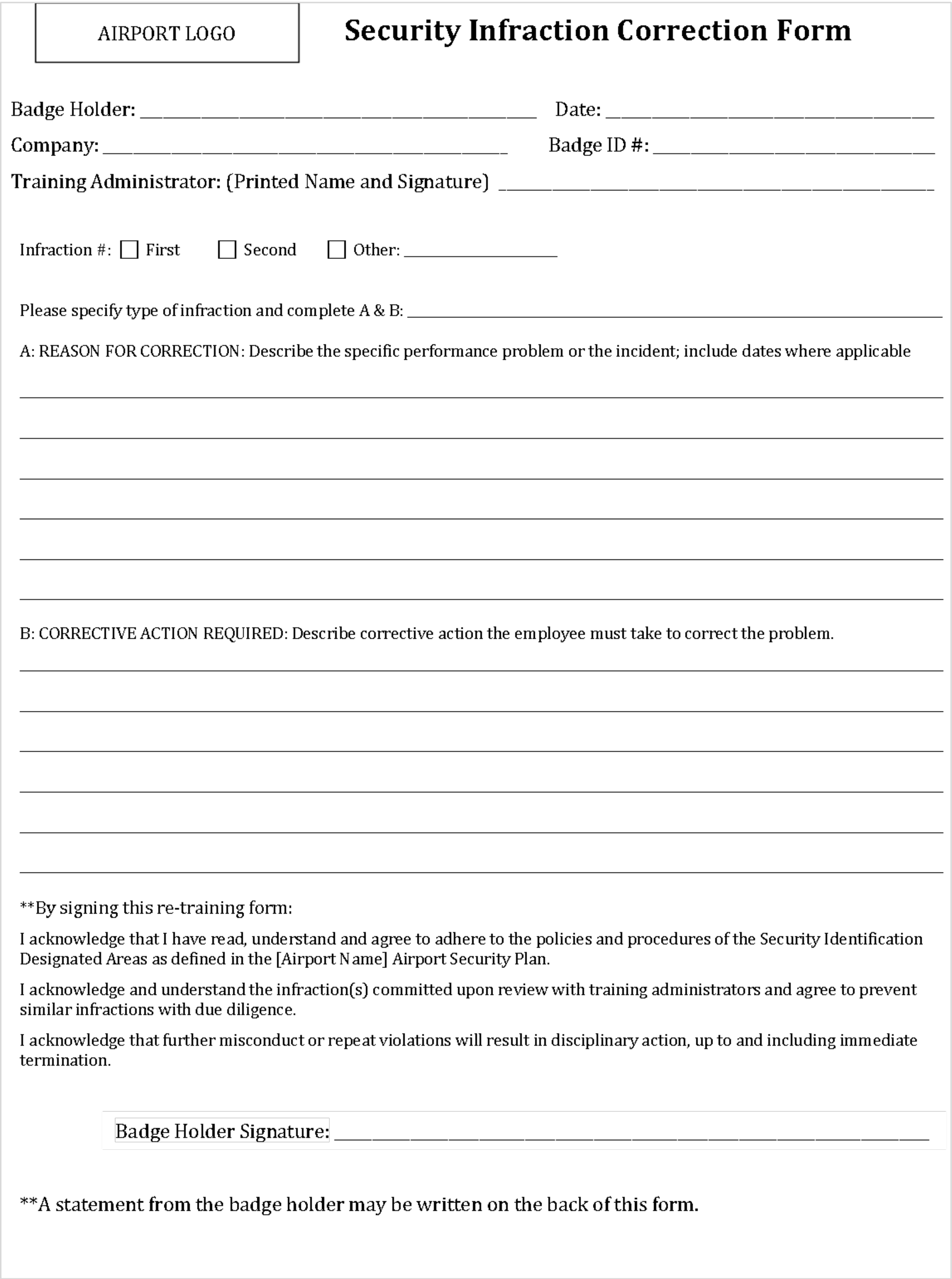
□ Emergency contact information may be found on the back of your ID badge: #___.

5. BRIEFING AND FAMILIARITY TOUR

Phase #:	Date:	AIRPORT ID#:	Name (Printed):	Signature:	AIRPORT ID#:	Training Provided by:

Tenant Management, Trainer, Construction Superintendent, Subcontractor Superintendent, or designee is required to conduct security and safety briefings for all new employee after an extended leave and following airside construction phase changes. The checklist is to remain on file and must be available for AIRPORT personnel upon request. REV 4

APPENDIX B: SECURITY INFRACTION CORRECTION FORM



AIRPORT LOGO

Security Infraction Correction Form

Badge Holder: ______________________________ Date: ______________________________

Company: ______________________________ Badge ID #: ______________________________

Training Administrator: (Printed Name and Signature) ______________________________

Infraction #: □ First □ Second □ Other: ______________

Please specify type of infraction and complete A & B: ______________________________

A: REASON FOR CORRECTION: Describe the specific performance problem or the incident; include dates where applicable

____

____

____

____

____

____

B: CORRECTIVE ACTION REQUIRED: Describe corrective action the employee must take to correct the problem.

____

____

____

____

____

____

**By signing this re-training form:

I acknowledge that I have read, understand and agree to adhere to the policies and procedures of the Security Identification Designated Areas as defined in the [Airport Name] Airport Security Plan.

I acknowledge and understand the infraction(s) committed upon review with training administrators and agree to prevent similar infractions with due diligence.

I acknowledge that further misconduct or repeat violations will result in disciplinary action, up to and including immediate termination.

Badge Holder Signature: ______________________________

**A statement from the badge holder may be written on the back of this form.