PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0065 January 2026

Synthesis of Security Practices for Airside Vehicle Operations

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

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

Kim Dickie
KPD Consulting, LLC
Powell Butte, OR

Michele Freadman
M. Freadman Consulting, LLC
Attleboro, MA

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 0065 PROJECT PANEL

Frank Capello *Broward County Aviation Department (Retired)*
Brian Daniel *Dallas Fort Worth International Airport*
Joseph Gaudio *AirTera*
Gaël Le Bris *WSP USA Inc.*
Dustin Loftis *Phoenix Sky Harbor International Airport*
Darren Ngo *George Bush Intercontinental Airport*
Eleanor Robichaud *Kinexis Consulting LLC*
Gary Smedile *Independent Consultant*
Andrew Young *Chrysalis Global*

AUTHOR ACKNOWLEDGMENTS

The PARAS 0065 Research Team would like to thank the following organizations, groups, and individuals for their contributions to this research. Without their support, it would not have been possible.

The authors wish to thank all of the airport operators who volunteered to participate in interviews to understand practices at their airports. Their input formed the foundation of the research.

The authors also want to thank the Project Panel for their feedback and expertise throughout the research. Their guidance shaped the goals of the research as well as the final product.

Finally, thanks to National Safe Skies Alliance for facilitating not only this research but the variety of security-focused research that the PARAS program offers to the airport community.

CONTENTS

TABLES & FIGURES

SUMMARY

Airside vehicle operations are a critical component of airport security, presenting unique challenges that span access control, risk management, operational safety, regulatory compliance, and coordination with tenants and external partners. PARAS 0065: *Synthesis of Security Practices for Airside Vehicle Operations* consolidates a wide range of practices, technologies, and strategies employed at US commercial airports to secure vehicle movements on the airfield and mitigate potential security vulnerabilities. The study draws from over 20 interviews with airport operators of varying sizes and operational complexity, supported by federal regulations, past PARAS reports, and relevant industry guidance.

The report focuses on security practices related to driver authorization, vehicle permitting processes, credential oversight, escorted vehicle access, gate operations, and airfield construction activities. It also addresses the deployment of security technologies such as access control systems, surveillance tools, and intrusion detection, and examines how data, inspections, and cross-functional safety programs can reinforce security outcomes.

Key findings highlight the importance of clear driver endorsement and provisioning protocols, ongoing compliance monitoring, structured permitting programs, visual identification standards, designated vehicle access points, and the strategic use of escorts and inspections. To support these efforts, airports are increasingly integrating safety-driven protocols, such as routine vehicle checks and situational awareness initiatives, into their security framework. Technology adoption is frequently focused on automation, mobile enforcement, and real-time monitoring to complement security programs and reduce operational burden without compromising airport integrity.

This synthesis provides a practical reference for airports seeking to assess or enhance their airside vehicle operations-related security protocols. This consolidated resource supports flexible implementation while reinforcing the foundational principles of accountability, access control, risk management, and situational awareness necessary for secure vehicle operations in the airside environment.

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

AC	Advisory Circular
ACS	Access Control System
ADS-B	Automatic Dependent Surveillance–Broadcast
ALPR	Automated License Plate Recognition
AS	Authorized Signatory
ASP	Airport Security Program
ATC	Air Traffic Control
CMAE	Construction Movement Area Endorsement
CRDF	Centralized Receiving and Distribution Facilities
CSPP	Construction Safety and Phasing Plan
DMV	Department of Motor Vehicles
EAA	Exclusive Area Agreement
GA	General Aviation
GIS	Geographic Information System
GSE	Ground Service Equipment
IDMS	Identity Management System
LEO	Law Enforcement Officer
MA	Movement Area
NMA	Non-Movement Area
NOV	Notice of Violation
OCIP	Owner Controlled Insurance Program
PIDS	Perimeter Intrusion Detection System
PNO	Planned Non-Operation
RFID	Radio Frequency Identification
SeMS	Security Management System

SMGCS Surface Movement Guidance and Control System

SMS Safety Management System

VIN Vehicle Identification Number

SECTION 1: INTRODUCTION

Commercial airports face persistent challenges in mitigating security vulnerabilities caused by vehicle operations in regulated areas. One of the most complex aspects of this effort involves managing vehicle access and movements on the airfield. Drivers and vehicles operating in security restricted areas—including the AOA, SIDA, and Secured Areas—can introduce security vulnerabilities if not properly credentialed, controlled, and monitored.

While vehicle access is essential to support airport operations (e.g., aircraft turnaround, infrastructure maintenance and repair, deliveries, and construction activities), each entry point and vehicle movement must be actively managed to ensure security and compliance with airport, TSA, and FAA regulations. Given the complex interplay between operational demands and federal security requirements, airport operators must balance security, safety, and efficiency in every decision, policy, and requirement related to airside vehicle access, operations, and control.

This report serves as a resource for airport security and operations professionals who are responsible for mitigating security vulnerabilities associated with airside vehicle operations. It provides a synthesis of current security practices implemented at a diverse set of US commercial airports, organized into actionable strategies. These strategies encompass access point policies, vehicle permitting, escorting, compliance and auditing, leveraging safety practices, emergency response protocols, and the use of technology and processes to improve security monitoring and enforcement. Where relevant, examples illustrate how these strategies have been successfully implemented, including both common and unique practices and innovative approaches.

The synthesis consolidates viable solutions discovered during the research that can help airports strengthen the security of airside vehicle operations without impeding operational continuity. Where possible, scalable options have been included to support implementation across airports of different sizes, layouts, and resource levels.

1.1 Purpose of This Report

This report synthesizes current industry practices for managing airside vehicle operations through a security lens. The research supports airport operators by documenting how various strategies, ranging from credentialing controls and vehicle permitting to escorting procedures and emerging technologies, can be applied to strengthen the security of vehicle operations on the airside at commercial airports of all sizes.

The report draws upon interviews with airport operators, federal regulatory guidance, and prior PARAS studies. Special attention was given to identifying scalable practices, security-enhancing adaptations of safety programs, and the use of technology to streamline access while maintaining compliance.

Through this synthesis, airport operators are equipped with practical, real-world examples of how to adapt their policies and procedures to mitigate risk, ensure regulatory alignment, and maintain a secure and efficient airside environment for vehicular activity.

1.2 Research Methodology

This research was conducted through a comprehensive literature review and targeted airport interviews. The literature review examined regulatory guidance, existing research publications, and relevant industry materials to establish foundational knowledge and identify known strategies. The research team

also conducted interviews with airport security and operations personnel from airports of varying size and complexity. Interviewees were selected to represent a cross-section of the industry, and discussions focused on real-world practices, lessons learned, and local adaptations of federal requirements.

In total, more than two dozen industry reports and regulatory documents were reviewed, and interviews were conducted with 21 airports. The research also emphasized practices tied to credentialing, vehicle permitting and oversight, escorting, construction coordination, technology use, compliance and auditing, and safety-informed security strategies.

This dual methodology ensured the research is grounded in both formal requirements and operational realities, enabling practical application across a wide range of airport environments.

SECTION 2: AIRFIELD DRIVER AUTHORIZATION & BADGE ENDORSEMENTS

Airport operators manage airfield driving privileges through a structured authorization process that is often integrated with the airport's credentialing system. Driving privileges are issued based on operational necessity, job responsibilities, and successful completion of mandatory training requirements.

To maintain both operational efficiency and regulatory compliance, airports apply multiple strategies to carefully limit and control airside driving privileges.

2.1 Airfield Driving Authorization Process

Authorization for airside driving privileges typically begins in the credentialing office during the initial badge application process. The Authorized Signatory (AS) initiates the request for driving privileges based on operational need, specifying the type of privileges—Non-Movement Area (NMA) or Movement Area (MA)—on the application and, in some cases, identifying specific vehicle access gates needed to perform assigned duties.

An authorized airport representative, typically a manager or specialist within the security or operations department, reviews the request and approves or denies the driving privileges based on the applicant's role and operational responsibilities. Applicants conditionally approved for airside driving privileges are assigned the corresponding driver training modules in addition to any other required training, evaluation, and testing before they are issued driving endorsements.

One airport strengthened oversight of driving authorizations by requiring each AS to complete and pass every driver training course they are authorized to request for their employees. This approach was seen as a way to move the AS role beyond clerical functions, replacing a "box-checking" mindset with practical knowledge of airside operations. The airport reported that this requirement reduced the number of basic inquiries escalated to Operations, as the signatories were better equipped to answer questions and assess driving privilege requests independently. While this practice may not be feasible at larger airports due to volume and operational constraints, it may be a valuable strategy for small or mid-sized airports that rely more heavily on the AS roles.

The assignment of driving privileges is based on operational need and risk exposure. Common strategies to limit this exposure include:

- Issuing MA driving privileges only to airport personnel (security, operations, facilities and maintenance, wildlife control), law enforcement officers (LEO), firefighting personnel, and select FAA employees
- Limiting tenant driving privileges to a maximum percentage of each tenant's badged workforce
- Requiring tenants and contractors to designate authorized airfield drivers who will escort other vehicles on the airfield and limiting the number of vehicle escorts each tenant or contractor may have

Airports may incorporate driving requirements and rules directly into the badge application process, requiring applicants to acknowledge security restrictions such as:

"I understand that I may not drive within the secure or movement areas unless I have received proper training and authorization by the Airport. The vehicle I am driving must also be an authorized vehicle, approved by the Airport, with proper identification markings."

Driving rules and requirements are often also included in airport's rules and regulations or detailed in separate Driver Training Manuals.

2.2 Airside Driving Endorsements

The research identified four common driving designations/endorsements, each with distinct training requirements, operational procedures, and in some cases air traffic control (ATC) communication requirements:

- **Non-Movement Area (NMA)** – vehicle movement permitted on taxi lanes, aprons, vehicle service roads (VSRs), and aircraft parking areas not controlled by the FAA
- **Movement Area (MA)** – vehicle movement permitted on taxiways and runways under FAA control
- **Surface Movement Guidance and Control System (SMGCS)** – vehicle movement authorized during low-visibility conditions
- **Construction Movement Area Endorsement (CMAE)** – vehicle movement authorized along designated construction routes that may cross both NMA and MA

Not all airports utilize all four endorsements; most commonly, airports assign only NMA and MA driving privileges.

2.2.1 Driving and Access Indicators

To comply with 49 CFR § 1542.211 *Identification Systems*, airports use a wide variety of badge elements to clearly indicate driving privileges at a distance, supporting both security and operational awareness in low-visibility or high-traffic environments. Common badge endorsements include:

- **Letters or Icons:** D (driving privilege), M (movement area), T (tow qualified); vehicle, airplane, or tower symbols
- **Text:** Non-Movement, Ramp, Movement, Full
- **Colors:** Red, blue, green, or orange icons; colored strips with text; icons or text with high-contrast backgrounds for viewing from a distance; distinct badge colors for different levels of area access permissions

Because badge designs vary widely across airports, icon and color placement are typically customized to meet the airport's operational and security needs, but are generally in a consistent order and location on the badge within each airport. Airports that use color-coded badge backgrounds (e.g., red for SIDA, blue for AOA) generally have cleaner, easier-to-read badge faces.

Additional specialty indicators may include:

- Low visibility endorsements (e.g., SM, SMGCS)
- Construction endorsements (e.g., CMAE, CMAP)
- Contractor identifiers (e.g., C)
- White badges reserved for LEOs and first responders

Badge management procedures include processes for reprinting badges if driving privileges are added, suspended, or revoked. To improve flexibility, some airports use tamper-proof stickers designating driving authorizations. Stickers can be removed immediately in the field by authorized personnel in cases of severe violations, avoiding the need for immediate badge reissuance while clearly indicating that the individual is no longer permitted to drive in regulated security areas (see Section 2.3.2 for further discussion of tamper-proof stickers).

2.2.2 Badge Visibility and Readability Features

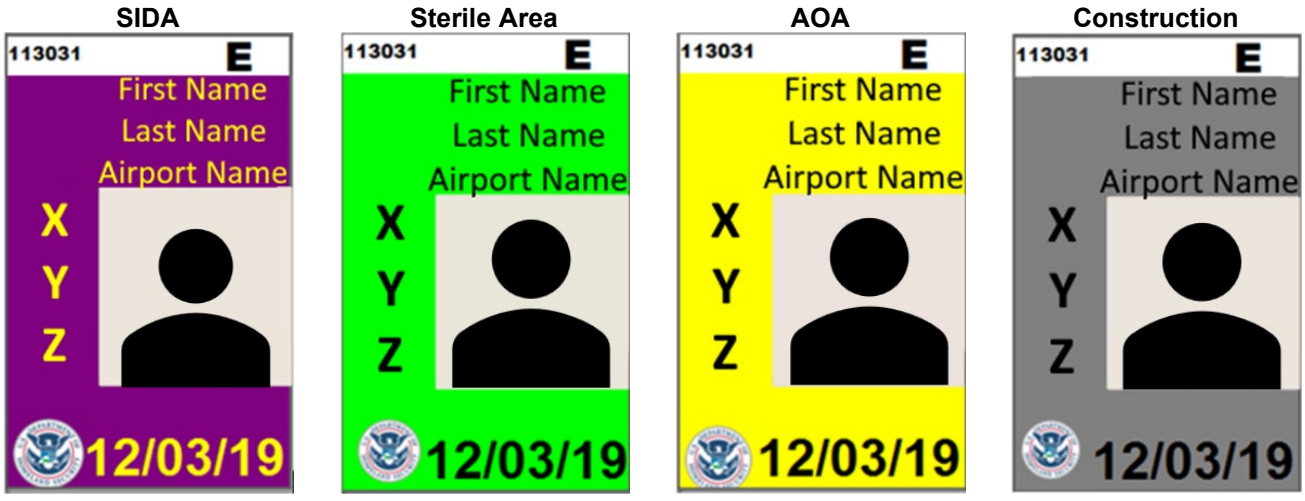
To enhance situational awareness and safety, many airports incorporate design features that enable badges to remain visible and recognizable in a variety of environmental conditions. Important features for badges and icons intended for airside use include:

- Bright, high-visibility colors (e.g., white or neon yellow, orange, green)
- Reflective materials for nighttime and adverse weather visibility
- Luminescent elements to provide passive illumination in low-light conditions
- Large, clear fonts and recognizable symbols for distance readability
- High-contrast color combinations optimized for clarity and visibility
- Patterned overlays to support identification for individuals with color vision deficiencies

These features ensure that personnel operating on the airfield can be quickly identified and verified, consistent with FAA safety guidance and TSA security regulations.

Figure 1 presents examples of badge colors used to quickly identify access authority (information redacted for security). The “E” on the upper right grants escort authority in the specified area.

Figure 1. Examples of Color-Coded Badges



2.2.3 Identifying Expired Licenses and Potential Violations

Individuals are required to maintain a valid state driver’s license as a condition of maintaining airport driving privileges. If a driver’s state license lapses, the airport must remove the individual’s driving privileges and may add the individual to a stop list shared at vehicle access control points to prevent them from entering a security restricted area.

To ensure drivers meet legal requirements, some airports have implemented practices to track the status of state-issued driver's licenses through their identity management system (IDMS) or badge management systems. This enables the system to flag expired licenses and prevent access or initiate a privilege review. In some cases, risk management or law enforcement have access to state systems to receive notifications of license suspensions or revocations, allowing airports to take timely corrective action. These practices are not universally adopted and often depend on state, city, or county-level data sharing agreements, but they serve as valuable compliance and liability mitigation strategies.

To proactively identify badge holders with lapsed or revoked state-issued driver's licenses, some airports print the driver's license expiration date directly on the airport badge, often highlighted in a distinct color (e.g., red) for quick identification during badge inspections and challenges. This strategy allows security and operations staff to verify both badge and license validity during routine checks. If a badge holder's driver's license is found to be expired, the airport can take immediate corrective action.

To further strengthen tracking, airports are moving from displaying only month/year driver's license expiration formats to full month/day/year formats, providing greater precision in license verification and compliance enforcement.

2.3 Driving Endorsement Changes

Initial driver training is often completed prior to issuance of a person's first airport badge, allowing the driving endorsement to be printed directly on the badge and avoiding the need to reprint the badge. Many airports align the expiration dates for driver training, security training, and badge validity to streamline recordkeeping and simplify compliance tracking. However, airports with two-year badge renewal cycles may face challenges aligning a two-year badge and security training cycle with the annual recurrent training required for MA driving privileges.

The misalignment between key expiration dates can increase the burden on credentialing offices by requiring more frequent badge reissuance. Two strategies were identified to address this challenge without altering the badge expiration period: issuing a separate driver authorization credential or using tamper-proof stickers to indicate driving privileges. Both approaches allow airports greater flexibility to maintain compliance and security standards without requiring badge reprinting every time a training cycle is completed or a privilege is revoked.

More information on badge expiration and management can be found in PARAS 0020: *Strategies for Effective Airport Identification Media Accountability and Control*.

2.3.1 Separate Driver Authorization Media

Some airports issue a secondary credential, similar to a state-issued driver's license, to authorized airside drivers. These airport-issued licenses typically include the driver's photo, an expiration date, and indicators showing the specific areas where the individual is permitted to operate vehicles. Badge holders are required to carry both their airport ID badge and their airport-issued driver's license while operating a vehicle on the airfield and must present both upon request.

Using a separate driver authorization media allows the credentialing office to modify or revoke driving privileges without reprinting the primary security badge. These licenses are renewed upon driver training expiration, providing a flexible method to maintain compliance without burdening the core credentialing process.

2.3.2 Tamper-Proof Stickers

To reduce operational burden, many airports use tamper-proof stickers affixed to the badge to indicate active driving privileges. Stickers provide flexibility by allowing authorized personnel to immediately remove driving endorsements in the field following a violation or suspension, without confiscating or reprinting the badge. The tamper-proof design of these stickers prevents transfer from one badge to another, as the sticker obliterates the approved markings when removed from a badge. The use of stickers also decouples driving privilege renewals from badge expiration dates, allowing driver training cycles to operate independently of badge renewal.

In some cases, airports will initially issue stickers to denote provisional driving privileges for new badge holders, allowing them to operate vehicles during a probationary or training period. Once the individual successfully completes a full training cycle, the airport reprints the badge with a permanent endorsement icon. This two-step approach helps distinguish provisional drivers from fully authorized personnel, provides a visual cue for security and operations staff while conducting an inspection or challenge procedure, and alleviates the workload for credentialing teams by deferring full badge reprints until individuals demonstrate long-term retention, which is especially helpful for managing high-turnover populations.

SECTION 3: LIMITING AIRFIELD VEHICLES

Airports rely on a wide range of vehicles to support daily operations across both MAs and NMAs of the airfield. These vehicles are critical to functions such as aircraft servicing, maintenance, fueling, construction, emergency response, and regulatory oversight. Vehicle operators may include airport staff, tenants, contractors, vendors, and federal agencies, each with specific operational needs that require airfield access.

Because airfield environments are highly sensitive and tightly regulated, this operational need is balanced by access control measures and risk management practices that aim to protect safety, security, and operational continuity. Vehicles must be properly permitted, insured, marked for identification, and operated by credentialed personnel. Airports develop permitting programs, inspection protocols, and vehicle standards to ensure only authorized, roadworthy, and operationally justified vehicles are granted access.

3.1 Operational Need for Vehicle Access

Airports adhere to FAA guidance by restricting airfield access to vehicles that have a valid operational need, are operated by credentialed personnel, and are compliant with airport and TSA regulations. Examples of the types of vehicles commonly permitted to operate on the airfield include:

- Airport operator vehicles (e.g., operations, facilities maintenance)
- Tenant and contractor vehicles
- Parcel and vendor delivery trucks
- Construction vehicles (e.g., concrete trucks, flatbeds, tractor trailers)
- Waste management and hazardous material trucks
- Fuel delivery and refueling trucks and equipment
- Ground service equipment (GSE), including baggage tugs, air stairs, and deicing vehicles
- Airport law enforcement vehicles
- Airport and local emergency response vehicles responding to an emergency
- Vanpools shuttling employee groups
- Federal agency vehicles (e.g., FAA, TSA, Customs and Border Protection, Secret Service)

Airports have a variety of restrictions on the types of vehicles permitted on the airfield, typically based on specific risk factors. For example, several airports restrict the use of golf carts anywhere on the airfield due to safety and security concerns, but others permit their use solely in and around privately leased hangars, in cargo areas, or to transport maintenance parts along designated routes. Commonly restricted or limited vehicle types include:

- **Personal vehicles –** some exceptions for general aviation (GA) hangar tenants
- **Bicycles, Segways, trikes, and motorcycles –** some exceptions for motorcade escorts
- **Autonomous vehicles –** no self-driving features can be active on the airfield
- **Armored vehicles –** some exceptions for cash and valuables-in-transit under escort
- **Vehicles transporting explosives, firearms, or hazardous materials –** requires a TSA-approved airport security program (ASP) Changed Condition or Alternate Measure to permit on airfield

As an additional control measure, airports may also restrict access to vehicles with obstructed visibility, such as dark window tint on rear or side windows, to help ensure compliance with TSA-mandated vehicle inspections. This strategy supports gate inspection protocols by allowing security personnel to visually verify interior contents during inspections and reduce the risk of concealed threats.

Authorization exceptions for restricted vehicle types are rare and typically require approval by an airport security or operations manager, and occasionally FAA or TSA.

3.1.1 Insurance Requirements

Vehicles permitted on the airfield must meet minimum liability insurance requirements, which can vary between airports and operating areas. Personal vehicles not covered under the company's insurance are generally prohibited from accessing the airfield unless under escort. Typical insurance coverage ranges from $5 million to $10 million. Some airports have recently increased the minimum coverage to account for inflation. Insurance requirements for private hangar operators are often lower than other tenants (around $500,000) when their access is restricted to the hangar space.

To further reduce safety and liability concerns, airports may restrict certain vehicle types from being driven on the airfield, such as exotic cars being shipped via airside cargo or heavy construction equipment (e.g., bulldozers and excavators). Instead, these vehicles are transported on flatbed trailers and unloaded near their destination, minimizing operational risk and potential damage to airfield surfaces.

Responsibility for verifying insurance often falls to the credentialing, operations, or security department. However, due to the complexity of insurance verification, it may be more appropriately handled by the procurement/business management team, risk management department, or legal counsel who have expertise in the subject. This approach ensures a more accurate review and reduces the burden on credentialing and operations staff who may not fully understand the nuances associated with insurance.

To maintain uninterrupted access to the airfield, the vehicle owner is required to have active insurance for the duration of the vehicle permit, project contract, or tenant lease. Requiring the airport authority to be listed as an additional certificate holder on the insurance ("additional insured") provides several key benefits. In addition to receiving notifications of cancellations or lapses in coverage, this designation extends liability protection to the airport in the event of an accident caused by a tenant, vendor, service provider, or other authorized operator. Lapsed insurance can result in vehicles being placed on stop lists, removed from the airfield, and denied access until coverage is restored and any corrective actions completed.

Airports can support small businesses working on airfield projects through an Owner Controlled Insurance Program (OCIP). This is a policy purchased by the project owner (i.e., airport authority) to cover all contractors and subcontractors working on a designated project. Under this model, small businesses are only required to meet a lower base coverage threshold to hold an agreement with the airport (e.g., $2 million), with the OCIP providing supplemental coverage to meet the airport's full insurance requirement.

3.1.2 Vehicle Marking Requirements and Identification Standards

To support security, accountability, and compliance with FAA guidelines, airports enforce detailed vehicle identification requirements for all vehicles authorized to operate on the airfield. These markings serve as a visual verification tool for both airport personnel and security staff and are essential for distinguishing authorized vehicles within security restricted areas. Any vehicle lacking the appropriate

markings is generally denied access to the airfield or removed from the airfield until corrective action is taken.

In accordance with FAA Advisory Circular 150/5210-5D, airport operator-owned vehicles must display identification information on the side of the vehicle in a font that is at least 16 inches (410 mm) in height and placed conspicuously. While this specific requirement does not extend to tenant or contractor vehicles, many airports have established local standards to ensure markings are visible and standardized across all permitted users. These standards often require that company names and logos be professionally produced, clearly legible, securely attached (e.g., sticker, magnet) to prevent foreign object debris, and prominently displayed on both sides of the vehicle.

Airport specifications for tenant and contractor vehicles generally include minimum lettering heights mirroring FAA requirements, logo visibility from a specified distance, and contrasting colors for enhanced readability. Some airports incorporate additional requirements for low-light conditions, such as reflective materials or high-contrast color combinations. In most cases, markings are placed on the driver and passenger doors or front and rear bumpers for maximum visibility. Inclusion of the company's contact information is also a common requirement, enabling operations or security staff to contact the vehicle operator directly, often a faster method than cross-referencing permit databases in time-sensitive situations when the operator is not with the vehicle (i.e., the vehicle is parked).

Airports vary in their enforcement of securely affixing logos to vehicles. While magnetic placards are permitted at some locations, others require permanent (sticker) decals or painted markings to prevent issues such as placards falling off, being tampered with, or being transferred to an unauthorized vehicle. The increased use of aluminum and plastic body panels in modern vehicle construction has introduced additional challenges, as magnetic signs may not adhere securely to these materials, leading some airports to phase them out entirely.

To ensure consistent enforcement and visual verification of the logos, some airports maintain a centralized logo database as part of the permitting program. Companies are required to submit a digital version of their logo during the application phase, which is stored electronically and also printed in physical format for use at vehicle access points. This allows gate personnel to confirm that vehicle markings match the approved logo, even during network outages. If discrepancies are identified, the vehicle is denied access until the markings are corrected or verified. Companies are required to notify permitting authorities whenever their logos change, ensuring that the logo database remains up to date.

Vehicle inspections are often conducted during permit renewals to confirm compliance with the airport's marking standards. These inspections allow airport staff to verify that logos are properly affixed, remain legible, and match the records on file.

3.2 Vehicle Permitting Programs

Formal vehicle permitting programs allow airports to verify a vehicle's operational need, mandatory insurance coverage, and compliance with airfield access regulations. Key characteristics of these programs include:

- **Permit Application Process:** Vehicle operators submit an application and proof of insurance. Some airports require a letter from the AS demonstrating the vehicle's operational need to access the airfield.
- **Managing Departments:** Vehicle permit issuance and tracking are typically managed by security, operations, or credentialing departments.

- **Permit Types:** Some airports distinguish between roadworthy vehicles and specialized GSE, issuing separate permits for each.
- **Permit Fees:** Fees generally range from $15 to $100. In some cases, higher fees are used to discourage permit requests for an unnecessary number of airfield vehicles.

Permitting programs are often incorporated into the ASP or airport rules and regulations. Vehicles without a permit are restricted from entering the airfield without an escort.

3.2.1 Registration and Safety Inspections

Vehicles that are authorized to cross the airfield boundary and operate on the airfield are required to meet specific eligibility requirements prior to permit issuance or access authorization. These typically consist of valid state registration or proof of roadworthiness, consistent with local motor vehicle standards.

Generally, airports do not independently require routine safety inspections beyond what is mandated by their state's Department of Motor Vehicles (DMV). In states where periodic vehicle inspections are required for registration, proof of inspection is generally required as part of the airport's permitting process. Security staff assigned to access control points may be instructed to deny entry to any vehicle lacking current registration or inspection documentation to reinforce regulatory compliance.

The permitting process often links the issued permit to the vehicle's license plate and Vehicle Identification Number (VIN), allowing security personnel to verify registration details before granting or renewing access. This approach supports enforcement efforts by reducing the risk of permit misuse, such as license plate or credential swapping.

In some cases, challenges arise with vehicles that have suppressed or "ghost" license plates—registrations that are deliberately excluded from public databases and Automated License Plate Recognition (ALPR) systems. These plates are lawfully used by law enforcement, government agencies, and other regulated entities for security-sensitive operations. However, their exclusion from standard verification systems complicates airport permitting. To maintain access control integrity, such vehicles are not eligible for standard permitting at many airports and must be escorted by authorized personnel while operating within security restricted areas.

Some vehicles are registered under a "planned non-operation" (PNO) status, which indicates they are not authorized for use on public roadways. These include GSE, golf carts, and other vehicles restricted to airfield operations. PNO-designated vehicles are limited to operations within specific areas of the airfield and are not permitted to exit the secure perimeter. If a PNO-registered vehicle is found outside its designated area or attempts to reenter a security restricted area, it may not be permitted access unless escorted by appropriate airport personnel back to its assigned location. Enforcement actions, such as Notices of Violation (NOV), may be issued to the responsible tenant or operator for such actions.

Implementation of on-site safety inspection programs can support the operational and compliance needs of vehicles that do not operate on public roads. These inspections typically apply to vehicles without state registration (e.g., GSE or PNO-designated equipment) and are used to ensure continued operational safety within the airfield environment. In most cases, the airfield operations department is responsible for conducting these inspections. However, some airports have delegated this responsibility to third-party contractors to reduce workload on internal teams while maintaining consistent inspection standards.

3.2.2 Vehicle Permit Indicators

Visible vehicle permits are the primary method of confirming that a vehicle is authorized to operate within security restricted airfield areas. Permits are typically issued as windshield stickers (Figure 2), dashboard placards, or hang tags, with placement designed to enable quick verification by security personnel at access points and during airfield operations.

Figure 2. Example Ramp Permit Sticker (redacted)

Airports can emphasize the importance of clearly marked vehicles and treating unpermitted or unidentified vehicles as potential security threats by codifying this expectation into their security training and rules and regulations. This requires all airport badge holders to challenge not only individuals but also vehicles whose authorization on the airfield is not immediately apparent. Failure to report a suspicious or unmarked vehicle may result in enforcement actions (e.g., NOV) against the badge holder. This approach reinforces situational awareness, strengthens personal responsibility, and broadens the application of security protocols across the airfield community.

Although permit designs vary between airports, several common features were identified:

- A unique, serialized permit number tied to both the vehicle and its associated company
- Clear expiration dates, sometimes integrated into the permit number (e.g., last two digits of the year)
- Color-coded backgrounds that change annually to quickly distinguish valid permits from expired ones
- Airport logos to reinforce authenticity

Below are examples of an airport's vehicle permits changing appearance each year for rapid recognition of expired stickers.

Figure 3. Examples of Vehicle Permit Security Features

Stickers are the most commonly used permit type, typically placed on the driver's side of the windshield or on the front bumper for maximum visibility. Many airports prefer stickers for their enhanced security features. These are designed to be difficult to remove without visible damage, minimizing the risk of

unauthorized transfer. Some are destructible or tamper-evident stickers that self-destruct when removal is attempted. Many airports have invested in in-house printing equipment to streamline sticker production, allowing for greater flexibility and reduced long-term costs.

To further safeguard the integrity of the permitting process, application of the sticker to the vehicle can be tasked exclusively to airport operations or security personnel. This ensures that a visual inspection of the vehicle is conducted at the time of permit issuance, facilitates prompt return of expired permits, and eliminates the risk of vehicle owners improperly affixing or transferring permits themselves.

Figure 4. Example Hang Tag

Dashboard placards and hang tags (Figure 4) are also used at many airports, particularly for vehicles operating exclusively within GA areas or for official vehicles, such as unmarked law enforcement or Secret Service units. Unlike windshield stickers, hang tags and placards are often issued to individual operators rather than tied to a single vehicle, which creates additional security risks. Because these types of permits are easily transferable, airports should weigh their operational convenience against the risk of unauthorized vehicle substitution.

Some airports have implemented specialized programs to manage undercover or law enforcement vehicles operating without traditional markings. One example is the use of dashboard placards issued to law enforcement agencies that include both the agency's name prominently displayed on one side and a form detailing vehicle information, signed by an AS, on the reverse side. Security personnel at access points are trained to review both sides of the placard to confirm legitimacy.

Technologies such as Radio Frequency Identification (RFID) are widely used at many airports to enhance airfield access control. Integrating RFID chips into stickers, hang tags, or placards enables security personnel at the vehicle gates or on the airfield to quickly scan vehicles with handheld or mounted readers. RFID-enabled permits allow for real-time verification of vehicle authorization status and can automatically flag vehicles placed on security watch lists, reducing reliance on manual verifications and further strengthening airfield access control. While RFID is a well established technology, some airports are still expanding or refining its use.

3.2.3 Vehicle Permit Renewals

Vehicle permits are often issued on a one-year cycle, providing a balance between operational efficiency and ongoing compliance oversight. Annual renewal schedules enable airport permitting departments to manage application volumes in a controlled manner while ensuring that key documentation (e.g., insurance certificates, vehicle markings) remains current. To discourage unnecessary or casual registrations, a nominal fee (e.g., $5–$15 per vehicle) is often charged with each renewal.

Adopting alternative permit durations for select vehicle populations can further support the balance between operational efficiency and compliance oversight. For example, airport authority vehicles or other critical fleet vehicles may receive two-year permits to reduce administrative burden and cost. Temporary permits, typically valid for less than a year, may be issued to support short-term contractors or projects requiring brief airfield access.

A more stringent approach is to renew permits quarterly. This frequent renewal cycle requires insurance verification every three months, allowing the airport to detect insurance policy lapses, cancellations, or

suspensions with minimal delay. The trade-off to this strategy is increased administrative burden and cost.

Airports may align permit expiration with the driver's badge expiration date or the vehicle's state registration expiration. This distributes renewal activity throughout the year, which eases administrative peaks but requires robust tracking mechanisms to prevent oversight or gaps in vehicle authorization. In these cases, security personnel stationed at vehicle access points play a key role in reminding drivers when a permit is approaching expiration.

Alternatively, airports may issue all vehicle permits on a fixed annual cycle. Under this model, renewal applications are accepted several months before the expiration deadline to allow sufficient time for document audits, insurance verification, and visual compliance inspections. In some cases, each company's AS may be required to participate directly in the renewal process. An annual report listing all vehicles registered under the company is sent to the AS, who must update the roster to remove retired vehicles and add new ones as necessary, promoting shared accountability for accurate recordkeeping.

Expired permits are managed through established return and compliance processes. Many airports allow a short grace period (typically around two weeks) for drivers to return expired permits to the issuing office. New permits may be withheld until the previous permit is physically returned, reinforcing chain-of-custody standards. After the grace period expires, vehicles associated with unreturned permits may be placed on a stop list, prohibiting entry until the issue is resolved. In some cases, the airport may escalate enforcement by placing the company's entire fleet on the stop list, applying collective pressure to ensure prompt compliance.

To further encourage timely returns, some airports assess daily fines for each day a permit remains outstanding after the grace period ends. In certain cases, airports treat unreturned vehicle permits as equivalent to lost airport-issued badges, applying similar administrative penalties and requiring formal incident reporting before replacement or reissuance.

3.2.4 Vehicle Permit Management

Vehicle permitting is most commonly managed through a database or other electronic means. The complexity and scale of the system used varies based on the airport's need and available resources, but may include:

- A dedicated IDMS module
- A third-party platform integrated with the airport's badging system
- A custom spreadsheet or database tailored to the airport's permit workflow

Permitting databases typically log:

- Vehicle make/model, license plate, and VIN
- Permit ID number and expiration date
- Assigned driver(s) and associated company
- Insurance documentation status
- Access type (e.g., AOA-only, full SIDA, PNO-restricted)
- Company logo and contact information

Among other features, the information captured in the permitting recordkeeping system allows the airport to track the total number of permitted vehicles, monitor the fleet size per company, and add vehicles to stop or allow lists.

When combined with access control system (ACS) logs, permit data also supports trend analysis on vehicle movements and helps identify patterns of misuse, such as unauthorized entry attempts, expired permit activity, or drivers operating vehicles beyond their approved boundary in the regulated security area.

3.3 Enhanced Vehicle Permitting Practices

Airports that seek to reduce unnecessary vehicle presence on the airfield and strengthen control over tenant-operated fleets may implement enhanced vehicle permitting policies. These policies build on standard permitting practices but apply stricter thresholds to improve compliance, encourage operational discipline, and mitigate security risks associated with abandoned, uninsured, or inoperative vehicles.

Stricter enhancements have been adopted by some airports seeking to reduce administrative burden, promote accountability, or address persistent compliance gaps. By layering these practices into their permitting programs, airports can improve airfield security and safety without significantly disrupting operations.

Examples of enhanced vehicle permitting strategies include:

Stricter insurance standards, such as increased minimum liability coverage or more frequent proof-of-insurance submissions (e.g., quarterly), to ensure continued compliance and financial accountability.

- A large hub airport governed by a regional airport authority requires vehicles to carry layered coverage: $1 million in commercial general liability, $500,000 in auto liability, and a $10 million umbrella policy. Additionally, the airport must be listed as a named insured on all documents. These requirements apply to both over-the-road vehicles and airside equipment, and no permit is issued without active, verified coverage on file.
- A small city-owned airport preparing for Part 139 certification is using insurance requirements as a strategic lever to limit airside congestion and tenant noncompliance. As part of their airfield transition planning, airport leadership is considering raising insurance minimums to reduce the number of inactive or underutilized vehicles that tenants keep parked indefinitely.

Increased permitting fees, which may discourage registration of unnecessary or low-use vehicles and incentivize resource sharing or fleet consolidation.

- At a large county-operated hub airport, all vehicles operating on the airfield must pay a fee each quarter for permit renewal. The recurring cost encourages tenants to proactively assess whether vehicles are still needed, especially for infrequently used or redundant equipment. Although the quarterly fee is relatively low (five dollars per vehicle) the frequency of payment serves as a regular reminder to maintain compliance.
- A medium city-owned airport implemented a $50 annual registration fee for GSE, which has had the added benefit of incentivizing tenants to remove unused or inoperable equipment from the ramp. This modest increase helped reduce airfield congestion and promote more intentional fleet management across the tenant community.

Mandatory safety inspections at the time of permit issuance or renewal to maintain airside operational safety. With this practice, the permitting process is tightly linked to inspection outcomes, reinforcing the role of physical safety as a prerequisite for continued access.

- A mid-sized city-owned airport requires an annual inspection of all tenant and contractor vehicles before renewing permits. The inspection confirms that vehicles display proper markings (e.g., magnetic logos, lighting, and visible identification) and that safety equipment such as a rotating beacon is present and functional. Vehicles that fail to meet the requirements are denied a permit until the deficiencies are corrected.
- At a large county-operated airport, vehicles are expected to display valid state safety and emissions stickers. Permit requests are denied if the vehicle fails to meet these state-level standards. Additional inspections are conducted randomly or in response to complaints, with the airport operations team authorized to revoke permits or remove vehicles from service if they are deemed unsafe.

Permit quantity limits per tenant, requiring justification for each registered vehicle and encouraging tenants to periodically assess and remove underused or redundant vehicles.

- At a small city-owned airport, all tenant companies receive an annual list of permitted vehicles and are required to verify or update the list before renewing permits. Tenants must identify vehicles to be removed and justify the need for any additions, prompting annual evaluation of actual fleet usage and discouraging accumulation of inactive vehicles.
- At a large authority-operated hub, airport staff initially attempted to assign vehicle access thresholds based on tenant type and activity level; for example, allocating a percentage of total permitted vehicles to passenger carriers versus cargo handlers or hangar tenants. Unfortunately, the formal allocation system encountered tenant resistance and was not fully adopted, although the airport continues to apply access restrictions through other means.

To support these policies, some airports have implemented enforcement mechanisms beyond permit denial. For example, vehicles found operating without a valid permit, with lapsed insurance, or in unauthorized areas may be subject to towing or impoundment procedures. This is particularly common when a vehicle is left unattended in a restricted area or is determined to be inoperable. These measures are typically documented in airport rules and regulations or lease agreements, providing the airport with the legal authority to enforce them. All associated costs are charged to the vehicle owner or responsible tenant.

At airports where these measures have been adopted, tenants report greater attentiveness to permit renewals, insurance compliance, and vehicle removal procedures. The financial and operational consequences of noncompliance serve as a deterrent, improving overall program integrity.

3.4 Consolidated Receiving and Distribution Locations

Airports are increasingly adopting centralized receiving and distribution facilities (CRDF) or consolidated receiving locations as a strategy to enhance airfield security and reduce traffic volume by reducing and controlling vehicle and personnel access. These facilities serve as regulated, controlled facilities where merchandise and consumables are screened and placed in a secure, controlled vehicle prior to movement toward security restricted areas of the airport. This process significantly reduces the number of third-party vehicles and unbadged drivers permitted onto the airfield.

CRDFs are typically managed by third-party operators who are responsible for conducting TSA-required inspections of incoming merchandise and consumables intended for the Sterile Area. The facilities are divided into public and security restricted areas, functioning as restricted-use portals into the secure airfield. After inspection, goods are transferred into a CRDF delivery vehicle operated by properly badged drivers and then transported to their final destinations on the airfield. Under this model, vendors are prohibited from entering the security restricted area with their own commercial delivery vehicles.

Consolidated receiving docks operate under a similar security concept but without a permanent facility or dedicated operator. Vendors deliver goods to a designated inspection location near the secure perimeter, where goods are screened by tenants or designated screening staff. Once cleared, the goods are loaded into tenant-controlled and permitted vehicles for final transport within the secure airfield.

Both approaches share critical operational and security benefits:

- **Minimized third-party access:** Vendors remain outside secured perimeters, significantly reducing the number of vehicles without airport permits entering the airfield.
- **Screening accountability:** All goods and vehicles entering the secure environment are subject to standardized inspections, enhancing chain-of-custody control and supporting TSA compliance.
- **Reduced escort responsibility:** By eliminating the need to escort unbadged drivers, airports can allocate operational and security staff more efficiently.
- **Improved airfield safety and security:** Reducing the number of third-party vehicles operating on the airside decreases traffic congestion and reduces the risk of unauthorized access, security breaches, or incursions involving unfamiliar or untrained drivers.

Additionally, both CRDFs and consolidated receiving docks support operational flexibility. Airports can scale the complexity of inspection and delivery methods aligned with security risk, resource availability, and operational needs without materially compromising access control integrity. This flexibility makes CDRFs an effective option for airports of varying sizes and operational profiles.

PARAS 0024: *Consolidated Receiving and Distribution Facilities at Airports* provides in-depth information on establishing and operating CRDFs and consolidated receiving locations.

SECTION 4: VEHICLE ACCESS GATE POLICIES AND PRACTICES

The development of specific access point usage policies helps tighten control over vehicle movements, improve driver and vehicle credential verification, and close identified gaps in existing access control procedures. Elements of access point policies may include:

- **Limiting vehicle entries and exits** through airfield gates within a specified period to discourage excessive or unauthorized movements
- **Requiring security personnel to scan their own badge** when processing drivers, to log who granted access
- **Validating multiple credentials** at the point of entry, including the driver's airport badge, state-issued driver's license, and vehicle permit, to reinforce layered identity verification
- **Restricting gate usage by company** to restrict tenant or contractor access to designated vehicle gates based on operational need, which reduces opportunities for unauthorized movements across the airfield

These policies promote tighter control of security restricted areas and enhance accountability for vehicle and driver movements.

4.1 Designated Vehicle Gates

Designating specific vehicle access gates for defined operations, construction, stakeholder groups, and traffic management is a common and effective strategy for improving security, managing traffic flow, and tailoring access controls to meet operational demands and mitigate risk. While the use of designated gates may not directly reduce the number of vehicles on the airfield, it allows airports to concentrate security resources, minimize unnecessary cross-airfield travel, meter traffic at vehicles gates, and reduce potential safety hazards and security risks by limiting the distance and duration of vehicles operating within regulated security areas.

At many airports, designated gates are used to separate high-risk or high-frequency vehicle types from general traffic. Common designations include gates for construction traffic, delivery vehicles, catering, emergency services, oversized or specialty vehicles or loads, and tenant-specific operations. This tailored approach not only supports efficient gate operations but also reduces congestion at primary access points and lowers the risk of vehicle incursions or conflicts on the airfield.

Routine gates serving daily operations should be optimized for continuous high throughput and reliability. In contrast, gates supporting irregular operations (e.g., construction or seasonal activities) can be designed with flexibility, often with customized layouts, temporary structures, or tailored gate technology. For instance, some airports opt to staff construction gates with part-time guards or monitor them remotely through cameras and standoff observations by security or LEOs in compliance with the ASP and security regulations.

Other designations include:

- Dedicated gates for fuel and waste-hauling trucks to allow for easier inspections and minimize distance traveled on the airfield by large vehicles
- Catering and vendor deliveries redirected to consolidated receiving locations or screened through dedicated access points

- Vehicle gates restricted for VIP, law enforcement, or security-sensitive traffic, often with specific inspection protocols or escort requirements
- Access points tailored to low-clearance or extra wide vehicles (e.g., flatbeds, cranes, maintenance equipment), with gate geometry and signage adapted accordingly

Airports can require companies to submit a formal justification for alternate gate use, which must be reviewed and approved by security and/or operations management.

Strategic gate designation is an important part of a broader gate operations and staffing model, requiring an analysis of traffic types, anticipated volumes, and operational purpose to determine which gates can remain secured but unstaffed, which support just-in-time staffing models, and which require full-time security personnel presence. Emergency gates, for example, may remain locked or monitored remotely, but be equipped with remote openers to allow immediate access without manual intervention.

In some instances, airports proactively assign vehicle gates to tenant companies, contractors, caterers, and other stakeholders operating on the airfield as a means to meter and control vehicle traffic at the gates and on the airfield. Data from access control transactions, flight schedules, and other historical and predictive data can be analyzed and used to make informed decisions in partnership with Operations, Facilities, Engineering, and affected stakeholders. Communicating these changes to the airport community is critical and can be accomplished using existing messaging systems and platforms. This strategy can be dynamic and implemented temporarily during peak traffic periods, special events and conditions (e.g., construction projects, special movements, staffing constraints).

Through deliberate planning and clearly defined gate assignments, airports can significantly enhance the effectiveness of their airfield security programs while maintaining flexibility for evolving operational needs.

PARAS 0039: *Security, Operations, and Design Considerations for Airside Vehicle Access Gates* offers more details on designated vehicle access gate strategies.

4.2 Facility Design and Boundary Modifications

Deliberate and well-planned facility layout and boundary modifications can help limit security vulnerabilities, streamline ground operations, and enhance access control by minimizing the presence of third-party and non-essential vehicles within security regulated areas.

Consolidating trash collection points by relocating dumpsters and waste facilities closer to vehicle access gates reduces the distance garbage trucks must travel within the airfield. This approach limits how long these high-frequency, large and heavy third-party vehicles spend in security regulated areas and reduces the complexity of their routes. While this adjustment may require terminal tenants to walk or cart waste farther, it substantially reduces unnecessary vehicle activity within the airfield environment, decreasing the potential for safety incidents and access violations.

In a similar effort, transitioning to in-ground hydrant fuel systems allows aircraft to be refueled via fixed piping infrastructure rather than by fuel-laden trucks. These systems are common at large hub airports and are increasingly being explored at medium-sized airports due to their operational efficiency and safety benefits. These systems significantly reduce the presence of high-risk vehicles operating near aircraft by eliminating the need for full-capacity mobile fuel trucks and instead using smaller fuel carts connected to hydrant pits. This lowers the volume of vehicle traffic on the ramp and reduces the burden of escorting or credentialing full-sized fuel trucks.

Several airports have collaborated with TSA to revise security boundary lines, particularly where tenant facilities straddle or border security restricted areas. This often involves amending the ASP to redefine boundaries in ways that remove portions of tenant operations from regulated areas. In some cases, physical modifications, such as relocating perimeter fencing or altering gate access controls, are implemented to support the new boundary layout. These changes are sometimes made temporarily to accommodate construction projects or special events, but in many cases they become permanent improvements designed to limit the number of individuals requiring unescorted access credentials and reduce the need for routine vehicle access by tenant employees.

This approach aligns with recommendations from industry groups, such as the Aircraft Owners and Pilots Association, which advises airport operators to exclude GA facilities from SIDA boundaries when not operationally necessary. By limiting the scope of security restricted areas to those directly supporting commercial operations, airports can avoid imposing disproportionate security burdens on GA stakeholders while concentrating access control measures where they are most critical. This also reduces the number of GA vehicles and personnel navigating airfield areas under commercial security restrictions.

4.3 Shared Transport

Vanpooling is a voluntary but encouraged practice among tenants and contractors to transport employees across the airfield. By consolidating personnel movement into shared vehicles, vanpooling helps reduce the total number of vehicles requiring access to the security restricted area. This also reduces the number of drivers who require unescorted access privileges or escorts.

However, the practice also introduces a few operational trade-offs. At vehicle access gates, vanpools carrying multiple passengers—as well as baggage, tools, or personal equipment—increase the complexity and duration of inspections. Security personnel must verify the credentials of multiple individuals, conduct thorough inspections of property, and sometimes manage separate logs or manifests for each passenger. While this can slow vehicle gate throughput, the overall security posture is strengthened by concentrating access control efforts on fewer vehicles, each carrying a greater number of verified and screened individuals.

Tenant vanpooling is not generally required by airports, as operational needs vary between companies and facilities. However, airport operators often promote or incentivize the practice through tenant communications or lease language. In some cases, airports have supported vanpooling by establishing designated drop-off areas near airfield work sites, allowing shared transportation resources to be used more effectively.

4.4 Management of Prohibited Items

Many airports have experienced challenges related to unbadged drivers, particularly long-haul truck drivers, accessing vehicle gates to deliver aircraft parts, construction materials, and other critical supplies. These drivers often live temporarily in their trucks while in transit across the country and may carry personal items for safety and convenience, including firearms, knives, and multi-purpose tools. While not all these items are universally prohibited under federal regulation, many airports restrict them from entering security designated or airfield areas as a matter of policy and risk management.

The most significant security issue arises when firearms or prohibited items are discovered mid-inspection, triggering a security incident and complex legal, operational, and liability concerns. Once an inspection begins, airports face limited options for several reasons:

- Security personnel at vehicle gates are typically not trained, certified, or equipped to handle, store, or verify ownership of firearms or weapons
- Accepting possession of a firearm could invoke legal responsibilities, including bailment liabilities, and may expose the airport to significant civil risk
- Airports are reluctant to provide secure storage (e.g., gun safes, evidence lockers) for prohibited items at vehicle gates due to the legal and custodial responsibilities such infrastructure would create
- Without proper verification systems, there is no way to confirm lawful ownership of a firearm, raising additional security and legal concerns around returning the weapon

Recognizing the need for proactive solutions, some airports have established or are in the process of establishing new policies and procedures, developed in coordination with airport legal counsel, to address these risks while maintaining efficient access operations. These mitigation strategies include:

- Requiring the delivery recipient (e.g., the tenant or contractor accepting the delivery) to meet the truck driver at a designated location prior to reaching the access gate, allowing prohibited items to be safely divested before submitting to a vehicle inspection
- Adjusting the inspection process to include an initial verbal declaration asking drivers whether firearms, knives, or other prohibited items are present before the formal inspection process begins
- Posting clear signage at vehicle access points, particularly at construction or high-frequency gates, explicitly prohibiting weapons and other common prohibited items on airport property and warning drivers of the restriction and consequences for violations before they enter the inspection queue

These measures can reduce the likelihood of prohibited or unsafe items reaching the airfield, minimize the operational disruptions associated with midfield inspection discoveries, and protect the airport from unnecessary legal and liability exposure.

SECTION 5: VEHICLES IN AIRFIELD CONSTRUCTION SITES

Construction projects on or near airfield operating areas introduce complex security challenges, particularly when contractor vehicles, equipment deliveries, and unbadged personnel require temporary access to restricted areas of the airfield. To mitigate these risks, airports must integrate security controls directly into construction planning and execution processes. A critical tool in this effort is the Construction Safety and Phasing Plan (CSPP), which outlines the operational, safety, and security procedures for managing construction activities within or adjacent to the MA, NMA, AOA, or SIDA.

As outlined in FAA Advisory Circular 150/5370-2G, *Operational Safety on Airports During Construction*, the CSPPs incorporate project-specific access routes, vehicle gate usage, haul path restrictions, escort procedures, credentialing requirements, and boundary controls. By embedding these elements early in the planning process and aligning them with broader access control protocols, airports can ensure that temporary construction operations do not erode long-term security standards.

FAA has developed a sample CSPP that may be useful to airports during construction phases. https://www.faa.gov/documentLibrary/media/Advisory_Circular/150_5370_2F_CSPPSample_RwySealingMarking.pdf

Construction projects on or near the airfield require early coordination to ensure security controls remain intact despite temporary operational changes. During the planning and design phases, security staff collaborate with project teams to:

- Identify the geographic footprint of construction areas and haul routes
- Evaluate the feasibility of fencing the project site outside of the AOA, SIDA, or MA boundary
- Determine where secure boundaries may need to be redrawn
- Review design and project documents to ensure construction activities comply with security standards

Temporarily redefining secure boundaries to exclude construction areas from regulated areas can significantly reduce the administrative and operational burden of badging, escorting, and vehicle inspections. When redefining boundaries is not feasible, additional barriers, signage, and markings (e.g., painted lines, portable fencing, concrete barriers) are used to clearly demarcate security restricted areas and reduce vehicle deviation risks.

PARAS 0037: *Planning and Operational Security Guidance for Construction Projects at Airports* contains more information about managing vehicle access, escorting, and credentialing during construction projects.

5.1 Construction Gate Access and Monitoring

Construction vehicles can be routed through permanent or temporary vehicle gates. Regardless of configuration, gates must support access control and inspections consistent with airport security standards. Gate procedures typically include:

- Badge checks or credential validation
- Identity verification against Stop or Go Lists
- Vehicle permit validation
- Random or scheduled inspections

When possible, a dedicated gate assigned to the project and monitored by an approved contractor, third-party security firm, or airport operations staff trained in gate protocols is the most effective approach. Temporary gates must meet both FAA and TSA requirements, including equipment standards and access control.

Badge readers are sometimes used when the majority of workers are credentialed; however, visual ID checks remain common, especially when dealing with rotating subcontractors. Stop Lists and Go Lists are commonly used. Both lists require daily updates and distribution to affected locations in either hard copy or electronic format to ensure accuracy.

5.2 Escorting Practices on Haul Routes

Escort procedures for construction convoys are often stricter than standard airport worker escorts due to the elevated security risks and dynamic work environments associated with large-scale or airfield-adjacent projects. These elevated risks may include unvetted, unfamiliar, or rotating drivers; vehicles carrying hazardous materials; oversized or slow-moving equipment; and convoys operating near critical infrastructure or active aircraft movement areas. Dynamic work environments can involve shifting haul routes, evolving work zones, and changing airfield conditions that require tighter coordination, communication to airfield operators, and oversight. Common requirements include:

- Lead and rear escorts for construction convoys
- Escort ratio definitions for different types of construction vehicles
- Continuous line-of-sight between vehicles
- Designated routes defined in the CSPP or security plan
- Restrictions on stopping or deviating from route

Haul routes are usually marked with temporary lighting, barriers, and signage to reinforce boundaries. Where haul routes cross operational surfaces, airports can deploy portable traffic lights, flaggers, or radio-equipped escorts to coordinate crossings. Checkpoints may be added along longer haul paths to verify escort compliance and credentials.

5.3 Contractor Credentialing and Driving Limitations

Contractor badging requirements vary greatly based on project scope and timeline. For long-term or high-impact projects, most or all contractor personnel are issued temporary airport badges. Shorter projects may rely on badged supervisors or third-party personnel who escort crews.

Construction-specific badges, distinct from the airport's standard badge, are commonly issued to construction personnel to clearly identify temporary credentials. Badges are usually set to expire at or before the end of the project to reduce risks from unreturned credentials.

Driving training requirements may include project-specific training on gate procedures, access limits, and radio coordination. In some cases, security awareness acknowledgment forms are used to ensure all contractor personnel understand the limits of their access and their responsibility to report suspicious behavior.

SECTION 6: EMERGENCY RESPONSE OPERATIONS

Emergency response operations must balance the need for rapid access with the obligation to maintain perimeter integrity and secure movement within restricted areas. While emergency responders often require expedited access to airfields during critical incidents, airport security protocols must still mitigate risks such as impersonation, unauthorized access, and procedural breakdowns during high-pressure situations, such as VIP movements.

6.1 Designated Access Points for Emergency Vehicles

Emergency response access is typically channeled through designated vehicle gates that support expedited entry while maintaining regulatory compliance. These gates may be permanently designed for irregular operations (e.g., emergencies, special events), and should accommodate large emergency vehicles without compromising security controls. Features supporting emergency gate operations include:

- Remote opening capabilities, enabling security personnel to open gates quickly without requiring additional access control equipment or on-site intervention
- Staging of airport resources (LEOs, operations and security personnel, contract security) to ensure compliance
- Visual verification protocols, where personnel monitor approaching emergency vehicles via CCTV and confirm agency markings or flashing lights
- Designated staging areas, outlined in airport emergency response plans and on signage, to coordinate incoming mutual aid support without disrupting ongoing airfield operations

Irregular or infrequently used gates for emergency access should be equipped with secure ACS and monitored by cameras, especially if not permanently staffed and located in remote areas of the perimeter.

6.2 Dedicated and Co-Located Emergency Services

Some airports have dedicated emergency services to reduce reliance on external responders. These units typically have authorized access to the airfield to maintain constant readiness. In most cases, the first responder personnel are badged to enter the restricted areas of the airport, although not all personnel will have airfield driving privileges. Tiered badging structures can be implemented to limit driving privileges to shift leads or specific roles or ranks.

Some fire stations are located inside the airfield perimeter to eliminate the need for emergency access protocols except under mutual aid activation. Others have been designed to straddle the fence line with two sets of access doors, effectively creating a sally port–style access point that allows the free flow of authorized emergency vehicles. This feature preserves security while enhancing tactical flexibility during emergencies.

Authorized airport emergency vehicles may be registered similarly to tenant fleets, with permits linked to VINs and plate numbers.

6.3 Mutual Aid and External Responders

To reduce risk from impersonation (e.g., cloned emergency vehicles), TSA recommends that mutual aid responders be escorted upon entering the airfield. It is common practice for airports to require that unbadged emergency personnel wait for an escort before proceeding beyond the gate. Escort responsibilities are typically assigned to airport operations, LEOs, or fire personnel, depending on the nature of the response.

Badging and training select shift captains from nearby fire stations grants them direct access through vehicle gates, allowing them to serve as the escort to avoid delays during time-sensitive incidents. These individuals undergo the same training and credentialing as airport personnel, maintaining regulatory compliance and improving response times. Some airports utilize an emergency response badge that is generally distinct from the airport's security badge in color (e.g., white or orange background) or with a visually unique icon or text (e.g., white strip, 'Emergency'). Figure 5 is an example of an airport badge (redacted for security) with gold and white vertical stripes to quickly identify a LEO from a distance.

Many emergency responder vehicles are issued an emergency vehicle authorization license plate (also known as E-plate) or sticker through the state DMV. These provide visual indicators for airport personnel to verify authorization once inside the regulated security area.

Figure 5. Example LEO Badge

SECTION 7: AIRFIELD SECURITY SIGNAGE AND MARKINGS

Airports rely on a combination of visual indicators, pavement markings, and signage to enhance airfield safety, support secure operations, and reinforce driver awareness. These measures help prevent unauthorized access and vehicle deviations, and play a critical role in supporting compliance with federal security requirements and FAA design standards.

A variety of FAA Advisory Circulars (AC) provide technical guidance on airfield design and surface markings. Among the most relevant are:

- AC 150/5300-13 – *Airport Design*
- AC 150/5340-1 – *Standards for Airport Markings*
- AC 150/5340-18H – *Standards for Airport Sign Systems*
- AC 150/5345-39 – *Specification for L-853, Runway and Taxiway Retroreflective Markers*
- AC 150/5345-44 – *Specification for Runway and Taxiway Signs*

A more comprehensive list of federal guidance documents is included in Appendix A.

These standards cover critical safety elements, such as MA and NMA boundaries, but do not cover security elements or boundaries, such as the AOA and SIDA. As a result, airports often develop local visual standards to help communicate security boundaries on the airfield.

The most common solution is a painted red boundary line (Figure 6), used to mark the separation between security restricted and adjacent areas within the AOA, non-security restricted areas, or tenant leaseholds. These markings provide immediate visual cues for drivers and support real-time decision-making on the airfield. Some airports enhance visibility by adding white border lines or reflective paint to the red markings.

Figure 6. Painted Security Boundary

Establishing a “buffer zone” between the AOA and SIDA/Secured Area using two sets of painted lines instead of a single boundary allows for minor, unintentional deviations by authorized vehicles (e.g., brief oversteering, tight turns) without immediately triggering enforcement actions such as an NOV. The buffer serves as a practical compromise, reinforcing boundary awareness while reducing punitive responses to low-risk infractions, especially in high-traffic or spatially constrained areas.

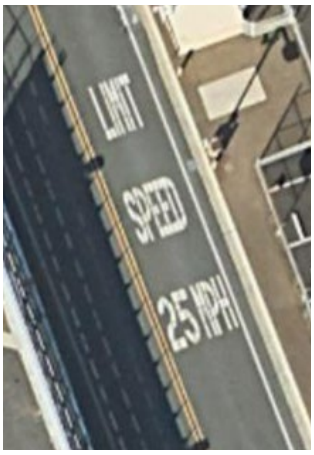
7.1 Supplemental Pavement Markings

Additional surface markings can be deployed to help manage vehicle movements and improve situational awareness. These include:

- Driving lanes and directional arrows to guide traffic around ramps and construction areas
- Color-coded markings to distinguish between different construction haul routes or areas
- Speed limits and large “STOP” messages painted at vehicle holding points and intersections (Figure 7)

Pavement markings are considered highly effective because they are less likely to be obstructed by vehicle placement than physical signs and are not susceptible to being knocked over or displaced. However, maintenance is an ongoing challenge as markings must be frequently repainted and can become obscured by snow, sand, or dirt. Bright colors and reflective paints can greatly enhance visibility and longevity, especially in low-light or low-visibility conditions.

Figure 7. Painted Speed Limits



Some airports have also implemented painted parking outlines and low-profile barriers to define designated parking areas for GSE and charter aircraft. These markings address persistent issues such as GSE blocking active roadways or aircraft parking in unauthorized locations.

7.2 Access Point and Perimeter Signage

Airports are required under 49 CFR §§ 1542.201 and 1542.203 to post signage at all Secured Area and AOA access points and along the perimeter (Figure 8). These signs warn against unauthorized access and are typically supplemented with additional airport-specific language such as state or local penalties. Many airports extend this requirement to tenants through lease agreements, requiring regulated signage to be displayed within leased areas that include or share a border with the Secured Areas or the AOA.

Figure 8. Secured Area Signage

Common security signage observed at vehicle gates and perimeter fencing/boundaries includes:

- Firearm and weapon prohibition notices, often citing relevant local, state, and federal laws (Figure 9)
- Lists of prohibited items, such as alcohol, tools, or knives
- Restricted area notices, including “Restricted Area – Authorized Personnel Only”
- GA/SIDA boundary signage to reinforce regulatory distinctions (Figure 10)
- “Fire Access Only” signs on emergency vehicle gates

Figure 9. Airport-Specific Signage

Figure 10. SIDA Signage

Placing signs at critical decision points, such as intersections or access road forks, is particularly helpful for new drivers who are unfamiliar with the layout.

In some cases, flashing lights are installed near or around the signs to draw attention in high-traffic or low-visibility areas. However, care must be taken to avoid light spill or glare that could interfere with aircraft operations or pilot visibility. Figure 11 shows a lighted vehicle gate arm at an airfield access point that enhances visibility and situational awareness of drivers approaching the access point at night.

Figure 11. Illuminated Gate Arm at Night

7.3 Maintenance and Adaptation

While signage is essential, it comes with physical limitations. Stop bars, poles, and signs are vulnerable to vehicle strikes, particularly near tight corners and temporary haul routes, or during snow removal operations. Routinely reassessing and repositioning signage based on traffic flow observations or incident trends allows the airport to address repeated challenges more effectively. Temporary signs are often deployed near construction areas or detour routes to reduce confusion and maintain compliance.

If signage has been moved or altered, it is important to ensure all related materials (e.g., training guides, airfield maps, driver diagrams, security orientation content) are updated where necessary. Inconsistent language or outdated visuals in training documentation can lead to confusion, misinterpretation of boundaries, and unintentional violations by personnel who rely on those materials for situational awareness. Ensuring alignment across physical signage and reference materials helps reinforce proper behavior, reduces risk, and supports compliance with access control protocols.

SECTION 8: VEHICLE ESCORTING PROGRAMS

TSA regulations impose strict requirements for escorting individuals without unescorted access privileges into security restricted areas of the airport. Under 49 CFR § 1542.211(e) *Identification systems*, airport operators must ensure that individuals without credentials are under positive escort at all times. This means the escort must maintain continuous visual contact with the individual, and be able to monitor the individual's activity and challenge unauthorized access or behavior when necessary. Escort program requirements include:

- Training requirements for individuals prior to authorization to escort, including procedures for summoning law enforcement and local escort procedures
- Approval processes for escorting requests and procedures, as well as a process to justify escort authority and confirm that escort privileges are essential to job duties
- Visual indicators on airport-issued badges identifying escort authority

Airports can define responsibilities of individuals authorized to escort vehicles on the airfield through local policies and procedures, including:

- Escort personnel must possess both escort and airfield driving privileges when escorting vehicles.
- Escorts must be in control of the escorted vehicle, either by driving it directly or operating a lead or pilot car; escorting from the passenger seat is not permitted.
- The escort assumes responsibility for the individual and/or vehicle being escorted and may be held liable for any incidents, with some airports requiring that the escorted vehicle be covered under the escort's insurance.
- Escorts must brief the escorted individual prior to entry, outlining expectations, restrictions, and operational protocols.

These responsibilities are typically formalized in the airport's rules and regulations to support consistency and accountability across tenant, contractor, and operations personnel.

PARAS 0035: *Synthesis of Escort Privileges and Escorting Practices* provides a synthesis of airport escorting practices and privileges that airports may also find useful.

8.1 Specialized and Enhanced Escort Protocols

Airports tailor their vehicle escorting programs to local operational needs, tenant behavior, or unique facility layouts. Examples of tailored protocols include:

Requiring advance notification to operations and control towers before entering MAs:

To ensure airside coordination and mitigate risk in MAs, airports may require advance notice of vehicle escort activities that will enter or cross taxiways and runways. Notifications are submitted to airport operations, ramp control, ATC, and/or dispatch prior to movement. This allows stakeholders to review the request, assess potential conflicts with aircraft operations, and ensure proper escort staffing. Entry into MAs without prior approval may trigger enforcement actions.

Restricting tenant escorting to employees actively engaged in the badging process:

To prevent misuse of escort authority and reduce the risk of unauthorized access, airports may only allow tenants to escort individuals who have formally initiated the airport's badging process. This

policy ensures that only vetted individuals who have submitted identification, completed training, or are awaiting fingerprint results may be escorted by tenant representatives. It limits escorting to those with a legitimate operational need and a verified path toward unescorted access.

Requiring pre-coordination with field maintenance or operations staff for heavy equipment escorts:

Large or slow-moving equipment (e.g., cranes, pavement rollers, lifts) presents unique challenges for airfield escorting due to their size, limited maneuverability, and potential interference with aircraft movement or visual lines of sight. At some airports, tenants must coordinate these movements in advance with field maintenance or airside operations to schedule access during low-traffic periods, identify safe haul routes, and assign qualified escorting personnel.

Requiring that concession vendor deliveries be escorted by designated airport security or operations staff in restricted areas:

To maintain tight control over delivery traffic on the airfield, airports may require that only airport-designated personnel escort concession vendors through secured airfield routes. This ensures consistency in escort practices and removes variability in how access is managed, especially for vendors who rotate frequently or use third-party logistics providers who are unfamiliar with airport-specific driving rules.

Requiring escorted passengers inside vehicles to present government-issued identification, which is logged at the gate:

To maintain a clear record of who is granted temporary airfield access, individuals under escort must present a valid government-issued ID (e.g., state driver's license, passport) before entering the security restricted area. This information is manually or electronically logged by access gate personnel to ensure traceability and facilitate enforcement if violations occur. This requirement also supports incident investigations and access audits.

Temporarily revoking privileges of badge holders with a history of airfield driving violations to "escorted-only" status:

Airports generally use progressive enforcement systems that limit driving privileges for individuals with repeated airfield violations, such as speeding, failure to yield, or improper entry into restricted areas. In such cases, the badge holder may be required to operate under escort until completing remedial training and all corrective actions. This approach promotes accountability while allowing continued access under controlled conditions.

Restricting escorted vehicles to specific access points for enhanced screening:

To better control and monitor escorted vehicle traffic, escorted vehicles can be restricted to designated access gates equipped for additional screening. These checkpoints may include pull-off areas for inspection, rejection lanes, specialized staff trained in vehicle inspection and escort protocols, or technology such as ALPRs. This ensures a higher degree of control over the movement of escorted individuals and vehicles.

These special policies and protocols are generally formalized in the airport's rules and regulations.

The following case study demonstrates a tailored escorting program that one interviewed airport developed in coordination with TSA and tenants to manage a specific type of airfield event.

The airport has an aviation museum located a few hundred feet within the secured airfield, with no public access point. Multiple times a year the museum hosts fundraising events where the public is invited to the facility as a special event. To safely escort members of the public during these events, the airport, TSA, and museum leadership developed a multi-escort handoff procedure:

1. The first escort approaches the arriving vehicle outside the gate, explains the rules, and initiates the escort process.
2. A second escort, positioned at the vehicle gate, opens the gate upon the first escort's signal and ensures that no other vehicles enter.
3. Traffic cones are used to mark an approved path through the airfield, avoiding any restricted areas. The first escort walks with the vehicle along the route until the third escort, stationed at the museum entrance, confirms visual control and assumes responsibility.
4. The third escort completes the escort process, guiding the vehicle to its designated parking area.

This process is reversed for vehicle departure, maintaining continuous positive control while allowing public access for limited, TSA-approved events. It serves as a strong example of a coordinated, layered escorting model adapted to a non-standard operational environment.

8.2 Escort Privilege Eligibility and Authorization

In accordance with TSA regulations, escort privileges are not universally granted to all airport badge holders. Instead, these endorsements are typically requested during the initial badging process by the individual's AS and must be justified based on operational need, consistent with TSA regulations. As with requests for vehicle driving privileges or airfield access, escorting authority is considered an additional security function that grants a heightened level of responsibility. At many airports, this authority falls under the purview of the airport security department, with approval and oversight responsibilities often assigned to the security manager or credentialing department.

Escorting requests may be submitted on the individual's badging application or a separate Escort Authority Request Form, which may include screening questions such as duration of employment at the airport, and role consistent with operational need or leadership status (e.g., supervisor, trainer, manager).

These additional checks allow the security manager to make informed decisions and reduce the likelihood of authorizing escorts who may not fully understand or comply with security expectations.

Some airports impose additional criteria beyond operational need to qualify for escorting privileges—for example, requiring that individuals must have worked at the airport for at least six months before becoming eligible for escort status. This policy ensures the individual has demonstrated familiarity with airport rules, layout, and operations, and also limits potential escorts to those who have demonstrated some level of reliability.

Assigning a limited number of escort authorizations to each company ensures that the privilege remains tied to a defined operational need and is granted judiciously. This approach conforms with TSA security requirements, prevents excessive distribution of escort authority, and facilitates control, oversight, and compliance tracking.

Several airports reported that they previously granted escort privileges to private pilots and hangar leaseholders, but they had since revoked escort privileges from this population after incidents involving unauthorized vehicle movements and surface deviations while under private tenant escort. Now, such privileges are granted only on a case-by-case basis, and often with enhanced scrutiny.

Once escort privileges are approved, escort training must be completed before escort authority is granted. Some airports meet the requirements under 49 CFR § 1542.213 *Training* by incorporating escort procedures into their SIDA training curriculum, while others provide separate or supplemental escort-specific training once escort privileges are approved. This training reinforces the seriousness of escort responsibilities and supports compliance with the airport's broader access control program. Upon completion of all required training, the badge is issued with the escort authority indicia, which access control staff use to verify authorization at vehicle gates, checkpoints, and other access points.

8.3 Escort Authority and Escorted Vehicle Indicators

Effective escorting programs rely on clear, visible indicators to distinguish both authorized escorts and vehicles operating under escort. These identification methods enable security and operations personnel to quickly confirm escort status, support compliance checks, and trace escort responsibility during audits or incident investigations.

8.3.1 Badge Indicators for Escorting Privileges

All airports use some form of badge-based visual indicator to identify individuals with escort authority, in compliance with federal regulations. These markings are typically integrated into the printed badge itself and serve the dual purpose of real-time verification at access control points and visible reinforcement of the badge holder's responsibilities. Common identifiers include:

- Letters or text such as "E," "ESCORT," or "EA" (Escort Authority) displayed on the badge face
- Color-coded backgrounds or strips indicating different levels of access and authority
- Specialized codes or labels for role-specific escorting, such as a "P" (for Pilot) used to designate escorts on construction haul routes

Some airports use serialized, tamper-evident stickers affixed to the badge rather than reprinting the credential. These stickers are linked to the badge number in airport records, allowing fast verification and streamlined tracking. If an escorting violation occurs and an NOV is issued, the sticker can be removed immediately to suspend escorting privileges without requiring a badge reprint, making this approach efficient for airports seeking administrative flexibility.

8.3.2 Vehicle Identification for Escort Operations

When escorting vehicles, most airports require a clearly visible indicator placed on or inside the vehicle to signal that it is operating under escort and to identify the responsible party. This practice supports compliance with positive escort requirements and helps airport personnel distinguish escorted vehicles from those with full operating privileges.

Many airports use reusable dashboard placards or hang tags to indicate a vehicle is under escort. These indicators often include:

- The airport's logo
- A serialized placard number tracked by the security office
- An expiration date or color-coded design to indicate current validity

Placards are generally placed on the dashboard, while hang tags are suspended from the rearview mirror for visibility. The serial number allows airports to maintain control over issued placards and track their return. Placards are reprinted in new colors, typically annually or quarterly, to make outdated versions

easy to identify. While quarterly reprints offer better control, they also result in increased administrative and printing costs.

Requiring visitors under escort to surrender a government-issued photo ID and provide a contact number when receiving a vehicle placard adds an extra layer of traceability and accountability. This practice helps link each placard to a specific individual, facilitates post-access follow-up if necessary, and discourages misuse by reinforcing the temporary and controlled nature of the escort process.

Some airports implement a fixed-series placard strategy, assigning a set of serialized placards to each tenant or contractor and conducting annual audits to verify control and accountability. Rather than issuing placards with individual expiration dates, this approach ties placard validity to the integrity of the entire series. If a significant number of placards are unaccounted for during an audit, the airport may invalidate and reissue the full set, reinforcing tenant accountability and maintaining control over escorted vehicle access.

In the event of a lost or unreturned placard, the airport can add the corresponding serial number to the vehicle stop list, preventing unauthorized reuse and triggering recovery or replacement protocols.

Escort-specific vehicle forms can be used in place of generic placards. These forms are filled out at the gate and left on the vehicle dashboard while the vehicle is operating under escort. Information collected typically includes:

- Driver's license number and contact information
- Vehicle make, model, and license plate
- Name of the escort and date of authorization

In some programs, the form must be retrieved upon exit, creating a closed-loop control measure that confirms the escort process was completed and allows reconciliation of the documentation against gate logs.

Some airports have explored the practice of issuing GPS tracking devices to drivers under escort. While this strategy offers a potential security benefit, its practical implementation has proven difficult. In trial programs, airports struggled to establish a reliable check-in/check-out process that ensured devices were returned after use. Without a controlled handoff, devices were often misplaced, forgotten in vehicles, or accidentally removed from service without notice. Even when recovered, devices frequently lacked sufficient battery charge for the duration of the escort period or had not received necessary software updates, rendering them ineffective during actual field use.

8.4 Escort Frequency Limits

While escorting is a necessary means of providing temporary or short-term access to security restricted areas, improper use of escort privileges can introduce security vulnerabilities, particularly if used to circumvent badging requirements. To prevent unvetted individuals from gaining prolonged access to security restricted areas, airports can implement strict limits on how often a person may be escorted before being required to apply for a badge. These thresholds typically range from 5 to 30 visits per calendar year, with each day of access counted as one visit, regardless of duration. Once the threshold is met, the individual must undergo the standard badging process.

This threshold-based approach serves several functions:

- Closes the escorting loophole often exploited by individuals seeking to avoid badging due to anticipated disqualification, existing disqualification, or other reasons
- Promotes accountability by ensuring escorting remains a temporary privilege rather than a substitute for credentialing
- Supports risk-based access control, applying additional scrutiny to frequent or recurring visitors

Flexible extensions may be granted by security management for defined short-term needs, such as limited-duration maintenance contracts. For example, allowing extensions beyond the standard 30-visit cap, but enforcing a hard-stop on further escorting after the sixtieth visit.

Automated systems, such as online portals or mobile applications, can be used to streamline escort request approvals and automatically flag when individuals approach or exceed visit limits. These tools reduce administrative burden, enforce policy in real time, and encourage early transition to the badging process for recurring visitors.

Where automated systems are not available or in use, manual tracking through visitor logs or digital spreadsheets allows gate personnel or security teams to monitor escort activity. Collecting basic information at the gate (e.g., name of visitor and other biographic information; ID number; name of escort and company performing escort function; duration of stay) enables security personnel to cross-reference against access history and internal security watch lists and stop lists.

Some escort request forms also require the requester to estimate the number of days escorting will be needed. This information allows credentialing or operations staff to flag repeat or prolonged access patterns that may exceed typical use.

8.5 Escort-to-Vehicle Ratio

Escort ratios are a critical factor in maintaining positive control and reducing airfield congestion. TSA requires escorts to maintain continuous visual contact with and control of all individuals and vehicles under escort but does not prescribe specific numeric ratios. As a result, airport operators are expected to define ratio policies that reflect their operational realities and security environment.

Airports use two primary approaches to define their escort ratios:

- Fixed ratios written into the ASP providing clear limits and simplifying enforcement
- Flexible guidelines to offer discretion based on vehicle type, purpose, and airfield traffic

Examples of fixed or conditional ratios include:

- A 1:1 escort ratio for non-airport employees, high-risk vehicles, or sensitive deliveries
- A 1:3 ratio for commercial or passenger vehicles in convoys with visible spacing and cooperative drivers
- Conditional limits based on vehicle type, such as 1:1 for dump trucks or heavy equipment versus 1:3 for smaller passenger vans
- Designated exceptions for authorized personnel, such as law enforcement or airport operations, to escort larger convoys (e.g., 1:4 or more)

Escort ratios may be adjusted for special operations or planned convoys, such as construction deliveries, chartered team transport, or funeral processions. In these cases, the airport may permit a higher number of vehicles to be escorted when both a lead vehicle (pilot car) and a rear escort are used to maintain control of the convoy.

8.6 Escort Management Systems and Request Platforms

Escort program tracking methods vary significantly depending on visitor volume and policy strictness. In low-volume environments or where escorting is heavily restricted, a manual log sheet that is later entered into a tracking spreadsheet may provide adequate recordkeeping. This method supports basic identification of repeat visitors, helps enforce visit thresholds, and maintains a record for audits or investigations.

Airports managing more frequent or complex escort activity may implement online portals where users can submit escort requests. These portals collect the escorting party's details, visitor credentials, purpose of visit, and time range requested. Submitted forms are routed to the security department for approval, and accepted entries are imported into a tracking database.

Advanced platforms may include features such as:

- Automated alerts when individuals approach or exceed escort visit thresholds
- Built-in badging triggers, prompting the user to begin the credentialing process
- Data exports for historical analysis or integration with IDMS

This approach supports a more scalable, proactive escort program, reducing manual enforcement and helping airports maintain compliance with TSA requirements for visitor supervision.

SECTION 9: TECHNOLOGY IN SUPPORT OF AIRSIDE VEHICLE SECURITY OPERATIONS

A diverse array of technologies is used at airports to manage and secure vehicle access to and operations on the airfield. These tools range from simple spreadsheets and mobile electronic forms to fully integrated systems and automated platforms. Technology selection and deployment strategies vary by airport size, layout, and resource availability.

Airports are increasingly moving toward automated systems that alert staff to deviations or violations, allowing personnel to focus on other critical functions without reducing situational awareness. Rather than relying solely on continuous manual monitoring, many airports are adopting event-based notification systems, particularly in low-traffic or infrastructure-limited areas. This strategic approach supports real-time responsiveness while reducing staffing burdens.

Tenants operating along the perimeter or within Exclusive Area Agreements (EAA) or Airport Tenant Security Programs (ATSP) may also install and manage their own access and surveillance systems. While these tenant-operated systems can supplement airport security, airports typically do not have real-time access to the footage or logs. Coordination for data sharing is usually outlined in lease terms, MOUs, or security agreements and should be actively managed to ensure continuity during response and investigation activities.

More information on tenant-controlled technology systems is included in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*.

9.1 Vehicle Gate Access Control

A robust and flexible ACS is foundational to securing the airfield at vehicle access points where infrastructure, operational needs, and tenant relationships introduce significant complexity. Access control technology enhances security most effectively when used as a tool for intentional segmentation, traceable accountability, and layered verification. Airports that align technology deployment with operational planning, credential management, and emergency response readiness are best positioned to manage secure, flexible, and resilient vehicle access systems.

A centralized ACS operated by the airport authority offers the greatest control and visibility over vehicle access. However, full ACS coverage is rarely feasible, particularly at legacy facilities, tenant-leased buildings, or remote perimeter gates. In these areas, tenant-operated systems often supplement airport control, especially under EAAs/ATSPs. While these distributed models are sometimes necessary, they also create variability in enforcement and oversight, requiring airports to establish clear governance policies and auditing procedures to maintain uniform security standards.

Moving away from single-factor authentication (e.g., badge swipe only, cipher lock codes) toward multifactor systems (e.g., badge swipe + PIN, biometric + badge) greatly enhances security by preventing access by unauthorized individuals who may have stolen a badge or observed a code as it was entered. This layered access requirement also creates an opportunity to enforce just-in-time access and log user activity, further enhancing audit trails and accountability.

A small city-owned airport selected an ACS platform already in use by other municipal departments (e.g., police, fire, and city employees) to allow shared badge use across multiple city facilities, including the airport. Each city department maintains its own database to track and manage badge holders, but the

system allows access privileges for different facilities to be added to a single ID media. This reduces the number of badges that must be issued, authorized, and carried. This approach also enables the city's IT department to support and manage the system without needing to learn or maintain a separate platform, improving efficiency and continuity across departments.

To address infrastructure and operational variability, airports deploy a mix of access control technologies, each chosen based on the risk profile, frequency of use, and physical constraints of the access point being secured. Commonly used technologies include:

- **Automated ACS** at high-traffic gates, often requiring multifactor authentication for vehicle entry
- **Passenger-side badge readers,** used to validate passenger airport credentials without granting access, allowing verification of all occupants during vehicle inspections
- **Cipher locks and lock-and-key systems** at low-frequency gates or tenant doors, though they lack logging capabilities and are increasingly being replaced
- **Portable badge readers and mobile driver's license scanners**, used for temporary construction gates, special events, or random inspections where network infrastructure is limited
- **AI-based access monitoring** used to detect tailgating, piggybacking, or unauthorized escorting and provides a real-time alert to security personnel to review and respond; particularly effective in unstaffed or low-visibility areas

These technologies are most effective when deployed with a security purpose in mind, such as isolating access points by role, enforcing auditability, or supporting real-time enforcement actions.

9.1.1 Access Control Permissions

An ACS is most powerful when tightly integrated into the badging process and daily airfield operations. During the credentialing phase, the AS can submit a list of gates or areas the individual needs to access based on job duties. This list can then be used to set access permissions within the ACS.

Role-based access configurations allow airports to control gate access by defined user groups (e.g., fuelers, airline employees, delivery drivers, emergency responders), reducing the administrative burden of managing permissions individually. For example:

- Vehicle access may be segmented by SIDA vs. AOA
- Further refinements may allow or restrict access based on specific EAAs, tenant locations, or time-of-day rules
- Special access groups can be created for construction crews, vendors, or seasonal operations, enabling temporary but controlled access

By aligning access permissions with operational roles and integrating them into the credentialing process, airports can enhance security, streamline gate control, and reduce administrative workload while maintaining flexibility to meet evolving operational needs.

9.1.2 Access Control Challenges and Contingency Planning

Despite its advantages, ACS deployment is subject to practical constraints:

- Network and power limitations can restrict the use of mobile badge readers or advanced authentication capabilities at remote perimeter gates and on the airfield

- Gate-level failures may create unplanned detour routing, where a driver's credential may not allow access to an alternate gate
- Temporary infrastructure (e.g., during construction) may lack connectivity to support standard access equipment

To mitigate these risks, airports can develop contingency plans within their ASP or SOPs that account for manual overrides by authorized personnel; temporary access adjustments through portable systems; procedures for rerouting vehicles; and procedures for ensuring alternate gate access is logged, approved, and time limited.

PARAS 0017: *Access Control Card Technology Guidance* offers more in-depth guidance for access control technology.

9.2 Surveillance and Detection Systems

Surveillance and detection systems are a core element of an airport's airfield security, particularly for airfield vehicle operations. While camera coverage alone is not sufficient to secure the airfield, when strategically integrated with an airport's ACS, inspection protocols, and airfield operations, it can significantly improve situational awareness, support rapid incident response, and deter unauthorized access. These tools are most effective when paired with analytics or access validation protocols that trigger alerts or initiate manual verification procedures.

9.2.1 CCTV Systems

CCTV systems are widely used to monitor ramp areas, taxiways, vehicle gates, and perimeter fence lines. Optimized systems place cameras at strategic points that offer overlapping coverage, particularly at vehicle gates and high-risk access points, enabling forensic after-action review and incident reconstruction. Overlapping fields of view are essential for ensuring full scene capture and reducing the likelihood of blind spots or ambiguous footage.

Cameras trained on perimeter fencing and access points are often angled to monitor specific gate hardware and latching mechanisms for signs of tampering. This supports both real-time detection and forensic investigation.

While many airports operate centralized camera networks, others use a hybrid model in which tenants manage their own surveillance systems through lease agreements or EAAs. In these cases, the airport generally does not have real-time access to tenant footage but can request video following an incident. Lease language or security agreements often define the terms for footage retention, access, and cooperation in investigations.

Tailoring the resolution, field of view, and storage parameters to the function of each camera is crucial to a well-designed surveillance system. Cameras used for vehicle inspection or identity confirmation may require higher pixel density or zoom capabilities, while those used for detection and movement tracking may prioritize coverage and analytics support over image clarity.

More information on surveillance systems at airports can be found in PARAS 0034: *Optimization of Airport Security Camera Systems*.

9.2.2 Long-Range and Thermal Cameras

Long-range pan-tilt-zoom cameras mounted on control towers or elevated poles are used to monitor remote areas and supplement physical patrols. These cameras can track the movement of vehicles across open ramp areas or haul routes, allowing operations or security personnel to observe activity from centralized command centers without requiring constant physical patrols.

Many long-range cameras are equipped with thermal imaging capabilities, allowing them to detect movement in low-visibility conditions such as fog, night operations, or glare. While these cameras are typically procured for airfield safety monitoring, the security department often has access to the feed for real-time situational awareness or post-incident investigation. In this way, safety and security departments can share assets and collaborate on coverage needs across the airfield.

When deployed in support of security objectives, long-range and thermal cameras offer a valuable force multiplier. They are particularly useful during high-risk operations, such as VIP charter movements or high-volume construction projects where unescorted vehicle deviations must be quickly detected and addressed.

9.2.3 Virtual Gates and Fences for Non-Barrier Control

Virtual gates and fences are scalable solutions for managing access across complex or constrained airfield layouts, particularly where traditional physical barriers (e.g., swing arms, fencing, manned posts) are impractical. Virtual gates are most effective when deployed in areas where vehicles need access across controlled lines (e.g., AOA to SIDA) without disrupting aircraft movements.

When a vehicle approaches, the driver may be required to hold their badge up to a camera being monitored by a video operator who confirms authorization and signals entry approval. If a vehicle bypasses the gate, an alert is automatically triggered in the operations center and security or law enforcement is dispatched. Key components of a virtual gate include:

- Painted pavement markings (e.g., red stop lines or “STOP” warnings)
- Visual cues such as red/green lights or flashing indicators
- High-resolution, zoom-enabled cameras positioned to verify credentials remotely
- Operators in an access control center who monitor the feed, verify the badge, and provide real-time entry authorization or intervention

Virtual fences are ideal for maintaining regulatory separation between areas without installing permanent infrastructure. They are most effective for controlling aircraft-only access or delineating temporary boundaries during construction. Components of virtual fences include:

- Visual delineators such as portable barricades or painted lines
- Cameras with object detection analytics that trigger alerts if a person or vehicle crosses the boundary
- Radar and thermal sensors to support slew-to-cue camera panning, allowing cameras to automatically focus on moving targets

If an object, person, or vehicle crosses the virtual boundary, the system will alert the operations or security department to investigate further.

The following case study highlights how virtual fencing technologies can provide an adaptable, cost-effective solution for complex airfield layouts where physical barriers are either infeasible or operationally disruptive.

At one interviewed airport, a tenant operating an aviation technology facility maintains a hangar with direct access to an active taxiway. This created a regulatory challenge as the layout allowed tenant employees to cross into the AOA without passing through a TSA-regulated access point. The arrangement raised concerns from TSA who required the airport to establish a clear security boundary that would not disrupt the tenant's aircraft operations. The airport evaluated three potential solutions:

1. **Badge all 500 tenant employees, granting each individual unescorted access to the AOA**
   Rejected due to cost, administrative burden, and TSA concerns about widespread credentialing without operational need
2. **Construct a physical fence and install a gate for aircraft access**
   Rejected as impractical, as the taxiway was in frequent use and would require complex scheduling and escorting for every aircraft movement
3. **Implement a virtual fence using radar and thermal cameras**
   Ultimately chosen for its scalability, visibility in all weather conditions, and ability to maintain unimpeded aircraft operations while satisfying regulatory boundaries

The virtual fence solution, currently being commissioned, uses radar sensors to detect movement across the designated boundary area. When a person, vehicle, or object enters the detection area, the system triggers a slew-to-cue function, prompting nearby thermal and high-resolution cameras to automatically pan to the source of movement to facilitate real-time visual confirmation.

9.2.4 Automated License Plate Recognition Systems

ALPR systems are increasingly used at vehicle access gates to automate the screening of inbound vehicles. These systems can check license plates against internal stop lists, state motor vehicle registration records, and law enforcement databases such as the National Crime Information Center. This provides an additional verification layer and allows security personnel to focus on inspections and driver screening.

AI-enhanced ALPR systems can significantly improve reliability and accuracy by compensating for common issues such as plate glare, angled entry, or poor lighting. Camera placement and height should be carefully matched to the expected vehicle types and approach patterns. Integration with the airport's ACS can allow the system to automatically deny access to flagged vehicles or log an alert for further evaluation.

9.3 Perimeter Monitoring and Vehicle Tracking Technologies

Layered surveillance systems and vehicle tracking technologies allow the airport to secure the airfield perimeter, detect unauthorized movements, and improve real-time awareness of ground operations. These tools are especially important in areas with limited physical visibility, infrequent patrols, or heightened vulnerability, such as remote fence lines, construction areas, and taxiway crossings.

Perimeter and vehicle tracking technologies are most effective when deployed as part of a layered security strategy, combining fixed infrastructure (e.g., perimeter systems, CCTV) with mobile and data-driven tools (e.g., GPS, RFID, geofencing).

9.3.1 Perimeter Intrusion Detection Systems

Perimeter intrusion detection systems (PIDS) remain a critical component of perimeter protection, particularly in low-traffic or remote areas of the airfield such as wooded areas, water boundaries, and underutilized service roads. PIDS technologies include fence-mounted sensors, ground-based radar, buried cables, and vibration detection systems, which alert airport personnel to unexpected activity detected near the fence line. To maximize the effectiveness of these systems, airports can:

- Integrate CCTV cameras with PIDS to provide visual confirmation of alerts and reduce false positives
- Deploy thermal and infrared imaging in low-visibility areas, particularly for use during night operations and adverse weather
- Install mobile or solar-powered cameras in areas without reliable power or fiber infrastructure
- Combine analytics-enabled cameras with ground-based motion detection to help distinguish between actual breaches and environmental disturbances

These systems enable efficient allocation of patrol resources, allowing law enforcement and security personnel to focus on higher risk areas while maintaining continuous coverage of less active sections.

PARAS 0015: *Guidance for Airport Perimeter Security* offers additional information on securing the airfield perimeter.

9.3.2 Geofencing and GIS-Based Alerting

Virtual boundaries, or geofences, are used to monitor access control and vehicle movement within the airfield. By defining geographic perimeters through geographic information systems (GIS) or GPS platforms, airports can track when vehicles or equipment cross into unauthorized areas. Geofences can also help ensure PNO-designated or GSE vehicles remain within their assigned areas, triggering alerts if they deviate. This virtual zoning approach is especially useful for:

- Temporary operational changes during construction or special events
- Remote enforcement in areas where physical fencing is impractical
- Automated security alerts for unauthorized boundary crossings

To further support situational awareness, airports can use GIS-based applications that allow NOVs to be tagged by location, creating a live map of violations to support trend analysis and identify repeated weak points on the airfield.

9.3.3 Vehicle Tracking Technologies

Airports may supplement their perimeter protection by tracking the location and movement of airport-owned vehicles using GPS, RFID, or Automatic Dependent Surveillance–Broadcast (ADS-B) transponders (“squitters”). These technologies allow operations and security staff to reconstruct movement paths following an incident, locate a missing or stolen vehicle, and forensically verify that a vehicle remained within its authorized area.

Operational vehicles most commonly outfitted with trackers include airfield maintenance trucks, fire engines, police vehicles, snowplows, and fueling vehicles. In most cases, these tracking systems are only installed on airport- or city-owned vehicles; tenants or FAA entities may use similar systems on their vehicles, but the airport does not typically have access to that data.

Some systems can alert the airport if a tracked vehicle crosses a geofence, exits the airfield, or enters a restricted area. While real-time monitoring is not always feasible due to staffing or system limitations, the ability to generate alerts or conduct retrospective analysis is valuable for both compliance and investigations.

Tracking systems can also be used to automate and monitor escorting compliance. The escort and their escortees are issued locators and the system is configured to know which is which. After setup, the system will alert if any of the escortees move more than a specified distance (as low as 12 feet) away from the escort.

This approach has some administrative burdens, including tracking which device was assigned to which driver, verifying that location data synced properly with access logs, and replacing damaged or malfunctioning units. Without a dedicated staff or automated system to manage the device life cycle—including charging, resetting, and data download—the program may create more operational risk than it mitigates, particularly when attempted without full integration into the airport's security framework.

In response to concerns about the unauthorized use or theft of airfield vehicles, some airports have considered equipping select assets with remote or automatic disabling mechanisms. These technologies, including immobilizers and ignition kill switches, offer the capability of stopping a stolen or misused vehicle before it reaches a critical area of the airfield. Coordination is needed between security, operations, legal, and tenant stakeholders to determine liability in the event of equipment failure, vehicle damage, or injury while using vehicle disabling devices. Without carefully documented SOPs and real-time communication protocols, the devices could introduce more risk than they resolve.

9.4 Management Software

A range of software systems and custom-built tools are used by airports to support secure and efficient management of vehicle operations, including permitting, escort authorization, driving privileges, incident tracking, and training compliance. The choice of system is generally dependent on the airport's size, staffing, and operational complexity, with larger airports favoring integrated platforms and smaller airports using off-the-shelf products customized for their specific needs.

9.4.1 Commercial Software Suites for Complex Environments

Many larger airports with highly complex operational environments rely on commercial software platforms, often customized in collaboration with the vendor, to handle multiple access control management and tracking functions. These platforms are usually modular and scalable, allowing the airport to implement new functionality over time without overhauling core systems. These systems are often configured to manage:

- Vehicle permit application and tracking
- Escort request logging and usage thresholds
- Driving and escort authority assignments
- Incident and NOV tracking
- Inspection scheduling and compliance logs
- Visitor vetting and approvals
- Security and safety event reporting

When integrated with an existing IDMS, these modules allow for real-time status updates, streamlined credential issuance, and automated enforcement triggers, such as flagging drivers with expired training or escorted individuals who exceed visit limits. In some cases, data is cross-referenced to generate compliance reports by company or area of operation.

9.4.2 Adaptable Tools for Streamlined Environments

Airports with fewer airfield vehicle operations or limited budgets often rely on flexible, low-overhead tools such as spreadsheets, digital form builders, and basic databases. Online survey tools and form builders allow security and operations personnel to:

- Fill out forms in the field via mobile device or tablet
- Attach supporting images, videos, and location data
- Automatically populate online databases
- Evaluate the data with built in filtering, sorting, and data analysis features

Spreadsheets used for NOV tracking are structured to allow users to filter for repeat offenders, identify companies with multiple or recurring violations, and flag similar violations that may indicate systemic issues in access control, signage, or training. Airports can also generate graphs or charts from these logs to track weekly, monthly, or annual violation trends and share summaries with stakeholders or governing bodies.

SECTION 10: AIRFIELD SAFETY PRACTICES SUPPORTING SECURITY OBJECTIVES

Airfield safety and security programs share the same foundational goals of preventing incidents, protecting people and assets, and maintaining operational continuity. While traditionally managed through separate processes and oversight structures, many safety practices have proven highly effective in supporting airport security objectives, particularly in vehicle access management, situational awareness, and compliance enforcement. By leveraging these overlaps, airports can maximize the impact of existing safety protocols to reinforce their security posture with minimal added burden.

When coordinated across departments, these practices create a multiplying effect, reinforcing access control, improving enforcement consistency, and expanding the reach of the airport's security posture beyond the security department.

10.1 Integrated Safety and Security Management Oversight

At some airports, safety, security, and operations are co-managed or operationally integrated, allowing for more fluid coordination, reduced information silos, better alignment of policies, and improved efficiencies. In these environments:

- Security and operations managers often serve as joint decision-makers
- Personnel may be cross trained to perform inspections, respond to incidents, and enforce policies across multiple disciplines
- Staff can be deployed flexibly, allowing coverage of both safety and security functions based on operational needs

This integrated model supports rapid, coordinated responses to airfield incidents and reinforces a safety and security culture of shared responsibility across departments and the organization.

While US airports are generally more focused on implementing Safety Management Systems (SMS) in accordance with FAA requirements, some have begun to explore or adopt the Security Management System (SeMS) framework. These emerging programs draw structural inspiration from SMS, incorporating familiar tools such as:

- Anonymous reporting
- Root cause analysis
- Trend tracking
- Risk-based decision-making
- Contractor reporting structures
- Focus on continuous improvement

Aligning the SeMS structure with the SMS structure supports contractor familiarity and reduces barriers to implementation among stakeholders already familiar with SMS.

While SeMS programs are still evolving in the US, PARAS 0009: *Guidance for Security Management Systems* provides a reference point for airports looking to formalize their approach.

10.2 Driving Offense Notifications and Credential Oversight

Airfield driving programs typically originate in the credentialing office in concert with Operations, where badge holders are assigned training, as applicable, and authorized access privileges. Programs such as Rap Back allow airports to receive real-time notifications if a badged individual is arrested or convicted of certain offenses, including driving under the influence or similar offenses. Although this offense is not a disqualifying offense in 49 CFR § 1542.209 (d), upon notification, airports may suspend or revoke driving privileges to mitigate this risk, as an active driver's license is a requirement to operate a vehicle on the airfield. Airports notify the badge holder through a variety of means and the individual is provided an opportunity to prove that they possess a valid license and are authorized to drive.

Some airports also participate in state-specific monitoring systems. For example, California's Employer Pull Notice program alerts employers of changes to an employee's driving record, including accidents and license suspensions. These programs are especially effective when incorporated into the badging application process, with applicants signing waivers permitting periodic record checks.

This shared mechanism enhances airport security by proactively identifying high-risk individuals operating vehicles on the airfield.

10.3 Airfield Lighting Strategies for Security Visibility

Lighting infrastructure designed for airfield safety is also highly effective in supporting perimeter monitoring, visual deterrence, and security enforcement. Airports use lighting to:

- Improve camera visibility and license plate capture
- Support inspections and patrols in low-light conditions
- Illuminate perimeter gates and fence lines to deter trespassing
- Enhance situational awareness around critical infrastructure

Motion-activated floodlights and directional lighting in remote areas also draw attention to unusual movement or prompt unauthorized individuals to retreat. Backup lighting and portable light towers can be used to maintain security visibility for temporary situations.

10.4 Situational Awareness and Cross Departmental Reporting

Safety-focused programs emphasize continuous situational awareness, particularly in active airfield environments where aircraft, vehicles, and personnel operate in close proximity. This heightened safety awareness naturally supports security objectives by enabling prompt identification of risks, unauthorized or unsafe behavior or activities, accurate location reporting during incident response, and shared accountability among airfield staff.

Non-security departments, such as environmental or maintenance, should be encouraged to identify and report security concerns while performing unrelated duties. For example, environmental staff tracking vehicle emissions or fuel usage can report expired permits, invalid escorts, or mechanical safety issues discovered during their audits to the security department. These decentralized reports enhance enforcement reach and build a campus-wide culture of vigilance.

10.5 Reporting Tools and Recognition Programs

Airport security campaigns such as DHS's "If You See Something, Say Something" and internal initiatives such as "This is My Airport" have led to airports implementing a variety of reporting channels, including:

- Online portals for anonymous safety and security reporting
- Dedicated email addresses shared across security and operations teams
- Low-tech solutions, such as physical drop boxes, including one purposefully mounted in a camera blind spot to preserve anonymity

To reinforce a proactive security culture, many airports offer recognition programs that reward staff for reporting safety and security concerns or for correctly challenging credentials. When actively promoted and consistently implemented, these programs have proven highly effective at engaging non-security staff in the airport's broader access control and threat detection strategy.

For more comprehensive information on building a strong culture of security and reporting, see PARAS 0049: *Creating and Maintaining a Strong Security Culture at Airports*.

SECTION 11: COMPLIANCE AND AUDIT PRACTICES

Ongoing compliance monitoring is essential to maintaining airfield security, ensuring regulatory adherence, and mitigating insider threats. In addition to patrols and inspections, airports rely on systematic audits, documentation reviews, and trend monitoring to identify gaps, detect suspicious activity, and refine enforcement strategies over time.

11.1 Airfield Vehicle Inspections and Security Patrols

While inspections at the access portals remain a primary security layer, vehicle inspections conducted post-entry on the airfield are a vital component of layered defense. These inspections support real-time enforcement, allow for the capture of evolving compliance issues, and serve as a deterrent to lapses in safe and secure vehicle operation across the airfield environment.

Field inspection techniques vary to support both scheduled and opportunistic enforcement. Strategies commonly used at airports include:

- Vehicle patrols with ad hoc inspections and challenges
- Checkpoint-style “post-up” inspections at predetermined or random locations on the airfield
- Covert, stand-off, or low-visibility monitoring and observation
- Inspections of parked or unattended vehicles for expired permits or unauthorized access

Airfield vehicle inspections are typically conducted by operations or security personnel, LEOs, or third-party contractors. Some airports set daily inspection quotas to ensure consistent and frequent monitoring of the airfield, balancing proactive enforcement with other patrol responsibilities.

Several airports allow authorized tenants or construction managers to inspect vehicles at designated gates assigned for their use. This model expands inspection capacity, and oversight is maintained through CCTV monitoring and audit protocols. TSA, compliance teams, or LEOs may also provide spot inspections or oversight of contractor-run inspections to ensure compliance.

Vehicle inspections on the airfield prioritize verification of operational and security compliance. Common inspection criteria include:

- **Driver Credentials:** Valid airport badge with authorized driving privileges; in some cases, a check of the driver’s state-issued license against DMV databases for active suspensions, revocations, or expirations
- **Vehicle Permits:** Valid, visible permit that matches registration information in the permitting database
- **Vehicle Condition:** Operational safety indicators such as beacons, working lights, tires in good condition, and absence of fluid leaks
- **Company Affiliation:** Visual match between the company name/logo on the vehicle and that listed on the vehicle’s permit form
- **Stop List Inspection:** Verification that the vehicle and driver are not on any internal stop/prohibited lists or are included in current allow/authorized lists
- **Prohibited Items Check:** A physical inspection to identify weapons, explosives, contraband, or other restricted items not permitted on the airfield under airport or regulatory policy and governing laws

During airfield vehicle inspections, airports may require drivers to remove the keys from the ignition and engage the emergency brake prior to the inspection process. While primarily implemented as a safety measure to prevent unintended vehicle movement, this procedure also serves to ensure the driver cannot flee or evade inspection once it has commenced.

When inspecting escort caravans, personnel verify that the escort holds appropriate authority, is compliant with ratio and supervision requirements, and that each passenger possesses valid credentials or government-issued ID. For non-badged passengers under escort, the ID may be logged in the inspection report.

Some airports have created an inspection matrix that directs inspectors to a subset of safety and compliance items to check during each encounter (e.g., tire treads, brake lights). This method expedites standardized inspections while allowing for flexibility and unpredictability.

Field inspectors may utilize mobile technology (e.g., badge readers, driver's license readers) to verify access and driving privileges against relevant databases.

More sophisticated tracking systems allow the inspector to generate an inspection log in the field to track the number of drivers inspected and any associated findings. Paper-based inspection logs may also be used to track inspection information for a less complex process.

Mid-field inspections also serve as a mechanism for immediate enforcement. Vehicles failing inspection may be denied continued access to the airfield or be secured on site until deficiencies are corrected. Drivers found to have expired or suspended licenses may have their airport driving privileges suspended or revoked on the spot. Escort-related violations, such as unauthorized passengers or escort ratio breaches, can trigger NOVs for both the escort and escorted individuals, with potential suspension or revocation of escort privileges.

Research into vehicle inspection strategies is ongoing due to the current dynamic regulatory environment regarding employee screening. Documents that may be of use to airports interested in more information on vehicle inspections include PARAS 0019: *Employee/Vendor Physical Inspection Program Guidance* and PARAS 0039: *Security, Operations, and Design Considerations for Airside Vehicle Access Gates*.

11.2 Enforcement Actions

To reinforce the importance of controlling access to the airfield and reducing security risks, airports apply consistent disciplinary measures for violations of escorting procedures, airfield driving rules, and vehicle permit conditions. A well-defined enforcement program, when combined with proactive training and stakeholder engagement, helps create a culture of accountability where access privileges are viewed as earned and maintained through continued compliance.

To ensure consistency, many airports incorporate these enforcement measures into their airport security rules and regulations, lease agreements, and badge application processes. Progressive discipline, retraining requirements, and clearly communicated expectations help balance enforcement with education and continuous improvement.

More information on strategies to create compliance programs and improve compliance with airport policies can be found in PARAS 0054: *Optimizing Compliance with Airport Security Rules and Regulations*.

11.2.1 Airfield Driving Privilege Suspension and Revocation

Airfield driving privileges are subject to suspension or revocation for violations that jeopardize operational safety or security. Common causes include:

- Repeated speeding, failure to yield, or disobeying airfield signage
- Entering MAs or security restricted areas without proper clearance
- Operating a vehicle without required credentials or outside designated areas
- Causing or contributing to a surface incident or security breach

Suspension periods vary by airport and infraction severity but typically range from 30 to 90 days, with permanent revocation reserved for repeat or high-risk offenses. Individuals under suspension may be required to complete remedial training and requalification before privileges are restored.

When driving privileges are suspended or revoked, airports must remove the associated endorsements from the individual's badge to prevent unauthorized access to restricted areas. This step is critical to maintaining compliance with security and operational safety protocols.

11.2.2 Escort Privilege Suspension and Revocation

In some cases, driving suspensions may also result in temporary loss of escort privileges, particularly when the violation occurred during an escort operation or indicated a broader failure to follow airfield procedures. Escorting infractions typically involve:

- Failing to continuously accompany, monitor, and maintain positive control of and visual contact with the person being escorted
- Allowing access to unauthorized areas or allowing the individual to engage in unauthorized activities
- Escorting unbadged individuals without proper justification or approval
- Repeated misuse or procedural lapses despite previous warnings

Suspensions typically range from 30 days to one year, with many airports requiring retraining or formal reapplication before restoring privileges. At airports with more structured enforcement programs, repeat offenses may result in permanent revocation of escort authority.

In some cases, NOVs will be issued to both the escort and the individual being escorted. This joint accountability reinforces the requirement that both parties understand and follow the escorting procedures. Some airports exceed this standard by including escorting requirements in tenant leases and construction agreements, allowing serious or repeated violations to trigger enforcement actions, including financial penalties or, in extreme cases, breach of contract and lease or project termination.

11.2.3 Vehicle Permit Suspension and Revocation

Some airports will suspend or revoke vehicle permits as part of their broader enforcement strategy. Vehicle permits may be revoked, suspended, or placed on hold under the following conditions:

- Expired or lapsed insurance associated with the permitted vehicle
- Vehicle found operating outside its authorized area, such as a PNO-designated vehicle leaving its designated area

- Use of fraudulent or tampered permit indicators, including improperly transferred placards or stickers
- Persistent noncompliance by the vehicle's owner, such as repeated violations, an egregious violation, or unauthorized access attempts

In some cases, the airport may place the entire tenant fleet on a stop list until the issue is resolved, especially when all vehicles share a single insurance policy or owner. This collective enforcement method prompts rapid response and accountability from tenant companies.

11.3 Stakeholder Communication

Effective communication is essential to maintaining security compliance and operational continuity when implementing policy updates, regulatory changes, or temporary adjustments to airfield operations. Clear, consistent communication ensures that tenants, employees, and stakeholders are informed of their responsibilities on the airfield and are prepared to adapt, minimizing the risk of confusion, security breaches, and operational disruptions.

At most airports, the security department plays the primary role in distributing security-related information to the airport community, while the operations department is often responsible for distributing information regarding changes to airfield access, driving privileges, and vehicle operations. Security and operations personnel frequently leverage support from other airport departments (e.g., IT, public relations, airport business office, engineering, facilities, leasing, marketing) to ensure that critical security information reaches all impacted stakeholders through established communications channels. Common methods used to disseminate airfield security-critical updates include:

- **AS distribution lists:** Security departments send updates to each tenant's AS, who is responsible for sharing the information with their employees.
- **Mass communication platforms:** Email distribution services are used to send security announcements directly to employee email addresses collected during the badging process; the distribution list can be customized to only send the information to select populations (e.g., hangar lessees, MA drivers).
- **Internal information portals and mobile applications:** Employee intranet sites or applications are used to post policy updates, security bulletins, and airfield notices.
- **Radio communications:** Immediate but temporary changes (e.g., gate closures during SMGCS operations) are relayed via designated radio channels.
- **Security meetings:** Regularly scheduled stakeholder security briefings reinforce major or temporary changes and provide opportunities for clarification.
- **Physical posting:** Security staff stationed at vehicle gates communicate changes to each driver directly; signage (static or digital) is posted at vehicle gates to reinforce updates.
- **Direct outreach:** Important updates may be disseminated through phone calls, mailed notices, or even local newspaper announcements for wide coverage to stakeholders who visit the airport less frequently (e.g., hangar lease holders).

Airports employ multiple methods and layers of communication to ensure redundancy and maximize reach to employees with airfield driving privileges. Techniques such as read receipt requests on email notifications and mandatory acknowledgment prompts within internal systems provide additional assurance that stakeholders have reviewed critical updates.

Maintaining tenant trust and cooperation is especially critical when implementing new security measures or federal requirements. Several airports that recently transitioned to a federalized security program noted that proactive, repeated communication over several months prior to the transition was essential to easing concerns about stricter access controls and driving restrictions. Multi-channel strategies—including town halls, written frequently asked questions, and one-on-one meetings—give stakeholders opportunities to ask questions, express concerns, and build familiarity with the new requirements, improving compliance and reducing resistance.

Some airports have formalized event and project communications through their own locally developed system such as a Notice of Work program, where project sponsors submit details about work areas, temporary policy changes, or access restrictions. Approved notices are posted to centralized portals, searchable by date or location, and distributed to managers for dissemination to frontline employees. Such programs improve visibility of upcoming changes that may impact security restricted areas or airside operations.

When immediate or temporary access changes occur (e.g., SMGCS operations or emergency closures), airports may deploy visual and physical indicators such as:

- Freestanding display boards in roadways and gate approaches
- Traffic cones to signal lane or gate closures
- Lockout bags placed over badge readers to prevent access
- Flashing strobe lights installed at vehicle gates to indicate temporary restrictions
- Push notifications issued via radios or mobile alert systems

By coordinating early, communicating often, and delivering consistent security messaging through multiple trusted channels, airports strengthen both their operational resilience and their compliance with regulatory expectations during periods of change.

More detailed information on strategies to communicate with airport stakeholders can be found in PARAS 0003: *Enhancing Communication & Collaboration Among Airport Stakeholders* and PARAS 0044: *Strategies for Aviation Security Stakeholder Information Sharing*.

11.4 Security Log and Record Audits

Airports conduct regular audits of vehicle access and airfield operations records to detect anomalies or lapses in compliance. Audit frequency varies by airport and may be semi-annual, annual, or biennial depending on regulatory inspection cycles, emerging trends, or operational risk levels. Records commonly reviewed during these audits include:

- Issued vehicle gate keys, access codes, and access credentials
- Escort and visitor logs
- Logs from airport- and tenant-managed ACS
- Recorded CCTV footage
- Vehicle permit records
- Driver and escort training and authorization documentation

Auditors are often personnel from security, operations, credentialing, compliance, or risk management divisions looking for red flags such as missing approvals, expired credentials, odd-hour activity, or

repeated access denials. These issues may signal administrative errors, outdated records, or potential insider threats requiring further investigation.

In preparation for federal inspections by TSA or FAA, airports may host pre-inspection meetings with tenant managers to ensure readiness. These meetings clarify what documentation, training records, and vehicle compliance standards will be reviewed, and help ensure consistent enforcement across all airport users. Assigning an airport representative to act as a liaison to tenants can greatly assist with compliance planning, policy updates, and regulatory readiness. This direct engagement model fosters stronger communication and accountability while minimizing surprises during external audits.

11.5 Monitoring Enforcement Trends and Compliance Patterns

By collecting and evaluating data from multiple sources—including inspection logs, access control platforms, violations, and incident reports—airport security and operations can identify knowledge gaps, potential training deficiencies, and emerging vulnerabilities, optimize patrol strategies, and strengthen compliance across vehicle operators and tenant personnel.

Centralized databases allow for targeted trend analysis across time, location, and operator and can be a viable tool to track:

- Airfield inspection activity
- NOVs
- Driver and vehicle rejections at access points
- Badge challenges
- Escort violations or repeated escort requests that exceed the threshold
- Stop-listed or unauthorized vehicles and equipment discovered on the airfield (e.g., vehicles without a permit or with an expired permit)

Analysis and evaluation of the trends may prompt security, operations, or airport law enforcement to increase patrols in those areas and adjust inspection routes accordingly. This also supports more efficient deployment of limited resources and can inform long-term risk mitigation strategies, such as adjusting tenant access agreements, increasing lighting and surveillance in problem areas, and performing targeted inspections.

Airports may experience persistent challenges with inconsistent enforcement practices, particularly when staff hesitate to escalate incidents or formally document violations due to concerns about stakeholder pushback or conflict, perceptions that violations are minor or unintentional, and uncertainty around when a verbal warning should become a reportable incident. This results in missed opportunities to identify security and safety deviations and repeat offenders; undermines the deterrent effect of enforcement; and contributes to a false perception of compliance across the airfield. To address this, some airports are shifting toward more standardized enforcement protocols, including:

- Issuing written “warning NOVs” that are logged and tracked even if no formal or monetary penalty is applied
- Clarifying non-compliance or violation escalation thresholds for staff
- Training field personnel to use data systems for real-time input, analysis, and retrieval of past violation histories

Reinforcing the expectation that all violations (verbal and written) should be documented allows airports to more accurately assess the airport's security compliance performance and intervene before minor issues escalate into significant security concerns.

Monitoring enforcement activity is a critical feedback loop that informs risk-based resource allocation, targeted compliance interventions, and the continuous improvement of access control programs. Airports that embrace structured reporting and trend analysis are better positioned to maintain secure operations across the evolving airfield environment.

SECTION 12: CONCLUSION

Securing airside vehicle operations requires a layered approach, blending access control, permitting, operational discipline, and responsive enforcement. While regulatory frameworks such as 49 CFR § 1542 set baseline expectations, the diversity of airport layouts, tenant structures, and operational demands needs tailored implementation strategies. Improving the security of airside vehicle operations requires an understanding of the interdependencies between the airport's infrastructure and conditions, aircraft and ground vehicles, security and safety risks, and compliance with strict regulatory requirements.

This report has highlighted practices from a cross-section of US airports, offering a synthesis of both traditional and innovative approaches to manage airfield security by reducing risks related to airside vehicle operations. The report underscores the importance of combining policy, training, oversight, and technology to create a secure and well-managed airfield.

Many of the most effective strategies described in the report originate from collaborative efforts across departments, partnerships with tenants, and the integration of safety practices into security frameworks. Airports that strategically plan and coordinate, establish clear expectations, implement risk-based policies, enforce standards consistently, and use data to inform improvements are better positioned to adapt to evolving security threats, and operational demands.

As airports continue to modernize their infrastructure and expand their operations, the principles of risk management, accountability, oversight, and control must remain at the forefront of vehicle security programs to ensure secure, safe, and efficient airport operations, and movement of people and personnel on the airfield. This synthesis provides a roadmap for reinforcing those principles across the airfield.

REFERENCES

Aircraft Owners and Pilots Association. (2018). "TSA Airport Access Security Requirements." https://www.aopa.org/advocacy/airports-and-airspace/security-and-borders/tsa-airport-access-security-requirements.

Bender, Gloria. (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

Bender, Gloria and Entrekin, Andy and Welna, Jim and Gafford, Jessica and Zoia, Michael and Crosby, Mark and Dickie, Kim. (2022). *Security, Operations, and Design Considerations for Airside Vehicle Access Gates* (PARAS 0039). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0039.AirsideVehicleAccessGates_.FinalReport_.pdf

Department of Motor Vehicles. "Employer Pull Notice Program." State of California. Retrieved 26 November 2024. https://www.dmv.ca.gov/portal/vehicle-industry-services/motor-carrier-services-mcs/employer-pull-notice-epn-program/.

Federal Aviation Administration. (2022). "General Aviation Surface Safety Symposium: Morning Session." YouTube. https://www.youtube.com/live/Rfcdn8Hg8Vg?si=Qm7X5RkT8set1T0i.

Federal Aviation Administration. (2022). "Surface Safety Symposium: Vehicle Drivers & Other Airport Surface Operators: Afternoon Session." YouTube. https://www.youtube.com/watch?v=IskS3mqkldA.

Federal Aviation Administration. (2022). "Surface Safety Symposium: Vehicle Drivers & Other Airport Surface Operators: Morning Session." YouTube. https://www.youtube.com/watch?v=IskS3mqkldA.

Federal Aviation Administration. (2024). Autonomous Ground Vehicle Systems (AGVS) Technology on Airports (CertAlert 24-02).

Flamenbaum, Harold and Fleet, Dave and Gaisor, Ross and Varwig, Zach. (2017). *Employee Inspections Synthesis Report* (PARAS 0006). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0006.Employee_Inspections.FinalReport.pdf

Government Accountability Office. (2016). *Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates* (GAO-16-632).

Ground Vehicle Operations to include Taxiing or Towing an Aircraft on Airports, AC 150/5210-20A. (2015). https://www.faa.gov/airports/resources/advisory_circulars/index.cfm/go/document.information/documentID/1028089.

Hubbard, Sarah and Voyles, Richard and Souders, Dustin and Yang, Haoguang and Hart, Jason and Brammell, Sarah and Environmental Resources Solutions. (2020). *Advanced Ground Vehicle Technologies for Airside Operations* (ACRP Report 219). https://nap.nationalacademies.org/catalog/26017/advanced-ground-vehicle-technologies-for-airside-operations.

Landry, JoAnne and Ingolia, Shane. (2011). Ramp Safety Practices (ACRP Synthesis 29). Transportation Research Board. https://nap.nationalacademies.org/catalog/14599/ramp-safety-practices.

Miller Dunwiddie. (2021). *Consolidated Receiving and Distribution Facilities at Airports* (PARAS 0024). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0024.ConsolidatedRcvgDistFacilities_.FinalReport_.pdf

"Non-Movement Area Driver Licensing." (2024). AAAE Member Hub. [Forum Discussion]. Retrieved 5 January 2025. https://hub.aaae.org/discussion/non-movement-area-driver-licensing.

Operational Safety on Airports During Construction, AC 150/5370-2G. (2017). https://www.faa.gov/airports/resources/advisory_circulars/index.cfm/go/document.current/documentnumber/150_5370-2.

Painting, Marking, and Lighting of Vehicles Used on an Airport, AC 150/5210-5D. (2010). https://www.faa.gov/airports/resources/advisory_circulars/index.cfm/go/document.information/documentID/215227.

Pedestrians and Ground Vehicles, 14 CFR § 139.329. (2013). https://www.ecfr.gov/current/title-14/chapter-I/subchapter-G/part-139/subpart-D/section-139.329.

Polsgrove, Nathan and Gabrielson, Neil and O'Krongley, Tim and Ham, Richard. (2021). *Planning and Operational Security Guidance for Construction Projects at Airports* (PARAS 0037). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0037.AirportConstructionSecurity_.FinalReport_.pdf

Quilty, Stephen. (2013). *Helping New Maintenance Hires Adapt to the Airport Operating Environment* (ACRP Synthesis 49). Transportation Research Board. https://crp.trb.org/acrpwebresource13/acrp-synthesis-49-helping-new-maintenance-hires-adapt-to-the-airport-operating-environment__trashed/

Quinn, Julie and Williams, Katherine and Germolus, Shaun. (2021). *Synthesis of Escort Privileges and Escorting Practices* (PARAS 0035). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0035.EscortPrivilegesPractices_.Final_Report_.pdf

Rieder, René. (2021). *Recommended Security Guidelines for Airport Planning, Design, and Construction* (PARAS 0028). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0028.Recommended_Security_Guidelines_.FinalReport_.pdf

Rieder, René and Peel, Stacey and Swinstead, Liz. (2018). Gu*idance for Security Management Systems (SeMS)* (PARAS 0009). National Safe Skies Alliance. https://www.sskies.org/images/uploads/subpage/PARAS_0009SeMS_Guidance-Final.pdf

Security of the Air Operations Area (AOA), 49 CFR § 1542.203. (2002). https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1542/subpart-C/section-1542.203.

Security of the Secured Area, 49 CFR § 1542.201. (2002). https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1542/subpart-C/section-1542.201.

Security of the Security Identification Display Area (SIDA), 49 CFR § 1542.205. (2006). https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1542/subpart-C/section-1542.205.

Transportation Security Administration (TSA). (2006). *Recommended Security Guidelines for Airport Planning, Design and Construction*.

Zhang, Tianjian. (2018). "Knowledge Expiration in Security Awareness Training." ADFSL Conference on Digital Forensics, Security and Law. 2.

Zoufal, Donald and Bender, Gloria and Wendt, Douglas and Entrekin, Andy and Gafford, Jessica and Cusson, Sean. (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: REGULATORY REQUIREMENTS

FAA and TSA have established several regulations, Advisory Circulars (AC), and guidance documents to ensure airport operators control access to and movement on airfields. Notable documents include:

- 14 CFR § 139 – *Certification of Airports*: Prescribes rules governing the certification and operation of airports, including requirements for the safe operation of aircraft and the protection of persons and property on the airfield.
- FAA AC 120-57A – *Surface Movement Guidance and Control System*: Describes standards and provides guidance for developing SMGCS at airports, facilitating safe ground operations under low-visibility conditions.
- FAA AC 150/5210-5D – *Painting, Marking, and Lighting of Vehicles Used on an Airport*: Establishes standards for painting, marking, and lighting requirements for vehicles operating on an airport to ensure visibility and prevent accidents.
- FAA AC 150/5210-18A – *Systems for Interactive Training of Airport Personnel*: Provides guidance on the implementation of interactive training systems for airport personnel, with a focus on improving safety, security, and regulatory compliance.
- FAA AC 150/5210-20A – *Ground Vehicle Operations to Include Taxiing or Towing an Aircraft on Airports*: Provides guidance for safe ground vehicle operations on airports, emphasizing procedures to prevent runway incursions and accidents.
- FAA AC 150/5370-2G – *Operational Safety on Airports During Construction*: Outlines the necessary precautions, procedures, and communication strategies airports must implement to minimize risks to aircraft, vehicles, and personnel while construction is underway.
- FAA Order 7110.65, Chapter 3, Section 7 – *Taxi and Ground Movement Procedures*: Details procedures for air traffic controllers to manage aircraft and vehicle movements on the ground, ensuring safe and efficient operations.
- FAA CertAlert No. 22-07 – *Movement Area Training and Situational Awareness*: Emphasizes the importance of training for personnel accessing movement areas and promotes situational awareness to prevent runway incursions and other incidents. The alert encourages airport operators to review and enhance their training programs, implement clear communication protocols, and conduct random spot checks to ensure proficiency.
- FAA CertAlert No. 24-02 – *Autonomous Ground Vehicle Systems (AGVS) Technology on Airports*: Provides guidance regarding the testing, deployment, and operation of AGVS or autonomous vehicle technology in airport environments.
- 49 CFR § 1542 – *Airport Security*: Outlines requirements for airport operators to establish security programs that prevent unauthorized access to security restricted areas of the airport.
- *TSA Security Guidelines for General Aviation Airports*: Offers a set of voluntary security measures and best practices for general aviation airport operators to enhance security and control access to sensitive areas.
- TSA regulations covering:
    - Vehicle escorting programs
    - Badging requirements
    - Badge issuance and management
    - Defined security areas and access control