PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0050 April 2024

Public Safety and Security at On-Airport Rental Car Facilities

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Gloria G. Bender
James Welna
Andy Entrekin
Jessica Gafford
TransSolutions, LLC.

Michele Freadman
M. Freadman Consulting, LLC.

Mike Everson
Airport Law Enforcement Agencies Network (ALEAN)

Donald Zoufal
CrowZNest Consulting, LLC.

Jeff Weiner
Payal Harrell
PGAL, Inc.

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 0050 PROJECT PANEL

Daniel Barton *InterVISTAS Consulting*
Jason Byers *Dallas Fort Worth International Airport*
Frank Capello *Broward County Aviation Department (Retired)*
Scott Lawson *Security Technology Representative (Retired)*
Kevin Murphy *Airport Law Enforcement Agencies Network*
Julie Quinn *QuinnWilliams, LLC*
Jay Shipp *Dallas Fort Worth International Airport (Retired)*
Timothy Tyler *Metropolitan Washington Airports Authority*
Kevin Vandeberg *Huntsville International Airport*

AUTHOR ACKNOWLEDGMENTS

The PARAS 0050 Research Team would like to acknowledge the dozens of airport, rental car operator, and third-party facility manager representatives who graciously volunteered to participate in interviews and host site visits for the researchers. We are withholding acknowledgment of individuals and their organizations to protect the confidentiality of the interviews, but this research could only be successful with their assistance.

The authors would also like to thank the Project Panel for their guidance and feedback during the research, which helped shape the direction of the final document. Thanks are also given to National Safe Skies Alliance for facilitating the research and providing guidance, with particular thanks to the PARAS Program Manager, Jessica Grizzle.

Finally, we wish to thank the members of the Research's Red Team who participated in interviews and provided input on the major project deliverables. Their experience and airport perspective helped the Research Team create a more robust and useful document.

- Robert Boblitz, Baltimore Washington International Airport
- Raymond Laroche, Punta Gorda Airport
- Douglas Wendt, formerly Hartsfield-Jackson Atlanta International Airport

CONTENTS

TABLES & FIGURES

SUMMARY

This report consolidates the methods, strategies, tools, and technologies identified during the research that an airport can use to enhance security and public safety, and reduce criminal activity at on-airport rental car (RAC) facilities. Care was taken to provide scalable options for airports of all sizes, layouts, and demand levels. Throughout the report, blue callouts provide specific examples of effective, unique methods discussed in airport interviews. The report offers guidance to help the reader determine which solutions are most appropriate for their specific environment, circumstances, and challenges.

RAC operations are a critical service offered at an airport and a source of significant revenue to both the airport operator and any jurisdiction that collects taxes on the transactions. However, RAC facilities face a constant threat of criminals entering the facility and stealing vehicles. The fleet of expensive vehicles and the open, publicly accessible operations make RAC facilities attractive targets. Airport and RAC operators must focus on prevention and deterrence methods to protect the RAC facilities and assets, enhance public safety, and mitigate risk in the airport environment.

RAC operations and facilities are unique on the airport campus. All operations take place on the public side of the airport and thus are not under federal purview. They are often in an isolated location away from the terminal, which usually makes them a lower security priority. The space is leased, and the assets are owned by the tenant. However, criminal incidents occurring on airport property divert law enforcement resources from the airport to investigate and file reports. Additionally, reports of these crimes in media and internet review sites can damage the reputation of the airport, especially if connected to more serious crimes.

Airport operators have limited resources to understand the full breadth of RAC operations and security implications of various design elements and features. This report has been created to fill that gap and identify multiple methods, strategies, tools, and technologies that airport operators can leverage or implement to enhance the security of RAC facilities.

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

ASM	Airport Security Manager
CHRC	Criminal History Record Check
CPTED	Crime Prevention Through Environmental Design
CSB	Customer Service Building
CVG	Cincinnati/North Kentucky International Airport
EMV	Europay, Mastercard, and Visa
ESV	Electric Standup Vehicle
FBO	Fixed-Base Operator
GTC	Ground Transportation Center
LED	Light-Emitting Diode
LEO	Law Enforcement Officer
LPR	License Plate Reader
MSP	Minneapolis–St. Paul International Airport
NCIC	National Crime Information Center
NHTSA	National Highway Traffic Safety Administration
PIN	Personal Identification Number
POS	Point of Sale
PTZ	Pan-Tilt-Zoom
QR	Quick Response
QTA	Quick Turnaround Area
RAC	Rental Car
SLC	Salt Lake City International Airport
STA	Security Threat Assessment
TVA	Threat and Vulnerability Assessment
UV	Ultraviolet
VIN	Vehicle Identification Number

SECTION 1: INTRODUCTION

Rental car (RAC) operations are a critical service offered at airports, and the dollar value of the vehicles stored in and around RAC facilities is substantial. This makes security at RAC facilities a significant airport security concern.

Crimes committed on or near airport property impact the airport's liability exposure and reputation for safety and security, and undeterred criminals may inform others that the airport is a viable target. The crimes committed using vehicles stolen from RAC facilities also impact the neighboring communities.

Additionally, calls for service and police reports from RAC facilities consume valuable law enforcement resources, depleting law enforcement officer (LEO) coverage from high-risk areas of the airport. Improving the security of RAC facilities will reduce the time airport police spend responding to the facilities.

Maintaining the safety and security of an airport's public areas can be dynamic and complex. This is true for RAC facilities with the added complication that they are frequently located some distance away from the main airport terminals, which separates them from the airport's management, security, and law enforcement staff.

1.1 Vehicle Rental and Return Process

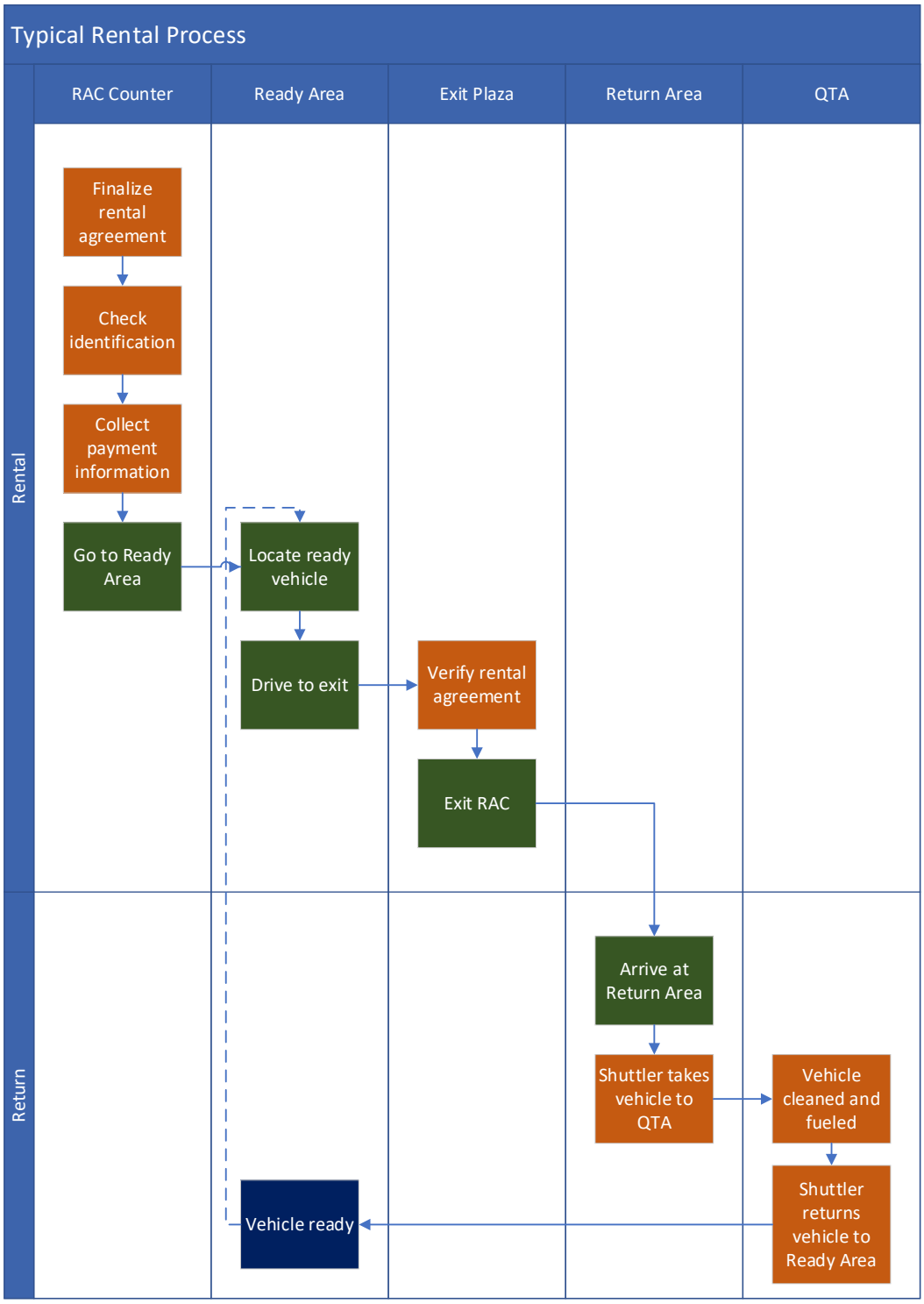
RAC facility customers typically reserve their vehicle online before arriving at the airport, so for most customers, the process at the RAC facility starts with the counter agent to finalize the rental agreement, check identification, and collect payment information. Some RAC operators allow their preferred members to bypass the counter and head directly to the RAC Ready Area to locate or choose a vehicle.

The customer locates their assigned vehicle or chooses a vehicle from a selection and drives to the facility exit. Many exits have security barriers to prevent vehicles from leaving the facility without some form of verification and authorization. This is often a staffed exit booth, but it can include equipment designed to scan preferred member accounts. If the contract is verified, the vehicle is permitted to exit the facility. If the contract cannot be verified, or the customer has chosen the wrong type of vehicle, the customer is not permitted to exit the facility and will be redirected to the Return Area.

When returning a vehicle, the customer drives to the appropriate RAC operator Return Area. They may either leave the keys in the vehicle or in a drop-box located in the Return Area or near the RAC customer counters. A shuttler then takes the vehicle to the Quick Turnaround Area (QTA) where it is inspected, cleaned, and refueled. Once the vehicle is ready for the next customer, the vehicle shuttler delivers the vehicle to the appropriate RAC Ready Area.

The rent and return processes are shown in Figure 1-1.

Figure 1-1. Typical Rental Process



1.2 The Challenges

Most auto crimes in airport RAC facilities can be attributed to one of three types of threat actors:

- Insider threat
- Local gangs
- Organized crime

Individuals working at the RAC facility may share their insider knowledge of the operations and security vulnerabilities and access to secure areas with friends and criminals. RAC personnel may also exploit their knowledge and access through several potential methods:

- Counter agents can accept fraudulent IDs or payments
- Vehicle shuttlers have authority to take the vehicle out of the facility
- Exit booth attendants can release the security barriers to allow criminals to leave the facility

Many RAC employees work for low wages and regularly drive or handle the keys to vehicles with significant value. This makes the incentive and opportunity to facilitate or commit criminal activities particularly high.

Organized criminal groups are much more likely to use fraudulent measures (e.g., counterfeit identification and payment) to steal vehicles. These groups are interested in selling or using vehicles to commit major crimes. Stolen vehicles are often shipped overseas in shipping containers as a revenue stream that funds transnational criminal networks and terrorist organizations.

Local gangs can create significant challenges for airport RAC facilities, and there has been a rise in gang activity in these facilities. Gangs often require new members to steal a vehicle and/or commit other crimes as a gang initiation and rite of passage. The vehicle may then be used to commit other crimes, such as burglaries, robberies, drive-by shootings, and drug trafficking. If not recovered quickly, the vehicle usually will be dismantled for parts. Criminals will often enlist juveniles to steal multiple vehicles, knowing that the criminal justice system is more lenient with juveniles.

Local gangs are more likely to steal a vehicle from a ready/return area with little concern over damage to the vehicle's exterior. Many will use a "sacrificial" vehicle to destroy, move, or immobilize security barriers and features. This vehicle creates a path for multiple vehicles to exit the facility without incurring similar damage.

It is common for gangs and organized criminal groups to move between multiple airports in close proximity and hit several RAC facilities.

There is no one-size-fits-all solution to improve security at RAC facilities. However, airport operators collaborating with their RAC stakeholders can help create a secure facility supported by situationally aware employees. Implementing effective mitigation measures and security enhancement may create a less attractive target for criminal activity and security threats at the facility.

In addition, there are several strategies that RAC operators can implement to improve security in RAC common areas and their exclusive areas. Many of these are the same strategies airports can implement (e.g., cameras and physical barriers), but several strategies can only be implemented by the RAC operator (e.g., policies and procedures).

The following sections discuss strategies, solutions, methods, and equipment that airport operators and RAC operators can use to enhance security and public safety at their RAC facility.

Airport operators can collaborate with RAC operators on common goals to identify opportunities for compromise and possible incentives for compliance. A meeting scheduled with RAC executives or the third-party facility manager should be dedicated to discussing the current security vulnerabilities, trends, and potential solutions. RAC operators may be unwilling to compromise on some security measures that they perceive will adversely impact their operations. Or, franchise owners who often are more amenable to airport security needs, may not have the financial means to implement some security measures.

Airport operators may need to offer incentives or services in exchange for implementing requested measures.

Developing persuasive business cases for security recommendations based on clearly articulated threats and vulnerabilities will significantly support the airport operator's case for implementing certain security measures to enhance security and public safety. This rationale can include presentations with data showing trends in criminals exploiting certain vulnerabilities, or documented cases from other airports and media.

SECTION 2: INFORMATION SHARING

RAC employees and site managers are stakeholders and partners in the airport's safety and security posture. RAC employees may have useful security-related information, and should have appropriate mechanisms and channels to provide that information. A common theme from this research is that airport operators and airport police that have more frequent interactions with RAC employees and site managers benefit from increased cooperation and timely reporting and information sharing on security issues and criminal activity.

The most common calls for service to airport police are attempted or actual theft from the facility, non-return of rentals (vehicle conversions), counterfeit credit cards and IDs, trespassers, and irate customers. Other information may include reports of security violations, individuals experiencing homelessness, weapons left in vehicles, or any number of other security concerns. RAC site managers may also share video footage with airport police in response to security incidents.

RAC operators are highly competitive and protective of their policies and practices, which can lead to delays in sharing critical information about incidents and trends. Additionally, the variety of reporting policies for RAC operators can result in extensive delays in law enforcement receiving information and entering stolen vehicles into the National Crime Information Center (NCIC) database. Developing formal and informal information-sharing practices among stakeholders (RAC operators, their employees, the airport operator, and airport police/security), and holding frequent discussions with RAC operators strengthens relationships, provides necessary education to support crime-prevention activities, and helps reduce or eliminate delays in information sharing.

2.1 Stakeholders and Partners

It is typical for a small group of stakeholders to be involved in the safety and security of RAC facilities. Some of these stakeholder populations include:

- **RAC employees and site managers.** Responsible for reporting suspicious or fraudulent activities to the airport operator or airport police.
- **RAC corporate or regional offices.** Often responsible for retrieving and submitting CCTV footage to LEOs with a formal request.
- **Third-party facility manager.** Responsible for the maintenance, operations, and sometimes security of consolidated facilities.
- **Contract security guards.** Responsible for patrolling the facilities, staffing/monitoring the exits, or shuttling vehicles.
- **Airport operators, security, and airport police.** Ultimately responsible for the safety and security of the RAC facilities if located on airport property or within airport jurisdiction.

RAC OPERATORS AND EMPLOYEES

There are four major RAC flagship brands with operations at US airports, some of which have acquired multiple RAC operators under holding companies. The operators typically seen at airports include:

- **Enterprise Holdings:** Enterprise Rent-A-Car, Alamo Rent a Car, and National Car Rental
- **The Hertz Corporation**: Hertz, Dollar Car Rental, and Thrifty Car Rental
- **Avis Budget Group:** Avis Car Rental, Budget Rent a Car, and Payless Car Rental
- **Sixt Group**

Some airports also lease space to smaller or local brands.

A parent company may own the operators, but some airports hold lease agreements with franchise owners. In general, operators within the same brand must comply with their corporate requirements, but the franchise owners' physical security measures or policies for reporting stolen vehicles and other incidents may differ from their affiliated holding company's policies. This may complicate certain information requests (e.g., CCTV footage).

RAC employees who staff customer service counters, exit booths, and the QTA, as well vehicle shuttlers, are often from temporary or contract staffing services. This workforce is particularly susceptible to high turnover and the type and breadth of background checks can vary widely from agency to agency.

Airport operators can have a difficult time conveying relevant security information to RAC employees because of the high turnover. RAC site managers are likely in the best position to share information with their employees. Regularly updating RAC operators, employees, and site managers on relevant security information will provide essential education to help them make informed decisions about their security measures and improve buy-in for new security enhancements.

THIRD-PARTY FACILITY MANAGERS

Some airports have a consortium for their RAC operators that is often tied to a legal agreement, such as a lease or concessions agreement (see Section 5.1). The consortium requires the RAC operators to make decisions as a group instead of individually. To fulfill this requirement, the consortium often contracts a third-party facility manager to act as the consortium's voice and to manage the maintenance, operations, and security of the consolidated RAC facilities. This entity is different from the airport's facility manager, although they may act as a liaison to make decisions about the facilities.

A third-party facility manager is helpful to any group of tenants operating in the same building because each RAC brand and local operator has their own unique priorities. The facility manager is an objective party responsible for managing and unifying the separate operators to ensure that the facility functions as prescribed and accomplishes its goals and requirements. RAC operators often contract with a third-party facility manager for select consolidated operations or facilities, such as QTA operations, even if there is no formal consortium.

AIRPORT OPERATORS AND POLICE

Airport security and police are responsible for the overall security of the airport, including on-airport RAC facilities. Typically, airport police are responsible for patrolling the common areas of the RAC facility (e.g., customer lobby, perimeter). They are sometimes responsible for patrolling the exclusive RAC spaces as well. The airport security department and police often conduct inspections, audits, and tests in RAC facilities to ensure security requirements are being met and policies are being followed. The airport property or contract manager is responsible for contracting matters. All of these departments will have a need to share information with the RAC operators or request information from them.

Sometimes, the airport will appoint a RAC liaison to work with the RAC operators or third-party facility manager. Often, this role falls to the airport security manager (ASM), airport properties manager, or a designated airport police department representative. Having a single point of contact for both the airport and the RAC operators helps ensure consistent communication between the parties.

Airport operators and police work with neighboring communities, airports, and jurisdictions to share trend data, suspect images, and information on criminal investigations. Some larger airports or airport systems employ crime analysts and resources, and may offer use of these resources to assist their

neighboring airports. LEOs have more opportunities to work with neighboring law enforcement jurisdictions through these connections.

Some airport LEOs participate in auto crimes task forces in their area. These are rarely specifically focused on rental vehicles, but they offer members valuable information about crime trends and methods to minimize vulnerabilities pertinent to rental cars.

CONTRACT SECURITY

Some airports and RAC operators contract security service providers to supplement their security and police forces. These individuals are usually stationed in the RAC facility overnight to patrol the common and/or exclusive areas during closed hours. They are also tasked with observing the facility to identify any vulnerable areas or gaps in security and report them to the RAC or airport operator for remediation.

Since contract security staff do not have arrest authority and can only issue citations on behalf of the airport, many RAC operators prefer to hire off-duty police officers to perform this function overnight.

2.2 Reporting and Information Sharing Mechanisms

Airport operators can support the security of the RAC facility by offering multiple communication channels and opportunities for RAC employees to share or report security information, and for the airport operators to share security information with the RAC employees. Airport operators should also encourage RAC operators to develop internal communications with their neighboring operators.

COMMUNICATION BETWEEN RAC OPERATORS

Information sharing among RAC site managers at the airport can greatly enhance situational awareness of activities occurring in the RAC facilities. RAC consortium meetings are excellent opportunities for site managers to discuss security concerns and improvement opportunities. A third-party facility manager or the airport liaison can help with negotiations and collaboration.

Sometimes individuals attempting to commit fraud at the customer counters will attempt at several RAC counters until they successfully complete the transaction or the police are called. Creating a means for RAC site managers to communicate attempted fraud transactions with other RAC site managers could further improve their ability to prevent criminal activity.

Some RAC site managers share relevant security information with their off-site locations. Encouraging effective communication between RAC site managers at the airport and with off-site locations provides an additional level of security awareness and information sharing in the RAC facilities.

COVERT REPORTING

Some RAC employees may not be comfortable alerting airport police to a possible security issue while the customer is standing in front of them. To address this potential concern, most RAC facilities have an administrative area immediately behind the RAC counters where employees can excuse themselves to contact the police or airport security in private.

If there is no back room or the employee cannot access that room, developing a secret code for employees to use with a manager or police dispatch is a good alternative. Phrases such as “I’m getting an error code on my computer” or “I need supervisor approval” can seem mundane to a customer but could be used to alert airport police of a potential fraudulent transaction in progress. This would need to be worked out in advance with the RAC employees, airport police, and airport/police dispatch.

AIRPORT DISPATCH AND 9-1-1

The majority of airports use the airport or police dispatch to handle calls for service from the RAC facility. Calling airport or police dispatch or the area's 9-1-1 dispatch will ultimately result in response from airport LEOs. Airport operators should determine the appropriate number to be called to ensure the fastest response.

> One airport operator indicated the airport property is geofenced so that any 9-1-1 call made within the boundary will automatically be redirected to airport dispatch, eliminating a step in the call transfer process and speeding up response time.
>
> Another airport operator created stickers with airport emergency contact numbers to give out to their badged population. Airport LEOs provided several stickers to the RAC site managers to give to their employees.

Airports that issue identification badges to RAC employees could print emergency phone numbers on the reverse side of the badge.

EMAIL

Email is a common method to contact RAC headquarters or regional offices, and is often used to request video footage. Information sharing through email is typically the airport operator emailing RAC site managers or the RAC third-party facility manager about changes to policies or operations or reminders on security requirements. Email is also the method airport operators and airport LEOs use to invite their stakeholders to monthly and quarterly meetings.

> Several airport police departments created the Airport Crime Taskforce – East Coast Group focusing on rental car theft after several airports in the region were hit by a large fraud ring. The task force has since grown to include airport police departments from fourteen states and several city, county, and state law enforcement agencies.
>
> The task force is completely virtual and hosted through a Gaggle Mail distribution list, which is paid for by one of the larger airports out of their security budget. Members send suspect images and be on the lookout notices to the task force email address, which distributes the messages to all the other members. Since the members are in the same geographical region, the same subjects are sometimes identified across several locations. The list has nearly 100 members, and most serve as the only representative for their airport or department. This alerts a large network of LEOs who can pass along the information to relevant airport personnel and RAC site managers or employees.

The turnover of RAC site managers makes it difficult to ensure airport and police liaisons have the correct email address for the appropriate person. Airport operators can recommend RAC operators connect the email address to a role instead of an individual (e.g., manager@avis.com). This role-based email would be passed on to the new manager and the liaisons would not need to update their distribution lists.

IN-PERSON

Many airport LEOs and security personnel conduct informal meet and greets during their patrols through the RAC facilities. This enables them to become familiar with RAC employees and build relationships that create the foundation for more open discussion. RAC employees often share information about suspicious activities and security gaps during these meetings.

Many airport LEOs and security personnel meet with RAC site managers or corporate loss prevention officers individually to discuss current security issues or recent incidents. They also use this opportunity to discuss crime trends and security improvement strategies.

During patrols, airport LEOs and security personnel may inform RAC managers of trends at their airport, neighboring airports, or crimes in neighboring jurisdictions to enhance their situational awareness and put them on alert for suspicious activities.

> One airport LEO reported sharing photos of suspects in crimes from neighboring jurisdictions or airports with RAC site managers. This increases their level of awareness and ability to detect potential fraudulent or criminal activities. However, RAC site managers should ensure that they are providing credible intelligence and not improperly profiling their customers based on the characteristics of the individual in the photograph.

TEXT MESSAGING

A less common but effective method of reporting is text messaging. Text message groups can be created between RAC site managers and airport LEOs and security personnel to allow the RAC managers to informally share information about individuals on Do-Not-Rent lists, individuals who recently attempted to commit fraud, and other relevant information with group members. It should be noted that some airports do not allow text messaging to be used in this manner due to their state public records laws.

RAC site managers can set up group texts without airport or police participation. Airport operators can facilitate the group chat by suggesting it to site managers and connecting them to each other.

STAKEHOLDER MEETINGS

Monthly or quarterly airport stakeholder meetings allow managers from tenant companies to discuss different airport initiatives. Security is often a topic at these meetings, with more focused discussions in response to security trends and incidents. Airport operators should encourage RAC site managers and third-party facility managers to participate in these meetings with the goal of working collectively to reduce security incidents and criminal activity occurring at the RAC facility.

> One airport indicated that their local auto theft task force met with RAC executives to discuss the growing trend of stolen vehicles from RAC facilities being used to commit serious crimes in the city. The task force offered several solutions to the executives, such as removing keys from the vehicles and performing background checks on RAC employees. Although the RAC operators did not implement every solution, the airport saw a noticeable reduction in criminal activity after this discussion.

2.3 Theft Packets

The biggest challenge in receiving information from RAC operators is timeliness of reporting incidents to airport police.

At many airports, RAC operator policies for reporting missing inventory or failure to return cases can hinder criminal investigations. Many RAC operators are hesitant to report due to lawsuits and other legal concerns, and often use in-house investigators to attempt to retrieve the vehicle first. This creates unnecessary delays in entering the vehicle and suspect into the NCIC database and notifying neighboring jurisdictions. In many instances, the rented vehicles are recovered, but law enforcement had not been informed of the recovery.

Incident reporting schedules vary widely between RAC operators and airport police as a result of local and state laws. Most operators report after about 30 days, but some may wait up to six months. This is based on the RAC operator following local regulations, the operator's fear of misreporting, and/or poor inventory control procedures.

> The fear of misreporting may be partly driven by a recent lawsuit against Hertz Global Holdings. The company was found to have falsely accused more than 360 people of car theft due to inaccuracies in their own reporting and inventory systems. Many of these incidents resulted in serious consequences for the accused, including felony charges and jail time. Hertz paid a $168 million settlement to the victims and reported that it has since updated its policies to prevent these types of incidents.[1]

In-progress reports (e.g., theft or fraud) should be made to airport police as soon as possible. Requiring the information to pass through multiple individuals can result in unnecessary delays and may corrupt the integrity of the information.

> One airport LEO stated that a RAC manager required all in-progress incidents of fraud or suspicious activity be reported to the site manager who would then report to the airport LEOs. This caused multiple instances of individuals who presented fraudulent documents fleeing the RAC facility before LEOs could respond.

Delays in reporting can also create forensic issues. Video footage may be overwritten or compressed to the point of being unusable, or witnesses may not be able to recall certain details. Relevant information should be collected as soon as possible to preserve details and improve the chances of apprehending criminals.

Explaining to RAC operators why early reporting can improve the chances of recovering the vehicle and prosecuting the criminal may help persuade them to report stolen vehicles in a timely manner. A change to company policies or an audit of the RAC employees' proficiency in adhering to policies may be needed. Airport operators or LEOs can offer to conduct the audit to help the RAC operator identify any necessary changes.

Law enforcement needs very specific information in order to enter the report into NCIC. Using a theft packet ensures that all of the information is complete and collected at one time. Electronic forms can help eliminate human error when entering the information into NCIC as it eliminates the challenges created by poor handwriting. Information typically requested in a theft packet includes:

- Letters for "Demand and Return"
- Signed "Failure to Return" affidavit
- RAC employee witness statement
- Rental agreement with suspect's signature
- Scans of IDs
- Video footage

[1] NYTimes.com. "Hertz to Pay $168 Million to Customers Accused of Auto Theft. December 5, 2022. https://www.nytimes.com/2022/12/05/business/hertz-theft-settlement.html

CBSNews.com. "Hertz CEO promises to 'do right' by customers after false theft reports." April 6, 2022. https://www.cbsnews.com/news/hertz-ceo-stephen-scherr-false-theft-reports/

- Incident report
- Vehicle description including vehicle identification number (VIN)

In addition, airport police will sometimes request:

- Anticipated pick-up and drop-off locations
- Stated destinations and purpose
- Payment transaction information
- How the customer arrived (e.g., on foot, in vehicle, or by public transportation)

The packets require notarization and often cannot be submitted to the police until at least 30 days after the crime or date of expected return of the vehicle; this process is designed to ensure adequate time for the renter to receive a notification letter. The completed packets are typically hand delivered to a LEO patrol or airport police officer.

The accuracy and completeness of these forms are critical to help the airport police investigate and local courts prosecute the case. Vehicle theft is a felony in many states, and the courts will dismiss cases lacking sufficient evidence and information.

One airport's Chief of Police has worked with their legal counsel to create a standard witness statement that can be filled out by the RAC employee. The airport had a number of stolen vehicle prosecutions dismissed because there was no witness statement. The pre-written statement is a fillable PDF with the ability to electronically sign the document. Figure 2-1 below is the redacted pre-written statement form.

Figure 2-1. Pre-Written Witness Statement Form

Date	Case #	Witness Name	D.O.B.

Home Address	Home Phone #

Work Phone #	Cell Phone #	E-Mail

I, the affiant, have been advised the following Voluntary Witness Statement is being made of my own free will:
On the _____ day of ____(Month)____, 20___at approximately ___(Time)___ a.m./p.m., within [Airport County] **, at near**
_____ , I personally witness the following:
(Address / Specific Location / Intersection)
(Please Print Neatly)

When a customer approaches the rental counter, I request a valid driver's license and review the name, photograph and license number. I also compare it to the person that presented the license and I match the license with the form of payment. I am certain in this case that I completed the above; therefore, the person who rented the vehicle was the same person who presented the driver's license to me during the signing of the rental contract.

SECTION 3: EMPLOYEE VETTING AND PUBLIC AREA BADGES

RAC facility employees working at an airport location can be divided into six broad categories:

- RAC site managers
- Counter staff or customer service staff
- Vehicle shuttlers
- QTA staff
- Booth attendants and security
- Shuttle bus drivers

It is common for one individual to perform several of these roles. It is also common for consolidated facilities to utilize a third-party facilities manager who fills some of these roles with their own personnel.

3.1 Operator Background Checks

RAC operators report that background checks they perform on their employees may include a criminal history check, warrant check, driving history, verification of mailing address, and drug testing. Applicants may be disqualified for felonies, crimes directly related to job responsibility (e.g., credit card fraud, auto theft, etc.), or if the applicant shows a pattern of behavior suggesting they will not adhere to rules. In this last instance, the hiring department may request a second evaluation from the director of corporate security.

RAC operators can be sensitive to certain vetting practices because they limit the available workforce. As a compromise, the airport can suggest the RAC operator staff the exit booth and vehicle shuttler roles with an individual who has undergone a more in-depth background check. These roles are in opportune positions to take advantage of their access to vehicles. The background checks of the vehicle shuttlers should ensure they have active driver's licenses and no auto crimes.

3.2 Public Area Badges

Some airports have a designated public area badge for airport workers who do not have an operational need to access the restricted areas of the airport. Airport operators typically either badge every individual who works on airport property, or they badge only the individuals working inside the terminal.

The most significant benefit to the public area badge is the Security Threat Assessment (STA) conducted for all TSA-approved airport badges. Additional suitability requirements, such as a criminal history records check (CHRC), are determined by the airport issuing the badge. These CHRCs are separate and distinct from the fingerprint-based CHRC requirement in 49 CFR §1542.209, as TSA does not authorize a fingerprint-based CHRC or Rap Back enrollment for airport workers who are applying for or hold a public area badge. However, the airport is free to require name-based CHRCs through other services.

> One airport only conducts STAs on RAC employees because they believe a CHRC would impact the available workforce. This strategy may help airports strike a balance between security and available workforce.

Another benefit to providing public area badges to RAC facility personnel is the security training that may be required as part of the badge issuance process. In some instances, this is the same or equivalent to SIDA training and includes topics such as situational awareness, security responsibilities, reporting mechanisms, and emergency procedures. Required recurrent training as part of the badge renewal process reinforces the employees' security responsibilities.

> One airport specifically issues public area badges to create a method of tracking the employees' training.

Some airports that issue public area badges include public area personnel in airport security initiatives, including challenge procedures, penalties for security violations, and incentive programs (e.g., reward and recognition programs). Including RAC employees in these initiatives can help improve situational awareness at the RAC facilities and remind employees of their roles and responsibilities for security at the airport, which strengthens the airport's security culture.

Many airports exclude non-badged employees from their security awareness program, but this overlooks a large airport worker population that can contribute to a positive security culture. Promoting the security program with RAC employees through flyers, promotional materials, recognition and incentive programs, and training will help increase security awareness in the RAC employee population.

CHALLENGES

The biggest challenge for airports desiring to issue public area badges to RAC employees is high turnover. This impacts the cost of issuing the badges as well as badge accountability and control. Each badge has a cost associated with conducting the background check, printing the badge, and training the individual. RAC operators will each need an Authorized Signatory to submit badge applications, and those individuals will also need training.

Additionally, it may be difficult to keep the RAC operators accountable for the public area badges, and the responsibilities associated with lost, stolen, unaccounted for badges, renewals, returned badges, and correctly displaying their badges. Since the badge is not required by federal security regulations, airport operators cannot use federal compliance measures for enforcement. However, airports may have specific rules and regulations that apply to this segment of badge holders.

Some airports use shorter renewal periods for high turnover populations. With this strategy, individuals in these employee groups are issued a badge for a shorter period of time (e.g., three months) at their onboarding. If the individual makes it to the first renewal anniversary, the renewal period is extended slightly (e.g., six months). This can continue as often as the airport operator deems necessary.

BADGING BASED ON ROLE

To conduct background checks on RAC employees without creating unmanageable workforce complications, some airport operators require a public area badge for only certain RAC employee groups. In many cases, the site managers are the only RAC employees required to hold a badge because of their job responsibilities. Third-party facility managers are also frequently badged.

Some airports issue public area badges to RAC counter staff in addition to the site managers because these individuals are customer-facing and handle payment transactions.

One airport operator with shuttle bus service to the RAC facility issued badges to the shuttle drivers to ensure they did not have excess or inappropriate driving or traffic violations. Driving records are not required in TSA background checks, but some airports perform one for airport workers driving on airport property to minimize liability exposure.

Vehicle shuttlers and QTA staff are rarely badged due to the high turnover of the workers, who are often supplied by temporary staffing agencies. These groups of RAC employees, more than any other, will require the airport operator to carefully consider the cost-benefit of badging them. Other strategies used to monitor these employees include access control cards, fuel cards, or cameras.

3.3 Visual Vetting

Most RAC operators require their employees to wear branded uniforms during their work shift. Since employees rarely must display identification media, this is often the only means to visually identify a RAC employee.

RAC employees working in the ready/return area, vehicle storage areas, QTA, or as vehicle shuttlers will typically wear a reflective vest for safety and to stand out from customers. Safety vests are a necessary safety measure for RAC employees but can create major vulnerabilities in the security of the facility.

The biggest challenge with reflective safety vests is that they can be easily purchased by the public and criminals use them to pose as a legitimate vehicle shuttler. Airport operators can suggest marking the vests in some way to distinguish them, such as branding the vests with the RAC operator's logo. Another option is to number the vests or mark them with a unique identifier and assign them to employees. If a vest goes missing, it can be flagged so that an individual wearing the vest with that number or unique identifier will be prohibited from taking a vehicle. If an active vest is used to steal a vehicle, an audit of the vest log should reveal who was assigned the vest on that day to help the investigation.

SECTION 4: EMPLOYEE TRAINING

In general, airport operators and police do not provide security training to their RAC employees for the same reasons many airports choose not to badge their RAC employees: high turnover, limited resources, and perceived low security risk.

RAC operators focus much of their employee training on fraud and counterfeit detection. This may also include some discussions on suspicious behavior indicators. Airport operators can encourage RAC operators to provide more situational awareness and security-focused training to their employees. When possible, presentations or materials created for the airport security training can be provided to corporate security or site managers with the intent that they provide the information to their staff.

4.1 Situational Awareness and Response Training

Situational awareness and response training helps RAC employees and site managers identify suspicious activities and security gaps, take appropriate actions to alert law enforcement, and maintain their personal safety during an incident. RAC operators provide some situational awareness training to their employees, but the material is very high level. The airport operator could potentially reduce criminal activities throughout the RAC facility by providing more in-depth training to RAC employees.

If RAC employees are issued a public area badge, they may receive the security training required for SIDA badges, depending on the airport's requirements. The topics of this training include airport rules and regulations, security responsibilities, situational awareness, and challenge requirements. Additionally, this training is recurrent, so the badged employees receive refresher training.

If the population is not badged, the only training offered from the airport is typically provided by airport LEOs. This is most often done informally during meet and greets with RAC employees. The topics of conversation are typically reminders of security responsibilities and are usually based on recent incidents or trends in security violations (e.g., propped doors). This training is not required, so it is not consistently or regularly given.

Only a small number of airport police indicated they had created a presentation or more formal training for RAC employees and site managers. Training topics airport LEOs offered to RAC employees and site managers included situational awareness, fraud indicators, rental vehicle theft case studies, fraud and counterfeit identification, and response to a rental vehicle theft, attempted theft, or suspicious person attempting to rent a vehicle. Most of these presentations were only used once as the high turnover made scheduling training too difficult.

Training can be given in multiple formats, but the most common is informally as one-on-ones with RAC site managers and employees. PowerPoint presentations can be specifically designed for RAC employees and the RAC facility. Topics can include red flag suspicious behavior indicators, airport security policies, and reporting channels.

> One airport's Chief of Police included actual CCTV footage in their presentation to highlight what suspicious activities look like in the real world at their airport.

Security awareness training for RAC employees should cover the following topics:

- Airport security policies and procedures
- Reporting policies and contact information

- Taking note of and reporting:
  - Suspicious statements, people, vehicles, or transactional anomalies
  - Missing equipment
  - Denial of service to suspicious individuals
- Emergency response
- Active shooter
- Assisting passengers during emergencies
- Personal safety
- Challenging other RAC employees

> The FBI, DHS, and TSA produced a video on vehicle rentals used in vehicle ramming attacks for the Truck Renting and Leasing Association and the American Car Rental Association. The video, entitled "Partners in Prevention: Vehicle Rentals and Vehicle Ramming," primarily focuses on heavy truck rentals but provides several examples of suspicious behaviors and red flags in vehicle rental customers. The video is only eleven minutes long, is hosted on the FBI website. This video could be sent to RAC site managers with the recommendation that they show it to their staff.[2]

Below are common training prompts included in situational awareness training across multiple industries:

Potential Risk Indicators of Vehicle Rental Fraud

Timing:

- Same-day reservation or within the past 24 hours, especially within one hour of pickup
- Undetermined date of return

Documents:

- Cannot present a boarding pass or itinerary
- Inability, reluctance, or refusal to produce required documentation
- Reluctance to provide complete personal information when completing the rental paperwork
- Providing multiple or inconsistent names, addresses, phone numbers, or other information on rental paperwork
- Providing a local address or phone number but presenting an out-of-state ID
- Presenting a foreign license without a passport
- Using cash for large transactions or a personal credit card in someone else's name

Behavior:

- Carrying no luggage but arriving from the airport
- Inability to recall information used to rent a vehicle
- Unusual nervousness
- Intended use of the vehicle is inconsistent with its purpose (e.g., renting a four-door sedan to move house)

[2] FBI.gov. "Partners in Prevention: Vehicle Rentals and Vehicle Ramming." Accessed April 30, 2024. https://www.fbi.gov/video-repository/vehicle-rentals-vehicle-ramming-013019.mp4/view

- Difficulty in explaining the planned use of the vehicle
- One or more open rental contracts

Inquiries:

- Inquiring about the price of vehicles in the lot or requesting the most expensive vehicle
- Unusual interest in the vehicle's size, weight, speed, capacity, clearance, and accessories, e.g., window tinting
- Unusual questions regarding mass gatherings, government, military, law enforcement, critical infrastructure, and key resources

Returned Vehicle Risk Indicators

Observations:

- Staining, discoloration, or unusual chemical odors in the passenger, trunk, or storage compartments
- Indications of vehicle tampering or alteration, e.g., panels misaligned, screws or fasteners missing, seats missing or ill-fitting
- Bullet holes, blood, guns, or other evidence of a potential crime

Items:

- Receipts for hazardous items or weapons
- Maps, blueprints, brochures, or photographs of landmarks or sensitive or critical locations
- Missing equipment, accessories, or license plates

Training can be developed and delivered by airport law enforcement, the ASM, or other subject-matter experts, such as the airport's crime analyst.

4.2 Fraud and Counterfeit Training

Fraud and counterfeit activities are a major concern for RAC operators, evidenced by the high number of calls for fraud and counterfeit, and the widespread use of ID verification equipment across RAC operators and airports.

> One RAC operator reported that their employees receive training on fraud and counterfeiting during their extensive onboard training. The orientation training also includes modules on business integrity, focusing on customer service and ethics. This RAC operator also requires annual recurrent fraud and counterfeit training.

During the rental agreement finalization, RAC employees are generally trained to ensure the names on all documents match, such as driver's license, credit card, passport, and itinerary. Many RAC operators require two forms of ID to rent exotic and expensive vehicles. To help prevent vehicle theft through fraud, most RAC operators also require a credit card that matches the name of the driver on the contract.

Since RAC employees are generally equipped with the training and policies necessary to identify fraudulent or counterfeit documents and alert law enforcement of suspicious documents, airport operators may find training efforts are better spent on situational awareness and security trends.

However, some airport operators may develop a fraud and counterfeit training program for the RAC employees if the RAC operator does not utilize document verification equipment or if there is a rise in

reported incidents. Much of the fraud and counterfeit training available for all industries covers the following:

Verification Methods

Identification documents, including international documents:

- Compare ID photo to customer and verify descriptors (e.g., eye color, height) match the individual
- ID address matches provided address
- Leveraging technology (ID scanners)

Forms of payment:

- Credit card information matches ID
- Credit card information matches transaction data on computer
- Paper money shows appropriate security features
- Leveraging technology (currency checkers)

Additional information requests:

- Two phone numbers and emails
- Flight itinerary
- Two proof-of-address documents
- Credit check

Red Flag Indicators

Fraudulent, stolen, or incomplete identification documents:

- Incorrect state holograms
- Fuzzy letters and numbers
- Misspelled words
- Peeling or loose lamination
- Raised edges around the photo
- Jagged edges, abnormal card thickness, or abnormal card flexibility
- Physical description on ID does not match customer

Fraudulent, stolen, or incomplete forms of payment:

- Large spacing of the letters in the names printed on the card
- Magnetic stripe is scratched off
- Stickers cover the security code
- The bank corresponding to the bank identification number does not match the bank listed on the card

Suspicious Behavior

- Distractions during the payment transaction
- Unusual payment requests, e.g., manually enter credit card information

Reporting Methods

- Discretely alerting others to fraud and counterfeit transactions
- Using predetermined code to alert the RAC site manager
- Maintaining control of documents and making copies
- Reporting mechanisms and policies

In-progress crime reports should include:

- Location of the incident (e.g., Garage A, level 1, Sixt rental counter)
- Explanation of the situation and when it happened (e.g., right now or within last five minutes)
- Description of the vehicle (if applicable) including make, model, year, color, and license plate number
- Brief description of the suspect including sex, age, height, identifying features, and one to two items of clothing they were wearing

The American Association of Motor Vehicle Administrators provides additional training resources for identifying counterfeit and fraudulent IDs.[3]

[3] **American Association of Motor Vehicle Administrators:** https://www.aamva.org/

SECTION 5: ENFORCEMENT MECHANISMS AND AUTHORITIES

Most airports do not have detailed security requirements or standards that RAC operators must meet or that are enforceable. Often, security is only mentioned with reference to complying with federal regulatory and airport security requirements found in airport rules and regulations or local ordinances. Additionally, security compliance references are sometimes included in the tenant lease and/or concessions agreement. Security requirements described in the lease or concessions agreements, airport rules and regulations, and local ordinances are usually very general.

Typically, RAC operators are not required to share their security plans, although they may be required to have them. One airport operator shared this clause from their airport rules and regulations:

> Policies and Procedures for activities within the Rental Car Center. [T]he Department may promulgate such additional written policies and procedures for the safe and efficient conduct of activities within the Rental Car Center that may be appropriate, a copy of which shall be provided to each Rental Car Company. All Rental Car Companies, their employees, contractors, and subcontractors shall comply with such written policies and procedures.

Another airport's lease agreement states:

> [The tenant must] [m]aintain a security plan to preserve safety and preclude damage and thefts, including but not limited to auto thefts.

Most of the enforcement mechanisms used to ensure compliance from RAC operators also delineate responsibilities for the various operations at the RAC facilities. For example, airport police may be responsible for patrolling the common areas, but the RAC operators may be responsible for their exclusive areas; the airport may be responsible for the base build of the facility, but the operators may be responsible for the equipment and the third-party facility manager may be responsible for the maintenance of the facility. Careful delineation of airport and RAC operator responsibilities in governing agreements or regulations will enhance the effectiveness of enforcement mechanisms.

Further discussions on enforcement mechanisms and legal agreements with tenants can be found in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*.[4]

5.1 Lease and Concessions Agreements

Lease and concessions agreements are common enforcement mechanisms used to ensure and enforce compliance with the airport's security requirements. The agreements do not always contain specific security language, but they usually will reference compliance with the airport's security and safety requirements and/or airport rules and regulations.

> One airport LEO described an event with a franchise RAC operator that airport police were called to mitigate. The RAC operator ran out of vehicles for their holiday customers, which resulted in stressed holiday travelers waiting in long queues in the crowded baggage claim. This created a massive security vulnerability in baggage claim that airport police struggled to manage.

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

> The disruption was so great that the airport board considered legal action to terminate the lease contract. The airport board would have based this decision on a requirement in the agreement to maintain a high service level.

It can be challenging to modify or amend lease or concessions agreements; many agreements can have terms of 30 years or more. Airport operators interested in modifying or updating the requirements in the lease agreement should work with their legal counsel, business office, and RAC operators to determine workable solutions. Leases or agreements that reference airport security regulations or local ordinances can be amended by changing the regulations or ordinances. These changes will have to apply to all tenants and concessionaires, not specific ones.

5.1.1 RAC Consortium

Airports with consolidated RAC facilities often require RAC operators to form a consortium that acts as a single voice for tenants in the facility based on a shared-use model. This requirement is typically included in the airport's lease or concessions agreement. Some airport operators without a fully consolidated RAC facility will require consortiums to manage specific shared RAC operations, such as a QTA or shuttle buses. These consortiums can also serve as exchanges for sharing security information, equipment, and resources in areas of common concern.

The benefit of consortiums to airport security is that physical security measures, and often technology, are deployed uniformly across the RAC operator exclusive spaces. Each operator contributes to the consortium budget, which is often used to procure a third-party facilities manager to handle certain operations, hire contract security, or procure equipment. The consortium will often appoint a liaison, typically the third-party facilities manager, to conduct discussions and attend meetings with the airport representatives. This position can be useful to help RAC operators cooperate, collaborate, and compromise on a wide variety of issues.

Below is sample language from an airport concessions agreement that requires the formation of a RAC consortium and the airport's participation in that consortium:

> Industry Agreement. Concessionaire shall enter into an agreement with the other Concessionaires for the joint use, maintenance, and operation of the Joint-Use Facility ("Industry Agreement"). Pursuant to the Industry Agreement, Concessionaire and the other Concessionaires shall form a management committee ("Management Committee"). The [Airport] shall be entitled to appoint a non-voting representative to the Management Committee who shall receive all communications, meeting notices, or other communications that would otherwise be afforded a voting member of the Management Committee. The appointment of a[n Airport] representative is for information and advisory purposes only and does not obligate or bind [the Airport] in any way to the actions, duties, and obligations of *the* Management Committee. The terms and conditions of the Industry Agreement shall be reviewed and approved by the [Airport]. Concessionaire must continue full participation in the Industry Agreement and meet all obligations thereunder for the term of the Industry Agreement.

Below is language taken from a concessions agreement requiring shared responsibility for the maintenance and repairs of the common use areas:

> Concessionaire Maintenance and Repair Responsibilities. […] The maintenance obligations of Concessionaire for any Shared Premises shall be shared between the Concessionaires occupying the Shared Premises.

RAC operators are not inclined to form consortiums unless obligated to do so, and the airport operator may experience pushback from RAC operators.

5.1.2 Contract Security

Many airport operators allow RAC operators to employ contract security services to patrol the RAC facility, staff the exit booths, shuttle vehicles, or monitor CCTV. Authorizing language can be mandatory or permissive. Below is an example of language in an airport concessions agreement that governs the use of contract security services at the RAC facilities:

> Security. Concessionaire, at its own expense, shall secure all exit lanes on its Premises in a method and manner approved in writing by the [Airport] to prevent the theft of vehicles. Concessionaire, at its own expense, shall also provide any additional or supplemental security services or devices required in writing by the [Airport], including private security services. Concessionaire may also provide any additional or supplemental security services or devices that Concessionaire may desire, at its own expense, except that such additional security must be approved, in writing, by the [Airport]. Any extra security shall be subject to the authority granted to the [Airport Police] and shall in no way interfere with the duties of the [Airport Police].

5.1.3 Facility Management

Typically, the airport operator will develop consolidated RAC facilities with all the basic safety and security measures in place. Sections of the facility will then be leased to the RAC operators. Often, the airport facility team is responsible for maintenance of the airport-owned buildings throughout the campus. Sometimes these teams hire a third-party facility manager to perform the usual functions of the facility team at the consolidated RAC facility. This allows them to concentrate their focus on higher priority buildings.

Alternatively, the airport operator may require the RAC consortium to hire a third-party facility manager to operate and/or maintain the consolidated facility and its functions. This requirement would be stated in the lease agreement. Below is an example from a concessions agreement requiring the RAC consortium to contract a third-party facility manager to operate the consolidated RAC facility:

> Facility Manager. Concessionaire and the other Concessionaires, at their sole expense and at no expense to [the Airport], shall retain a third party manager ("Facility Manager") to ensure full performance of the obligations and responsibilities of Concessionaire under this Agreement and the Concessionaires under their Concession/Lease Agreements, and to serve as a direct liaison with the [Airport] regarding the Concessionaires' use and operation of all portions of the Joint-Use Facility and performance in accordance with the Concession/Lease Agreements.

Each consolidated RAC facility operated by a third-party facility manager has unique rules and expectations of the third party; the duties of the facility manager are laid out in the contract with the airport or the RAC consortium. Some agreements request no security functions from the third-party facility manager, while others expect the facility manager to provide 24/7 security. The most common responsibilities of the facility manager are to maintain the facility and equipment—such as plumbing, vacuums, landscaping, lighting, road repairs, barriers—and ensure compliance with regulations regarding fuel safety, used oil, washer fluid, and other hazardous materials.

One airport outlined the third-party facility manager’s responsibilities in the concessions agreement with the RAC operators:

Duties of Facility Manager. The duties of the Facility Manager shall include, but not be limited to, the following:

- Receive and review information and documents from the Concessionaires, [Airport], and third-party contractors related to the operations of a rental car business;
- Prepare and solicit proposals for the maintenance of the premises leased to the Concessionaires;
- Comply and abide by the directions of the Management Committee;
- Report to the Management Committee;
- Act in accordance with the agreement(s) between the Concessionaires and the Facility Manager;
- Keep minutes of meetings of the Management Committee and provide them to the [Airport] after every meeting;
- Provide the [Airport] with an executed copy of the agreement(s) the Facility Manager has entered into with the Concessionaires, and any and all amendments;
- Make available to the [Airport] all books, records, vouchers, checks, papers, and documents kept or maintained by the Facility Manager related to this Agreement, the Concession/Lease Agreement(s), or the Industry Agreement;
- Train the Concessionaires' employees, and oversee vendors, contractors, and invitees;
- Ensure that all maintenance required by the Concessionaires is performed;
- Schedule, coordinate, monitor, respond to, and notify the [Airport] about required maintenance and preventative maintenance that is the responsibility of [the Airport];
- Create and enforce a training program for operations at the [RAC facility], which shall be approved in advance by the [Airport];
- Manage and coordinate locks, keys, and access control cards for the [RAC facility] in accordance with this Agreement, the Concession/Lease Agreement(s), and [Airport] policies;
- Manage access to the [RAC facility] by the Concessionaires' employees, vendors, contractors, and invitees;
- Coordinate with the [Airport] any improvements and changes made by the Concessionaires

Third-party facility managers have full control of the facility's operations budget and how the funds are distributed, with minimal input from RAC or airport operators. This includes full authority to initiate procurement of equipment or services that improve or enhance the operations and longevity of the facility, such as contract security guards and new security barriers, within the purchasing requirements of the airport authority.

One third-party facility manager described a situation where he found unused funds in the operations budget. He gathered the RAC executives and proposed using this additional funding to add cameras throughout the facility to enhance security. The RAC executives agreed, and the facility manager contracted the installation of 50–60 cameras in high-risk areas. A third-party surveillance suite was added to centralize footage from the cameras, which also enabled the airport, airport police, RAC operators, and third-party facility manager to quickly access the footage.

5.1.4 Facility Modifications

RAC operators are often allowed to make changes to their exclusive area with airport operator approval. Requirements and limitations to modify facilities on airport property are typically laid out in the lease agreement. The process for seeking permissions and permits for changes in leasehold areas is often covered by airport tenant improvement policies. The approval process is usually a work permit form or submission of a construction plan to the airport facilities or concessions department. Security personnel should be included in the approval of any security-related requests to ensure they have full awareness of the security measures in the facility. This includes the addition of security equipment, such as barriers or cameras.

Below are example clauses that control the RAC operator's ability to modify the facility:

> Tenant Compliance. Tenants are obligated to submit proposed tenant improvements using the current Tenant Design Standards Guidelines and submit a Tenant Improvement Application to the [Airport] Tenant Relations Coordinator and follow the approval process. Tenants are to familiarize and comply with any Maintenance Matrix guidelines associated with their lease agreements.
>
> Ownership of Tenant Improvements. Unless otherwise provided in a lease agreement, fixtures, installations, additions, alterations, and improvements made by the tenant on Airport premises becomes the property of the [Airport] upon the termination or expiration of the tenant contract without compensation to the tenant. The tenant may remove trade fixtures and equipment as specified in the Tenant's agreement with the [Airport] provided that damage to the infrastructure that may occur in the process is immediately repaired.
>
> Tenants shall not remove or demolish, in whole or in part, any improvements to the premises without prior consent from the [Airport]. The [Airport] may require the tenant to replace whatever is removed. Tenants should refer to their Agreement with the [Airport] for other contract termination requirements.

5.1.5 Fuel Theft

Fuel theft from the QTA is a problem at many airports. Assigning fuel cards to RAC employees can help track fuel consumption by user and identify anomalous transactions, but it does little to prevent fuel theft from occurring. More information on fuel cards can be found in Section 6.3.

One airport included the following language in their lease agreement to enforce penalties against the RAC operator for fuel theft:

> In the event an agent or employee of Lessee, or anyone using the access media issued to such an individual at the request of Lessee, misappropriates fuel, Lessee shall remain responsible for the charges unless the airport had actual possession of written notice to suspend the function of the access media used, prior to the misappropriation.

5.2 Airport Rules and Regulations

Airport rules and regulations are used to convey necessary security, safety, legal, and operational requirements to airport tenants. All tenants with a lease or concessions agreement with the airport are required to comply with these rules. It is common to reference the rules and regulations in the lease or concessions agreements with RAC operators.

In many instances, it is much simpler to modify or update the airport rules and regulations than it is to negotiate an amendment to a lease or concessions agreement. Any changes to the airport rules and regulations would apply to all tenants and concessionaires.

5.2.1 Additional Policies

The majority of security requirements and standards are expressed through the lease or concessions agreement and airport rules and regulations. However, airport operators can also create other policies, such as Technology Design Standards that govern how tenants can integrate with the airport's network infrastructure, or Video Surveillance Policies that govern how the footage can be used for security purposes.

One airport has the following language in its Video Surveillance Policy indicating that the tenant must have policies in place to govern the compliance of the system with privacy laws:

> The Authority may permit its IT Network and Integrated Security System backbone to be used by airport tenants to install their own cameras. In such cases, the Authority will not view, record, or store the images collected by airport tenants. Furthermore, airport tenants will be expected to have their own policies in place regarding the collection, use, and disclosure of personal information collected through these cameras, in compliance with applicable privacy legislation.

Another airport's Surveillance Technology Policy states:

> The Airport limits its use of recordings and other data from Tenant security cameras to the following authorized use cases and requirements listed in this Policy only.
>
> Authorized Use(s):
>
> 1. Reviewing camera footage in the event of an incident.
> 2. Approving Tenant's disclosure of digital recordings and other data from its security camera system.
>
> Prohibited use cases include any uses not stated in the Authorized Use Case section

5.3 Local Ordinances

State and local laws highly impact airport police investigative, enforcement, and prosecution capabilities. Most often, prosecution decisions will be made by external agencies like a district or state attorney's office. Some jurisdictions may require more proof or evidence of a crime beyond a mere showing of probable cause to initiate a prosecution. For example, one airport LEO indicated that local prosecutors had declined to proceed with several stolen rental vehicle cases because they lacked witness statements.

Airport operators looking to utilize local ordinances or state laws to help address concerns over criminal activity in RAC areas should coordinate with the local prosecutor's office. Understanding their requirements for successful prosecution will help the airport operator and police build a more effective enforcement program.

Some airport police have sought to reduce crime around RAC facilities by adopting and enforcing rules and local ordinances targeted at limiting access to those facilities to only those persons with legitimate business at the facilities. The example provided below is an attempt to use trespass regulations codified in a local ordinance.

Dallas Fort Worth International Airport enacted Resolution 2020-03-073, which limits use of the airport to authorized users completing business at the airport. The Resolution states:

Use of the airport terminals, terminal garages and rental car facilities will be limited to authorized users defined as arriving and departing passengers, hotel guests, persons meeting or picking up arriving and departing passengers, persons engaged in activities in which a permit has been issued by the Airport, employees and other personnel necessary for, or related to, the operation of the Airport and the rental car facilities.

This language gives the airport the authority to issue trespassing violations and remove individuals from airport property, including RAC facilities.

In general, airport security or police will issue a warning to trespassers in non-secure areas of airport property before taking further action. However, if the individual continues to remain on the property, airport police may be required to remove them. Whether an airport representative or LEO issues the warning varies by state, jurisdiction, and airport.

5.4 Compliance Assurance Measures

Regular security audits and inspections can reveal vulnerabilities that may allow criminals to bypass the security measures at RAC facilities or uncover criminal activity that has occurred.

Visual inspections of the security equipment and mechanisms in place can identify deficiencies and anomalies, such as loose bricks near traffic spikes, concrete barriers that have been shifted, or cable systems that are unsecured. Formal risk assessments and inspections should include the ASM, airport police, and the RAC operators or their liaison. A thorough inspection of each piece of equipment, camera field of view, access portal, and the facility perimeter should be conducted with the goal of identifying opportunities for criminals to commit crimes in the RAC facilities. These inspections can be done annually or biannually to ensure each facility's security profile is responsive to current crime trends.

Some airport operators hire a security consultant to conduct a site visit of consolidated RAC facilities to identify vulnerabilities. The consultant will prepare a report and then walk through the buildings with airport security and police to review the report, which can help airport police, security, operations, and RAC operators prioritize the security projects proposed by the consultant. RAC operators also occasionally hire consultants to perform risk assessments of their exclusive operating areas after experiencing a rise in criminal activity or before a new facility opens.

Audits can be performed on key logs, identification cards, fuel reports, security policies, training logs, or any other data on the RAC operations that is tracked. The goal of these audits is to identify discrepancies that could indicate criminal activity or a need for additional training. Audits are usually performed more frequently than inspections, sometimes monthly or quarterly.

Airport security and police can also test the RAC employees to identify individuals who are not following airport or RAC operator's policies or security measures that should be implemented. Tests can take several forms, such as integrity checks, which test if the QTA staff will report abandoned items, or a "secret shopper" who tests the RAC customer service employees by attempting to rent a vehicle with a fraudulent ID or credit card.

One airport operator indicated that they regularly perform integrity checks on RAC employees with the support of RAC corporate security. The RAC security manager will provide a vehicle for the airport representative to pose as a rental customer returning a vehicle. Cash, iPads, phones, and other attractive items will be "abandoned" in the vehicle to see if RAC employees return the property in accordance with their policies. Tracking devices may be used to help find the items if they are not properly returned. Employees caught stealing "abandoned" property are always terminated and are often also criminally charged. Collaborating with RAC corporate security provides transparency into the airport's security operations and helps the RAC operator evaluate their processes.

Airport operators can assign some of these quality assurance activities to LEOs or security personnel.

5.5 Penalties

Some airports will apply penalties to tenants for not adhering to security requirements outlined in the rules and regulations or the concessionaire and leasing agreements. Below is sample language from an airport's concessionaire agreement stating very clearly the consequences of breaching provisions in the contract:

Operations Violations. Concessionaire's failure to adhere to the operating requirements set forth in this Agreement is reasonably anticipated to result in significant inconvenience to the public, adversely affect the overall commercial business of the Airport, and reduce the amount of rent to be paid to Authority. Additionally, Authority resources will be expended in dealing with violations of this Agreement by Concessionaire. The parties hereby agree that total damages sustained by to Authority for violations of the provisions of this Agreement addressing this subject matter could be significant, but would be difficult to determine and to track. Therefore, the parties hereto agree that the liquidated damages amounts, set forth below for violation of Agreement terms addressing the referenced subject matter are reasonable estimates of the loss anticipated to be suffered or incurred by Authority. Concessionaire, therefore, hereby agrees that imposition of the liquidated damages set forth below is fair and reasonable and Concessionaire agrees to pay immediately upon demand by to Authority the following amounts as liquidated damages upon the occurrence of breaches, in any Agreement Year, related to operation violations:

- $100 per occurrence – first occurrence
- $200 per occurrence – second occurrence
- $300 per occurrence – third occurrence
- $1,000 per occurrence thereafter

For hours of operations violations, liquidated damages shall be as follows:

- $100 per hour or portion thereof, during which location is not open – first occurrence
- $200 per hour or portion thereof, during which location is not open – second occurrence
- $300 per hour or portion thereof, during which location is not open – third occurrence

5.6 RAC Policies and Procedures

On occasion, the airport operator must request the RAC operator adjust or add policies or procedures to comply with the airport's security requirements. In many cases, this may be a simple request of the RAC site manager that does not need to go further than the airport location, such as requesting the RAC employees call the dispatch number directly or that they remind customers that they must return the vehicle to the designated return area. Other policies may require more persuasion or incentives, such as requesting the vehicles be de-keyed before the closing manager leaves for the night.

The most difficult policies to work with will be at the corporate level, such as more robust background checks. Good relationships with RAC corporate executives, as well as persuasive and quantitative data to show a need, can help encourage discussions and compromises.

Airports should be prepared to offer a solid justification, compromises, and incentives as part of the discussion if they want to maintain a good relationship with the RAC operator.

SECTION 6: TECHNOLOGY

RAC operators are typically granted authority to install technology within their exclusive leased space and with airport approval. This often creates inconsistencies in technology deployed by the various operators across the airport and within consolidated RAC facilities.

Ownership of technology within the facilities can also create some challenges. RAC operators often deploy systems within their exclusive leased space but require formal requests from the airport operator for the footage or reports from those systems. Airport operators may add their own technology systems, but they often limit installation to common areas (e.g., customer lobby) and critical or vulnerable areas.

Cameras, access control measures, and fraud and counterfeit identification equipment are common technologies that airport operators require or request RAC operators to install in their exclusive areas.

6.1 Surveillance Systems

Actively monitored surveillance systems are one of the most practical and universal security solutions to improve public area security. Many airports are currently or have recently undergone a CCTV system upgrade to replace outdated analog cameras with digital, multisensory cameras and video analytics. Often, installing or upgrading the surveillance system is the easiest and most effective way to improve the security in an operations area.

> One airport LEO mentioned that the QTA was equipped with a standard perimeter alarm system that is activated when the facility closes for the night. The system sounds an alarm and sends a notification to dispatch security when the area is entered. This is a low-cost solution that has been successful for this airport.

6.1.1 Security Cameras

Security cameras are quite common in RAC facility areas of all types (e.g., flat lots, consolidated ready/return areas, QTAs, lobby counters). Adding or upgrading cameras throughout the RAC facilities can provide a measure of visible deterrence while improving the airport operator's surveillance within and around the facilities.

Ideally, camera infrastructure (power and internet connection), location and sight lines, and ownership should be determined during the design and construction phases of the facility. This is critical to ensure that the infrastructure does not limit the operability of the cameras.

> Several of the first consolidated RAC facilities at airports included infrastructure that did not support a digital surveillance system. This infrastructure had to be added or upgraded later.

It will save the airport operator time and money to include camera infrastructure during RAC facility design and construction, even if cameras will not be installed until a later date. Adding power and network infrastructure to a completed structure is much more expensive than if the appropriate infrastructure had been included during initial construction.

> One airport operator described an outside access door to the consolidated RAC facility that had been propped open several times. There were no cameras facing the door and the facility did not have power running to the outside of the building where a camera would need to be placed.

To solve the problem, the airport operator attached a solar-powered camera to a nearby pole, which allowed security to capture footage of a RAC employee propping open the door. However, one disadvantage of the camera was that the footage was captured on a storage card that had to be retrieved from the camera to be reviewed because there was no internet connectivity.

Parking garages or lots with overhead coverings allow for cameras to be mounted on the ceiling for footage to be captured almost anywhere within the building. Open lots will require the cameras to be mounted on light poles or other structures, which may limit the camera's view of the area.

When determining camera locations within a RAC facility, priority of placement should be given to:

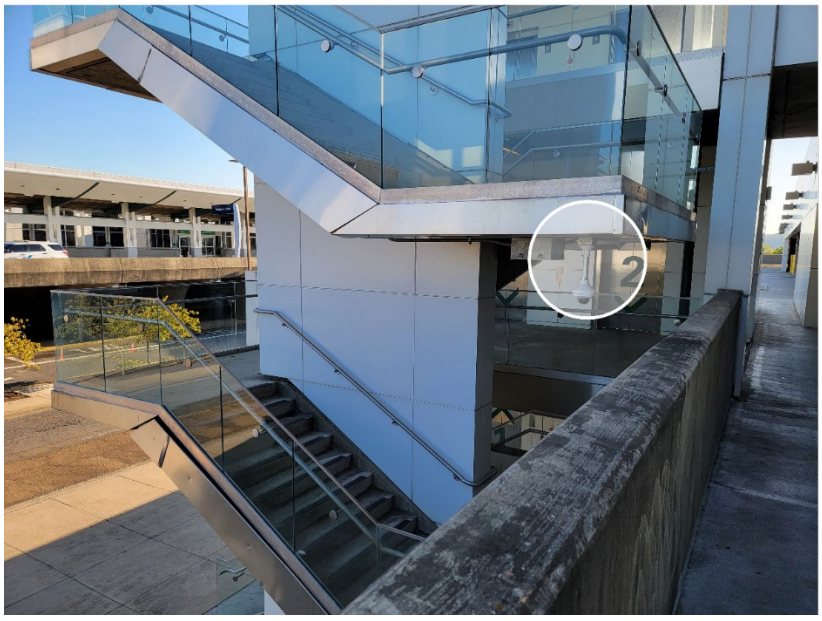
- Exit lanes – facing the driver
- Entrance lanes – facing the driver
- Customer service lobby – facing the customer
- Known vulnerable areas

Secondary priority should be given to:

- QTAs
- Areas where pedestrian and vehicle traffic cross
- Vertical cores (i.e., elevators, stairs, escalators)
- Vehicle storage locations
- Customer service lobby – capturing queues and crowds
- Customer service lobby – facing the employee

Most airports have outdoor cameras along the main terminal roadways, curbsides, and exteriors of parking areas. When possible, airport operators can position cameras along the customer journey to capture critical RAC areas, such as crosswalks from the terminal and RAC facility entrances and exits. Strategic placement of cameras in these areas can help airport security retrace a suspect's route during investigations. Figure 6-1 shows a camera that has been mounted in the stairwell for extra surveillance along the customer journey.

Figure 6-1. Camera Mounted in Stairwell



To be effective, cameras need to be positioned to ensure they not only capture critical areas and avoid blind spots but are not adversely affected by lighting variations, obstructed sightlines, and weather. Consultants can perform help determine the most effective mounting locations, where infrastructure is needed, and the best types of cameras. A good practice is to physically walk through the RAC facility with the planner and airport security or police to assess where the cameras will be deployed and each camera's capture area. A security risk assessment helps to ensure optimal camera placement.

> Many airport operators noted making changes to the original camera placement plan based on a walk-through. One airport operator performs a walk-through every five or so years to determine if the camera positions reflect current crime trends and operational changes in the area.

Cameras with pan-tilt-zoom (PTZ) capabilities are useful for active monitoring. Wide-angle cameras are effective for large, open spaces such as flat lots. Multidirectional cameras can monitor several directions simultaneously, as the camera heads can be positioned independently; these cameras can provide up to 360-degree coverage and are useful for areas with few viable mounting locations.

ACCESSING CAMERA FOOTAGE

Requesting footage from RAC operators can be challenging, but building a relationship focused on mutual security can help optimize the process. Many RAC operators have a policy requiring a formal email request from law enforcement or a subpoena. Knowledge of the operators' policies can help reduce unnecessary inquiries and delays.

Typically, each RAC operator has a small number of individuals authorized to access camera footage. In some cases, the footage can only be accessed offsite or by a regional manager. Airport operators and law enforcement departments can create a list of these authorized individuals and their contact information to request the footage directly from them and minimize delays.

Timely footage retrieval is often critical to solving criminal investigations in RAC facilities. Most RAC operators wait at least 30 days to submit a report of a stolen vehicle. Typical camera systems cycle the video footage every 30 days or so, compressing the old footage to save room in archive storage. This compression, depending on the extent, can make video footage pixelated or fuzzy, and make it difficult to identify small details and features.

Airport operators can assist RAC operators and airport police by ensuring video retention policies account for RAC operator reporting schedules and do not compress the footage before the minimum reporting deadline.

6.1.2 Video Analytics

Video analytic technology is frequently used to help airport police conduct stolen vehicle investigations. Video analytics can offer greater detection of security incidents and criminal activity and require less reliance on video monitoring.

Motion-activated cameras or video analytic technology can detect motion to alert security personnel of activity in a defined area. This may be useful for the perimeter of RAC facilities, especially in areas where pedestrians and vehicles are prohibited. This may also be useful for RAC facilities that close during certain hours, as airport security can focus on other areas until a motion alert is triggered. A similar technology is voice-activated recording. This may be less practical in a noisy traffic area but could be useful in enclosed lobbies that are locked overnight.

Facial recognition is a rapidly growing technology that could be useful for RAC facility surveillance, if authorized by governing laws. The technology can compare surveillance footage to law enforcement databases to identify individuals during criminal investigations. While more industries are moving toward facial recognition technology, some states highly regulate its use in public areas. For instance, Kentucky enacted a mandate that limits how law enforcement agencies can use the technology in their investigations (Ky. Rev. Stat. § 61.9305).

> One larger airport police department has access to facial recognition technology that it uses on behalf of other airports.[5] The (often smaller) airport police departments forward images of suspects in criminal investigations to the larger airport police department, which then uses the technology to compare suspects' images to several law enforcement databases.

To effectively utilize facial recognition capabilities, cameras need to produce good video quality and be positioned to capture an image of the suspect's face. Cameras can be mounted on bollards or attendant booths at vehicle height to capture the driver's face as they exit the facility (Figure 6-2).

Figure 6-2. Camera Mounted to Exit Booth to Capture Driver Images

Footage from cameras mounted behind the RAC counters to capture customer faces can also be used in investigations of fraudulent activity.

6.1.3 License Plate Readers

License plate readers (LPR) are used by some RAC operators within their exclusive space to track their fleet inventory. Airports occasionally install LPRs within the RAC facility, but it is much more common and efficient to mount the LPR on the access road leading to the RAC facility entrance or on the road where vehicles exit the facility.

Figure 6-3. LPR Pointed at Vehicle Exit

Many airport operators and police install LPRs along primary ingress/egress roads. This allows the airport to monitor more vehicles around the airport than solely rental vehicles, and can also assist with establishing timelines for investigations. Portable LPR trailers can be moved and stationed throughout the airport campus to address security trends. These provide a high level of deployment flexibility with minimal infrastructure requirements as most are solar powered.

LPR cameras inside RAC facilities are most often mounted at the entrance/exit, as shown in Figure 6-3, or a mobile LPR is used by a RAC employee walking through the ready/return and vehicle storage areas.

[5] All participating airports follow all requirements for use of facial recognition in law enforcement activities in their jurisdictions.

The output from an LPR is typically connected to law enforcement databases for identification. Many LPR vendors allow airport police to lease cameras and provide and maintain the connected vehicle databases.

Lighting is a critical component for accurate license plate recognition. Reflections from nearby lights or glare from the sun can obscure the plate number, and low light can also make it difficult to interpret. Stationary LPRs should be tested in low-light conditions and during different periods of the day when light levels change significantly, especially sunrise and sunset. Other factors, such as the color of the license plate and font, can cause the LPR to misinterpret or fail to read the license plate number. Multiple performance tests throughout the camera's life cycle can identify changes that may cause problems for the camera.

It should be noted that standard surveillance cameras strategically positioned within RAC facilities are capable of capturing good images of vehicle license plates. The airport police can then upload the image or enter the information into relevant vehicle databases.

6.2 GPS Tracking Systems

Luxury vehicles typically have built-in GPS tracking capabilities. Some systems even have the ability to disable the engine so that the vehicle can be retrieved from wherever it is parked. RAC operators do not turn on the GPS for airport police unless a formal investigation case has been opened, and some require a warrant first.

RAC operators will often use GPS technology to attempt to locate stolen vehicles before reporting the theft to the police. Several operators described using this feature to identify RAC employees stealing vehicles.

Some RAC operators use telematic devices to serve a similar function. The device is plugged into the vehicle and uses the same technology as in a smartphone to upload information to the cloud about the vehicle's location and maintenance requirements. The devices are inexpensive, but criminals and observant renters can easily identify and remove the device.

One airport LEO described a new trend of criminals using tracking devices to steal vehicles from RAC facilities. The criminal places a small battery-powered tracking device (e.g., Apple AirTag, Life360 Tile, or Samsung Smart Tag) inside an unlocked rental vehicle or on the outside of the vehicle. The devices use a "crowd GPS" network to notify the device owner when other smartphones detect the device's location. The vehicle is legitimately rented and driven off the property. The criminal then uses the device's location to find and steal the vehicle when it is in a less secure area.

This activity is an issue for several reasons. Notably, the devices are difficult to find if you do not know where they are located. Only iPhone users can receive alerts about an AirTag tracking them. Tapping on the notification will trigger the device to chirp until it is found. Android users must download an application for this functionality and conduct a manual scan. The LEO who described this activity reported that airport police performed tests to determine if the applications would work, but they were not successful in finding the test AirTags.

Apple responded to the increased use of its devices for illegal purposes by lowering the maximum amount of time the device can be away from its owner before chirping from three days to 24 hours (shorter times can be set by user). Each device has a serial number and must be registered with an Apple ID; law enforcement can work with Apple to identify the user based on the serial number.

6.3 Access Control

Access controls throughout the RAC facility can range from a simple lock and key system to access cards. Administrative offices behind the RAC counters often use key and cipher locks; airport operations, security, or police usually have the access code, a copy of the key, or access to a key. Padlocks and cipher locks are often used at the QTAs and RAC employee access gates.

> One airport operator reported that the lock on the rolling vehicle gate was being upgraded from a cipher lock to a card swipe system when they discovered that the default access code on the cipher lock had never been changed. The airport operator recommends that airports observe the RAC site manager or third-party facility manager change the lock code during every security walk-through. RAC operators should also be encouraged to change the code on a frequent basis as a mitigation measure associated with high employee turnover rates.

Access control is typically managed by RAC operators who issue access cards, assign keys, or provide cipher codes to their own employees. The third-party facilities manager may be responsible for these activities at consolidated facilities with shared access mechanisms.

Proximity or magnetic swipe cards are used at some RAC facilities to allow the vehicle shuttler to exit access-controlled Return Areas or the QTA. In most instances, the cards are assigned and issued to individuals but do not display the employee's identification; the high turnover of the RAC employees would make that cost prohibitive for the operator. When the individual is no longer employed, the cards should be recovered, if possible, and reprogrammed for a new employee.

If the card cannot be recovered, RAC operator policy is to deactivate it. However, airport security concerns over poor RAC operator badge control have been proven at some locations, and some operators inconsistently notify the third-party facility manager of employees who have separated from the company. Depending on the access authority granted to the cards, this and can leave RAC facilities and QTAs vulnerable to unlawful activity.

Some systems used by RAC operators use access control cards that have no tracking or audit capabilities. RAC employees are given a random card at the beginning of their shift and are expected to return the card at the end of their shift. These systems can be risky to use because there is no method to audit the card's activity or deactivate the access authority without reprogramming the physical card. If the card is not recovered from the employee, the card cannot be deactivated without resetting the system.

Not connecting the individual to the issued card makes it challenging to confirm if the individuals are using their assigned card, and there is no way to track which employee used what card on the day of an incident. RAC operators should be encouraged to use a system with auditing capabilities. If this is not possible, the site managers should, at a minimum, track and log the employee and their assigned access card every night to ensure the cards are returned. Ideally, the access cards would be unique ID media that displays the assigned employee's face, name, and employer.

Fuel cards with a code can be used to allow certain RAC employees to access the QTA and pump fuel (Figure 6-4). The cards are issued by the RAC operators or third-party facility manager after the employee completes the required fuel safety training. A benefit to fuel cards is the ability to audit which employees accessed the QTA and when, as well as track the employee's fuel usage. When the

Figure 6-4. Example of a Fuel Pump with Access Control

employee no longer works for the RAC operator, the card is recovered or access is terminated. Recovered cards can be wiped of identification information and reprogrammed for a different employee.

Correctly assigning access privileges is essential. Access control cards should only be issued to RAC employees based on their role or responsibility. For instance, QTA and fuel station access may only be available to QTA employees, or RAC site managers may be the only employees with authority to open vehicle access gates. This helps the RAC operator save money on cards and the process to issue, audit, and reprogram them. It also limits a RAC employee's opportunity to misuse a card's access authority.

6.4 Biometrics

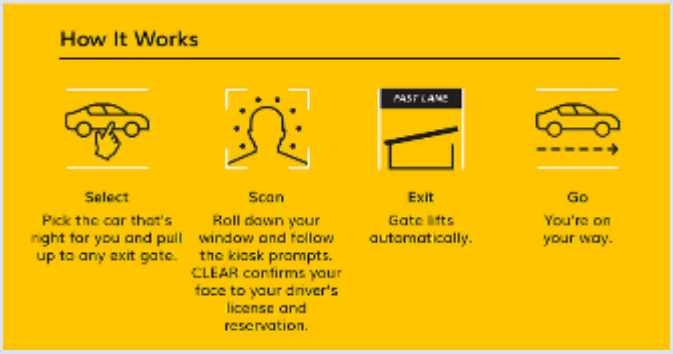
Some airport operators have suggested using biometrics during the rental contract process. As part of the customer vetting process, the RAC operator would capture an image of the customer's thumbprint. The prints cannot be run through any law enforcement databases (RAC employees would not have the authority to access them), but could be compared to customer databases. As an added benefit, if an investigation needs to be opened on that contract, law enforcement will have the suspect's thumbprint.

Implementation of any form of biometric ID verification for RAC customers would be the responsibility of RAC operators. It would require management of the customer database and associated biometrics at high levels of protection. RAC operators would also need to implement new policies for their customers in order to use their data for verification purposes.

While biometrics are not currently being used for vehicle rental agreements, there was a pilot biometric program that used facial scans to verify customers' identity, described below:

In 2018, Hertz Corporation and CLEAR partnered to create the Fast Lane Program for their customers. Hertz Gold Plus Rewards members with CLEAR could link their accounts so that their biometric data could be used to rent a vehicle without talking to an employee.

Figure 6-5. Fast Lane Infographic



Source: Hertz/CLEAR

As shown in Hertz's infographic (Figure 6-5), the customer selected their chosen vehicle, which had the keys inside, and drove up to the Fast Lane. The customer looked into the camera for a facial scan, which was compared to CLEAR biometric data for verification. If the customer had a valid renter's agreement, the barrier arm opened, and the customer could exit the facility.

The program was created to speed up the exit process, which can take an average of two minutes. The Fast Lane scan boasted that it could reduce that time to 30 seconds. Hartsfield–Jackson Atlanta International Airport, Los Angeles International Airport, and several other airports piloted the program in 2019.

The program was expanded to 40 airport rental locations within six months, but was it discontinued in 2020 for unpublished reasons.

It should be noted that Hertz would not have had access to CLEAR's biometric database; all biometric data would have been collected and secured by CLEAR. The system required pre-enrollment in the CLEAR database, which verified the identity of the customer relative to the identity of the person presenting themselves at the ticket booth.

Use of biometrics as a form of access control in RAC facilities was not reported during the research. This is likely due to the cost of equipment and administrative costs of programming biometrics for a worker population with high turnover. However, use of biometrics could potentially offer a significant boost to the security of the RAC facility by clearly tying an individual to an attempt to access a controlled portal.

6.5 Duress Buttons and Two-Way Communication Devices

Duress buttons and two-way communication systems in large, open areas allow a customer to quickly alert airport security to an emergency. The two functions are often tied together in a single device so that pushing the duress button activates two-way communication with airport dispatch. The devices provide deterrence to potential criminals and increase RAC customers' sense of safety. Additionally, they provide the exact location of the emergency for response personnel.

Figure 6-6. Example of a Duress Button

Duress or panic buttons are often placed throughout an airport's parking areas, including RAC facilities and ready/return areas. Buttons can be mounted on a pole, support column, freestanding pedestal, or inside the exit security booth. Some duress buttons activate a strobing blue light to deter an attacker (Figure 6-6). Most include an intercom system that connects directly to airport dispatch or a 9-1-1 center. Buttons in exit booths are often silent alarms that alert airport dispatch or 9-1-1 centers of an issue.

Some systems are capable of also activating a camera or adjusting a PTZ camera to focus on the area around the button. This feature aids investigations and can also allow airport security to quickly determine if there is an actual emergency or a false alarm. A good practice is to always have a camera covering the area around the duress button, even if it remains in sleep mode until activated.

6.6 Fraud and Counterfeit Verification Equipment

RAC operators view fraud and counterfeit activity quite seriously and offer in-depth training to their counter employees. Most operators will also furnish fraud and counterfeit detection equipment for each of their agent workstations. Some smaller operations and franchise locations may not have this equipment, but they should be encouraged to procure it. Airports can supply this equipment to the operator, but this is not a common practice.

During an interview at one airport, the airport's Chief of Police revealed that, several years ago, he told the RAC operators that the police department would not file reports of fraud or counterfeit until the operators deployed the appropriate equipment. The RAC operators quickly procured the equipment and reports were greatly reduced.

The ASM was present for the interview, and this was the first time he had heard of this situation. He immediately requested that the contracting office require fraud and counterfeit equipment be included in future RAC leasing contracts.

6.6.1 ID Verification Scanner

Most RAC operators use an ID verification scanner that captures images of the ID and verifies its authenticity by comparing the image and security features to online identity verification databases. The scanners are capable of scanning and verifying driver's licenses, ID cards, passports, visas, and many other documents from around the world.

The scanner takes an image of both sides of the ID and displays a red or green light to indicate authenticity. The scanner eliminates the need for manual inspections and reduces errors and customer delays.

When tied to the RAC operator's customer database, the scanners are also capable of automatically filling out rental forms using the information on the document, linking the customer to loyalty accounts and past rentals, and ensuring compliance with age requirements.

6.6.2 Point-of-Sale Terminals

Europay, Mastercard, and Visa (EMV) developed the microprocessor chip used in many debit and credit cards today. Cards with the EMV chip authenticate each transaction with a one-time-use code. The traditional magnetic stripe on the back of payment cards uses the same code each time, which makes it possible to duplicate.

A point-of-sale (POS) terminal is a device used to accept customer card payments. These terminals are required to comply with multiple industry standards set by international payment networks. Only EMV-ready terminals are capable of properly processing EMV transactions; fraudsters have an easier time scamming businesses that do not use EMV terminals. Fraudsters and scammers target businesses using older technology and equipment. Airport operators should encourage RAC operators to use EMV-ready terminals to help prevent use of counterfeit forms of payment.

Some devices are susceptible to criminals attaching card skimmers (Figure 6-7), which are devices designed to look like the POS terminal that are placed over the terminal to capture magnetic swipe data and personal identification numbers (PIN). USB keyloggers (Figure 6-8) look like a standard USB storage device but capture every keystroke of a computer's keyboard. Airport operators should remind RAC employees, particularly counter agents, to look for these devices to prevent security breaches.

Figure 6-7. Example of a Card Skimmer

Figure 6-8. Example of a Keylogger

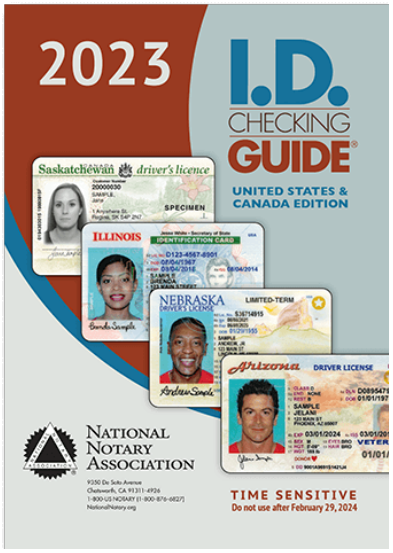
One RAC corporate security manager indicated that the corporate cybersecurity team sends out daily reminders to site managers to check for card skimmers and keyloggers.

6.6.3 Low-Tech Solutions

Ultraviolet (UV) light is a simple solution to help detect counterfeit money, credit cards, and driver's licenses by activating light-reactive security features such as watermarks and holograms. UV light is best used when paired with an online identity verification database or ID checking book to verify the markings are correct. Like any manual process, there is a high chance of error, but this will provide a small measure of security for little cost.

Airport operators can support RAC operators in identifying fraud and counterfeit documents by providing ID checking guides (Figure 6-9). These books can be used to compare an ID against hundreds of examples to determine if the ID is valid, altered, or counterfeit. The US version of these documents show every valid US, and usually Canadian, driver's license format. The documents also include details on more common immigration visas, federal and military IDs, and other forms of ID. The manual nature of using the ID guide could result in service delays and errors, but it can still be useful when no automated option is available.

Figure 6-9. Example of an ID Checking Guide



There are also online identity verification databases that provide access to thousands of ID and driver's license reference images and security features. Holograms, color shifting inks, and microprint can be confirmed on the presented ID using a UV light, magnifier, or ID scanner. The databases also include references to federal immigration documents, visas, military documents, and more. These services require an annual subscription, but they have the benefit of being continually updated.

If the RAC operator is not using an ID verification scanner, they could still scan IDs with a photocopier to maintain a copy of the ID should a report need to be filed against the customer.

One airport LEO reported that Sixt takes color photos of every ID document as well as a photo of the renter to add to the rental transaction. This has been beneficial to the LEOs when they need to open an investigation.

Some RAC operators are required by the state to accept cash transactions despite the potential for counterfeit activity. Bill validators are widely used across all industries and would help RAC employees identify counterfeit bills. The devices compare the presented bill's security features with the expected security features to determine the bill's authenticity. The US Currency Education Program provides training materials and courses on the security and design features in Federal Reserve notes. The free resources could be used for additional RAC employee training.[6]

[6] USCurrency.gov. U.S. Currency Education Program: Training Resources. www.uscurrency.gov/training-resources

6.7 Inventory Tracking

Some RAC operators use their cameras for inventory tracking rather than security purposes. This often means the camera viewing angles capture license plates but not necessarily faces. Airport operators should work with the RAC operator to educate them on the value of quality cameras strategically placed in locations that support both day-to-day operations and mitigate security concerns.

Additionally, airport operators should highly recommend that RAC operators who are not currently using cameras or mobile devices to begin tracking their vehicle inventory. One of the more common reports to airport police is for a vehicle missing from the RAC facility. Proper inventory control helps the RAC operator identify when the vehicle was last marked as being in the facility.

> One airport LEO reported that a RAC operator once did not realize a vehicle had been missing from the garage for weeks because they had not performed adequate inventory control.

Daily or twice-daily inventories ensure that the vehicle will not be missing for more than 24 hours, which will improve the chances of recovering it. However, this may be impractical for RAC operators with large fleets.

> Another airport LEO described an event where a vehicle was stolen from an unsecured storage lot behind the consolidated RAC facility (the keys had been left in the vehicle). The vehicle was used in several crimes before being returned to the lot. No one noticed the vehicle had been missing until several days later when a vehicle shuttler picked up the vehicle and noticed several bullet holes in the door.

Handheld scanners are commonly used to automate inventory tracking. These devices enable the user to scan license plates or VINs to be logged in a digital database. If used regularly and correctly, the system should be able to alert RAC employees to missing vehicles.

6.8 RAC Mobile Applications

Most RAC operator brands utilize mobile applications to push notifications to their customers and enable preferred members to bypass certain check-in processes. Some RAC operators allow eligible customers to bypass the contract review at the RAC facility exit by scanning a barcode or quick response (QR) code at a reader stationed at the exit lane (Figure 6-10). This completely contactless service allows the customer to complete the rental vehicle pick-up and exit process without interacting with another person.

Many RAC operators view this as a highly desirable service to offer their preferred members, but it also creates a significant vulnerability that can be exploited by criminals. The program relies on the fact that the member has successfully rented from the RAC operator multiple times in the past and is considered trustworthy. However, the database storing the user information can be—and has been—compromised. Information leaks like this result in many fraud cases across the country.

Figure 6-10. Preferred Member Code Reader

One airport operator described an incident where a RAC employee shared a preferred member's account code with criminal friends. The criminals used the RAC operator's mobile application to create a user account and upload a different driver's license. The application generated a barcode that was scanned at the preferred member exit without booth attendant interaction. In all, 20 vehicles were stolen with the barcode before the main suspect was caught.

RAC operators currently only utilize this service at a few airport locations, but continued success could result in increased deployment locations. Airports with RAC operators that are currently using mobile applications to bypass verification processes will likely find it difficult to discourage the practice. If the RAC operator is considering adding this service, airport operators may have the opportunity to negotiate or compromise with additional security measures to help close vulnerabilities. Potential measures may include:

- Cameras mounted at driver height at the exit lane that capture images of every driver exiting the RAC facility. If there is a preferred member exit lane, mounting the camera near the code reader may be the only clear shot of the driver throughout the entire renting process.
- Exit booth attendant scans the code. Most RAC operators utilizing a code reader at the exit lane also utilize a back-up mobile device for times when the stationary code reader is non-functional. While the interaction would be minimal, the brief time the exit booth attendant spends with the driver could alert them to red-flag behaviors.

6.9 RAC Self-Service Kiosks

Some RAC operators have deployed self-service kiosks (Figure 6-11) at select airport locations to lower the customer's average transaction time. The kiosks allow experienced customers to quickly retrieve their online rental contract or rent a vehicle on the spot without needing to speak to a RAC employee.

Figure 6-11. Examples of Rental Kiosks

These machines require the customer to scan a form of ID (driver's license, passport, etc.), which verifies that the ID has the expected security markers. Unfortunately, good counterfeit IDs are able to

fool the ID scanners that are typically installed in these machines, and criminals are able to use a stolen credit card with a fake ID that matches the cardholder's name to rent a vehicle. Criminals favor these machines because they can easily evade having to interact with a trained employee who is knowledgeable of risk indicators, suspicious behaviors, and fraudulent IDs and credit cards.

Many RAC operators recognize that the self-service kiosks are a security vulnerability and have reduced their usage or discontinued them entirely. Airport operators should encourage RAC operators to discontinue their use.

SECTION 7: VISIBLE DETERRENCE

Visible security is one of the most effective forms of criminal deterrence. Criminals are more hesitant to attempt to commit a crime if they think they are being monitored, the target is hardened, and they have a high probability of being caught.

Airport police patrols are the most common form of visible security at the RAC facility, but airport security personnel also deploy parked marked vehicles and occasionally utilize contract security.

7.1 Exit Booth Attendants

Many RAC ready/return facilities have security booths stationed at the exits. The exit booth attendant is responsible for verifying that the driver has a valid rental agreement and that the vehicle they are driving matches the agreement. Once verified, the booth attendant can open the vehicle barriers to allow the customer to exit.

This position is always staffed by the RAC operator and is often a RAC employee with no specialized security training. Occasionally, RAC operators may staff this position with contract security personnel.

Booth attendants serve a valuable role in preventing vehicle theft through the exit lane. However, they are also in a position to allow vehicle theft. For this reason, conducting background checks on the booth attendants can significantly enhance security of RAC facilities.

7.2 Airport Security and Police Patrols

Patrols are effective forms of visible security in RAC facilities. Most patrols at RAC facilities are performed by airport police either on foot, bicycle, electric standup vehicle (ESV; Figure 7-1), or in a vehicle, depending on the airport and the assignment. Many airport operators augment their police patrol force with non-sworn individuals, such as airport security/operations personnel.

Figure 7-1. Example of a Patrol ESV

Patrols inside the facility allow the LEOs or security personnel to speak directly to the RAC employees, answer questions, and discuss security policies with employees. This creates a trusting relationship between airport security and the RAC employees.

Patrol of RAC facilities is sometimes an assigned post, but more often is part of a patrol route. When the RAC facility is adjacent or connected to the airport terminal, patrols assigned to the baggage claim hall or check-in lobby are often tasked with patrolling the RAC customer lobby as well. These patrols would also be the first to respond to a call for service. RAC operations in the baggage claim hall benefit from the airport security already in the public area. Increasing the frequency of patrols around the RAC customer counters will greatly improve visible security and crime deterrence, as well as decrease response time to fraudulent transactions in process or suspicious activities.

Additional security patrols are often deployed during periods of high traffic and high crime trends, such as holidays, after local bars close for the night, and during extreme temperatures and weather that may attract trespassers to shelter in the facilities or vehicles.

For RAC facilities that have closed hours, assigning an LEO or airport security personnel to perform a sweep of the facilities after the last flight of the night can help ensure no one is loitering, sleeping, or hiding.

Some airport operators position a police vehicle near the front of the consolidated RAC facility entrance with the lights flashing to indicate a police presence that can quickly respond to calls for service and crimes in progress. Doing this several times per shift could deter potential criminals seeking an easy target.

Airport operators that have experienced an increase in criminal activity at the RAC facility may deploy plain clothes officers or perform surveillance/stakeouts to identify individuals who are committing crimes and the method. These types of surveillance activities have uncovered a number of organized crime rings involving RAC facilities across the country.

Mobile surveillance towers (Figure 7-2) are often positioned to monitor neighboring parking lots but can also be used to monitor activity at the RAC facility.

Figure 7-2. Example of a Mobile Surveillance Tower

7.3 Contract Security

Many airport operators utilize contract security guards to augment the airport security force. The guards may be stationed anywhere to support situational awareness and visible deterrence, but they are most often assigned to RAC counters in the baggage claim hall and the terminal curbs adjacent to consolidated RAC facilities.

Use of contract security to patrol and monitor RAC facilities, especially overnight, greatly improves visible deterrence. Additionally, these personnel can assist customers who inadvertently enter the RAC facility secure areas and become trapped behind the barriers, allowing the airport police to focus resources at higher priority locations.

> One airport experienced an increased number of people experiencing homelessness riding the airport people mover, which has a stop at the consolidated RAC facility. The ASM requested two new contract security assignments based on the increase in customer complaints: one to patrol the people mover and one to patrol the RAC facility.

Contract security service providers generally perform background checks on their security guards. Training is often in-depth and can be verified with training logs and certifications. While they have no arrest authority, contract security patrols can offer a visible deterrence to potential criminals.

RAC operators occasionally hire contract security, but it is not common. In addition to patrols, contract security guards can staff the exit booth and shuttle vehicle between facilities. These positions offer the most opportunity to commit vehicle theft and should be staffed with personnel who have had background checks performed on them. Since most security service providers conduct background checks and provide training to their guards, RAC operators can have greater confidence in the security

of the RAC facilities. Additionally, security guards have a much lower turnover rate than the vehicle shuttlers and RAC employees, and they can be quickly replaced with another qualified individual from the service provider.

RAC operators prefer to hire off-duty LEOs for patrol purposes as they have arrest authority that contract security officers do not. Most airport police departments interviewed for this research offer RAC operators the opportunity to hire off-duty officers. Airport police could offer RAC operators the opportunity to hire off-duty LEOs to perform certain security functions, as applicable in the specific jurisdiction and if there is available budget for this service.

Airport operators should work with contracted security guards, regardless of the contract owner, to coordinate surveillance activities and response to some incidents. This may help eliminate the need for LEO response to certain calls for service at RAC facilities.

7.4 Metrics

Metrics are key to determining the most effective strategy to deploy security personnel at RAC facilities. Investigators or crime analysts are responsible for developing regular crime analysis reports. Most reports are generated at least monthly, but some airport police generate the reports weekly or quarterly.

The reports can identify trends in criminal activity in certain locations (e.g., through a specific exit lane) or at certain times of the day (often overnight). These reports are used during airport operator and RAC executive meetings to justify budgets for security projects, implement new policies, or deploy security personnel to specific assignments. There are several metrics that airport police typically use to identify security trends:

- Time and day incident occurred
- Type of vehicle
- RAC operator affected and location, e.g., exit lane, counter, or kiosk
- Type of report
  - Failure to return, also known as vehicle conversion or theft by bailee
  - Fraud, swindle, and counterfeit
  - Theft by driving out of the facility
  - Missing from inventory

Some airport operators have additional metrics to help account for specific security threats occurring at their airport. Recording additional details can help the airport operator data map and connect security incidents. Skilled and experienced analysts will be able to identify data correlated with a circumstance that is not related to any security process.

> One airport operator added a metric to track the number of vehicles stolen using RAC Transfer Tickets. These tickets are used by vehicle shuttlers to check cars in and out of the ready/return area and QTA. One of the books containing these tickets had been stolen and the criminals used the tickets to steal multiple vehicles.
>
> The same airport operator also added the number of vehicles stolen using a Hertz Gold Member Account. In 2016, Hertz had a major data breach that leaked thousands of Gold Members' account numbers. Criminals stole the Gold Members' identities and used them to fraudulently steal several vehicles across the country.
>
> These metrics allowed the airport operator to connect multiple thefts and attempted thefts.

Airport police have found many benefits to staffing a full-time civilian crime analyst. The primary benefit of this role is that the analyst is responsible for proactively identifying and analyzing crime trends, which removes this task from department investigators and enables them to prioritize their investigative and criminal apprehension work.

SECTION 8: DESIGN CONSIDERATIONS

RAC facilities built with a focus on security increase RAC customers' perceived level of safety and security as they transit between the terminal, RAC lobby, and ready/return area. Crime Prevention Through Environmental Design (CPTED) is a planning methodology that includes passive design features that helps to foster both the perception and reality of a more secure environment.

The primary goal of CPTED application is to influence desirable behaviors and discourage undesirable behaviors, including criminal activity. This can be done through several strategies including physical security measures, improved lighting, natural access control through landscaping, and consistent maintenance of the facility.

8.1 Location

Choosing the location of a new RAC facility is an impactful decision on RAC and airport security operations. There are typically four location options for on-airport RAC operations. Each option has benefits and challenges to the security of the airport and the RAC facility.

Baggage claim hall: RAC customer service counters are located in the baggage claim hall or other terminal area (Figure 8-1). RAC ready/return areas and QTAs may be on-airport or may require a shuttle bus to an offsite location.

Benefits

- Consolidation of patrols
- Airport control over technology (cameras, access control) in the baggage claim area
- Faster response to calls for service

Challenges

- Congestion in the baggage claim is a vulnerability and creates a target
- Incidents at the counters may impact other airport operations and activities
- Proximity to restricted areas may create a target
- RAC employees may require a public area badge to work in the terminal (*this can be costly for some airports and a benefit for others*)

Attached to the terminal: The RAC lobby and counters are located in a separate area that is attached to the main terminal via a hallway or set of doors. RAC ready/return areas and QTAs may be located in an adjacent area and are often consolidated.

Benefits

- Consolidation of patrols
- Faster response to calls for service
- Vehicle stock within close proximity for patrols
- Standoff distance from the passenger areas

Challenges

- Proximity to the restricted areas may create a target
- Potential for additional technology requirements

Adjacent to the terminal: RAC operations occur in a building across from the terminal, typically accessed by crossing the airport curbside roadway. These are almost always consolidated facilities.

Benefits

- Standoff distance from the passenger areas
- Faster response to calls for service

Challenges

- May require additional or extended patrols
- Additional technology requirements
- Potential vehicle congestion along the curbside
- Increase in pedestrians crossing the road

On airport campus: RAC operations occur some distance from the airport terminal, usually requiring a shuttle bus or people mover to transfer customers. These may be flat lots scattered around the airport campus or a consolidated facility.

Benefits

- Standoff distance from the passenger areas
- Minimal impact on operations and activities at terminal
- Reduced activity in front of the terminal (*unless shuttle buses are not consolidated*)

Challenges

- Slower response to calls for service
- May require additional or extended patrols
- Additional technology requirements

In some cases, RAC facilities are spread out across several of these locations. RAC counters may be located in the baggage claim with a consolidated flat lot adjacent to the terminal and individual QTAs spread across the airport campus. Most airports will have limited options for locating the RAC facilities. However, if the airport operator can choose between several locations, carefully weighing the security benefits and challenges of each available location will help the airport operator make the best choice for their security needs and prepare mitigation strategies to combat the challenges.

Figure 8-1. RAC Counters at the Baggage Claim Hall

8.1.1 Proximity to Other Facilities

The distance of RAC facilities from the airport terminal and restricted areas may be the most critical choice for airport operators. This will impact vehicle and pedestrian traffic flow around the airport as pedestrians cross traffic lanes to access the facility, shuttle buses pick up and drop off customers, and rental vehicles enter and exit the facilities. RAC facilities built adjacent to the terminal are usually

accessible on the ground level via crosswalks but may also be connected via a sky bridge or underground tunnel.

> One airport operator had extremely limited space to locate the RAC facility near the main airport terminal. The only viable space straddled the AOA perimeter fencing of the neighboring general aviation apron. Instead of moving the fence line or demolishing a building to make space, the airport built a wall between the RAC ready/return area and the AOA to maintain security.

Airport facilities near the selected location may impact the security of the RAC facility. Many RAC facilities are located next to or inside the airport's parking lots/garages and share space with other RAC operations. While driving at the airport, it is common for customers to mistakenly enter a RAC facility when they meant to enter the adjacent parking lot, or for RAC customers to mistakenly enter the parking lot. This proximity to public areas also allows criminals to easily surveil the RAC facilities or enter on foot.

> One airport LEO discussed the challenges at their consolidated RAC facility due to its proximity to a city bus stop. The RAC facility is located near the outer perimeter of the airport property and a city bus stop is within sight of the RAC facility. This bus stop is also the last stop on the route, and everyone is asked to exit the bus. The airport has ongoing incidents of people trespassing in the RAC facility as a result.

Proximity to airport facilities can also be leveraged to enhance the security of RAC facilities. Cameras deployed on nearby buildings and roadways can be dual purposed to monitor the perimeter of RAC facilities. Staff of neighboring facilities can also monitor the activities in the RAC facility and act as a visible deterrence to criminals.

> Two airport operators indicated that the airport police had a substation close to the RAC operations; one was located across from the counters in the baggage claim hall and one was in a building next to the consolidated RAC facility. These airport operators indicated a high degree of cooperation with the RAC employees. The RAC facility built near the substation had very few crimes at the facility, especially for the RAC operator assigned to the position closest to the substation.

A location study should also consider future terminal expansion and whether the new building will limit expansion options.

> One airport is planning to build a new terminal in 10–15 years, and when building the consolidated RAC facility, the airport operator chose its location based in part on its proximity to the future terminal. The RAC facility will connect to the new terminal via a sky bridge.

8.1.2 Geographic Features

The physical geography of the chosen location can create certain security challenges. Steep grades and mountainous areas need extra care as the slope of the landscape can create areas for criminals to jump or climb over perimeter fencing or other barriers. Efforts should be made to minimize the vulnerabilities of these areas. Some airport operators install fencing to reduce a criminal's ability to access the area. Hostile landscaping such as thorny bushes can also be used to reduce access and align with CPTED strategies.

One airport built their RAC facility partially into the side of a tall hill, which enclosed the far side of the first two levels. This offered a natural barrier on that side, but also created potential access to the third level. To mitigate this problem, the airport installed a partial brick barrier along the portion of the third level where unauthorized persons could access the RAC facility.

Airports in naturally rainy and flood-prone areas often have drainage swales along the roadway to channel rain and flood waters away from the roads and buildings (Figure 8-2). These are necessary to manage the water, but also serve as natural boundaries that are difficult to cross, especially when they are wet and muddy.

Figure 8-2. Example of a Drainage Swale Along a Parking Lot

8.1.3 Jurisdictional Considerations

Some airport operators may encounter jurisdictional challenges when deciding on the best location for RAC facilities. Several airports straddle two cities or counties and must abide by the governance and rules of those cities or counties, as well as the airport's governing body.

One airport LEO indicated that the RAC facility was purposefully built on one side of the county line as part of a market-share agreement between the counties; revenue from the RAC operations would be included in that county's budget.

Another airport's consolidated RAC facility is located in a different city than the airport, but the airport police are responsible for the security of the facility.

While these jurisdictional challenges have not caused problems for the airport police in the above examples, locating the RAC facility in a different police jurisdiction has the potential to cause challenges when investigating and prosecuting criminal activity.

8.2 Layout

Layout and design of the RAC facilities is highly dependent on the available space and volume of RAC operations. Facility design should accommodate natural surveillance to improve situational awareness and sense of safety. This involves creating unobstructed sightlines from one end of the facility to the other by limiting the number of interior ramps, walls, closely spaced columns, and other structures. Glass-enclosed elevators and open-air stairways also improve sightlines and limit a person's ability to conceal themselves.

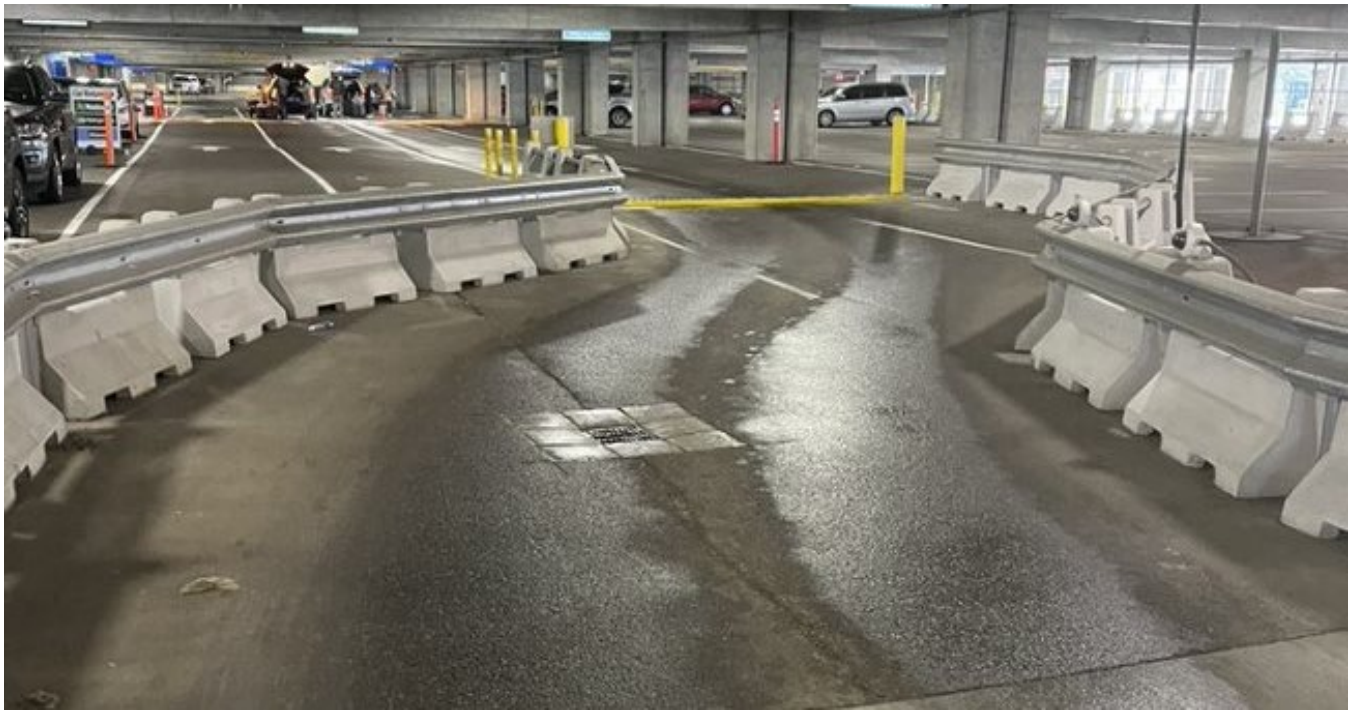
It is a good practice for airport operators to engage the RAC operators in the design of a new airport-owned facility. Design elements and features that may cause security vulnerabilities are often discovered after construction. Airport operators should consult with their RAC operators' corporate planners in the concept and design phases to identify any potential security concerns and learn from their experiences at other airports. The RAC planning managers have knowledge and experience that can be highly valuable at this stage.

8.2.1 Separating RAC Operators

Typically, RAC operators sharing a facility are leased space that includes customer counters, ready/return areas, vehicle storage lots, and vehicle lanes. In some cases, the RAC operators have their own level in the facility with a common lane to transition between levels.

RAC operators are generally responsible for installing and maintaining the physical and technological security features within their exclusive-use space. This arrangement can create varying levels of security throughout the facility. Separating the RAC operators using concrete barriers, fencing, or other barrier types (Figure 8-3) can prevent vehicle thieves from exploiting more vulnerable areas in another RAC operator's space.

Figure 8-3. Concrete Barriers Delineating RAC Operators



8.2.2 Consolidating Vehicle and Pedestrian Access Points

Providing a dedicated exit lane for each RAC brand allows the RAC operators to manage the security of their own exit. Most consolidated RAC facilities have multiple exits. However, multiple exits also provide multiple points of potential failure that a criminal can exploit, especially when they have varying levels of security.

Consolidating the exit area into fewer lanes with a single, shared exit location would reduce the number of potential points of failure and combine security technology and resources at a single exit. Contracts and consortiums may be required to implement a consolidated exit. However, a consolidated exit may be

difficult for some airport operators due to the variety of exit procedures for each RAC operator. Additionally, damaged or inoperable security barriers at the exit may render it unusable, potentially stalling service or forcing operators to use a non-secure alternative exit.

This concept is also true for pedestrian access points. Regardless of location, layout, or operations, RAC facilities are always in the public area and often open on multiple sides. This leaves the facilities highly vulnerable to unauthorized individuals entering on foot unless these access points are closed or access controlled. Limiting the number of pedestrian entrances and exits into the RAC facilities will funnel pedestrians into authorized areas and enable personnel to quickly identify when individuals have ventured into unauthorized areas. This can be done by building barriers such as fencing or walls, or by using hostile landscaping to discourage movement in certain areas.

8.2.3 Multilevel Facilities

It is common for consolidated RAC facilities to be multilevel structures to create a smaller footprint. Some consolidated RAC facilities only have two or three levels with one dedicated to vehicle storage and one or two dedicated to RAC operations such as the ready/return areas. Vehicle storage levels are typically intended to be inaccessible to customers and are often located on the upper level.

Multilevel facilities offer many benefits to the airport, such as consolidating security services, infrastructure, and resources while limiting access to the upper and underground levels.

> One airport built their RAC facility partially underground, which protects the lower level from casual observation.

Multiple levels can also create safety and security concerns. Stairs, elevators, and escalators are necessary to travel between the levels, but the vertical cores can also create concealed areas for people to hide. Open spaces underneath the stairs are often used for this purpose.

Figure 8-4. Open Sightlines in Stairwell to Reduce Concealment

There are a few design strategies to combat this challenge. Creating vertical cores with open sightlines will help prevent anyone from attempting to conceal themselves (Figure 8-4). This can be done using glass barriers or railings instead of solid walls. Conversely, blocking off potential hiding spaces with a wall, barrier, or fence can prevent access to these areas. These measures are best reviewed and included during the planning and design phases of construction, but some measures can be added later. Patrol officers should be directed to check the vertical cores during their patrols.

Stairs and escalators can be a safety hazard for passengers carrying luggage between levels; incidents of customers falling or tripping are common. Cameras in the vertical core can help the airport operator effectively conduct investigations and avoid liability claims by showing the incident was not caused by improper maintenance, negligence, or a defect. The cameras can also be used for security monitoring within the vertical core and the surrounding area.

8.2.4 Vehicle Return Locations

Vehicle drop-offs are typically limited to the RAC return area. The customer can either leave the keys in the vehicle or drop them in a drop box. The vehicle shuttler then takes the vehicle to the QTA for cleaning and refueling.

Pick-up procedures should be developed for any secondary drop-off location at the airport. One solution is to require RAC site managers or authorized shuttlers to present identification to retrieve keys from airport personnel or police. A locked drop box could also be utilized.

> One airport has a small fixed-base operator (FBO) that shares a runway with the airport. RAC customers catching flights at the FBO can leave the vehicle in the FBO parking lot and give the keys to an FBO employee. It usually takes some time for the vehicle shuttlers to retrieve the vehicles from this remote location—sometimes days if the FBO does not contact the RAC operator right away. The RAC vehicle shuttlers at this airport are not issued company identification and, until recently, were not required to show proof of identification to retrieve the keys.
>
> A group of criminals posing as vehicle shuttlers by wearing a similar reflective vest, retrieved the keys from the FBO employee and stole several vehicles from the FBO parking lot. This scheme was not uncovered until the actual RAC vehicle shuttlers showed up later to collect the vehicles. After this incident, the airport police worked with the RAC site managers and the FBO managers to develop a new procedure. Now, only RAC site managers can retrieve the vehicles returned at the FBO, and they must show their company-issued ID before the FBO employee will release the keys.

Occasionally, rental vehicles are left at the airport curbside with the keys left in the vehicle instead of returning to the appropriate area. The unattended vehicle in front of the terminal can cause security concerns and can also affect traffic congestion. Additionally, the vehicle is vulnerable to theft. When airport police respond, the customer is usually long gone and cannot be held immediately accountable. Security personnel assigned to the terminal roadways are trained to monitor unoccupied vehicles and have them ticketed and towed. The RAC operator will pass on any fines and towing fees to the customer.

8.2.5 Ground Transportation Centers

Airports are considering new strategies to consolidate services around the airport and most effectively use the available space. The future state of the consolidated RAC facility may appear more like the Cincinnati/Northern Kentucky International Airport (CVG) ground transportation center (GTC) (see Appendix A). The facility provides a central location for most of the airport's vehicle services, such as hotel shuttle buses, valet services, and RAC operations.

The centralized facility relieves vehicle traffic at the terminal curbside and makes it easy for the customers to find where they need to go for service. Additionally, the extra traffic movement and airport workers in the vicinity discourage criminal activity because of the increase in people observing and reporting suspicious activity.

8.3 Traffic Flows

The location of the existing roadways will be a major consideration for determining the best location for RAC facilities. Traffic entering and exiting the RAC facilities will impact the roadway traffic and can cause significant bottlenecks, traffic jams, and potentially vehicle collisions if not carefully designed.

RAC facility designers will look at the available footprint, existing traffic flow, and the space requirements for the RAC operators to determine the most appropriate traffic flow within the facilities and connecting to the roadways. This often requires modification to the existing roadways, but the facility designers will be able to account for this.

8.3.1 Pedestrian Traffic

According to the National Highway Traffic Safety Administration (NHTSA), 15% of pedestrians struck and killed by a vehicle in 2021 were in a marked intersection, highlighting the dangers of vehicular and pedestrian traffic flows inside and around the RAC facilities, especially where pedestrian traffic crosses vehicular traffic. [7]

Pedestrians crossing a roadway also increase the risk of a vehicular collision, especially when crossing multiple lanes of traffic. To improve vehicular traffic flow and pedestrian safety, pedestrian crosswalks need to be carefully placed, the area properly lit, and signage and crossing safety light controls installed.

Some airport operators may be able to erect a skybridge (Figure 8-5) or underground tunnel between the terminal and RAC facilities located adjacent to a terminal to remove pedestrian traffic from ground-level roadways. This alleviates traffic buildup caused by pedestrians stopping traffic to cross the street and lowers the number of stopped vehicles in front of the terminal. Security patrols can also use the skybridge or tunnel to access the RAC facility, avoiding the potential traffic hazard and allowing for faster response to calls for service.

Figure 8-5. Example of a Skybridge

Diverting pedestrian traffic away from vehicle traffic within the RAC facilities is also important. Many airports have experienced accidents or near accidents caused by inattentive vehicle shuttlers. This hazard can be reduced by limiting pedestrian traffic crossing vehicle lanes to designated crosswalks that are well lit and have clear sight lines to the vehicle lanes.

[7] **NHTSA:** https://www-fars.nhtsa.dot.gov/People/PeoplePedestrians.aspx

One strategy to separate pedestrians and vehicles is to add barriers, such as bollards, along the roadway with openings at the designated crosswalks. Pedestrians could jump over the barriers, but the struggle of also carrying their luggage over the barrier can make the crosswalks more convenient. Walls and fencing could also be used to prevent pedestrians from crossing as well as protect pedestrians on the walkway side from being struck by vehicles. However, walls and fences may be subject to fire code regulations.

Figure 8-6. Example of Walkway Between Vehicle Bumpers

Some RAC facilities are designed with pedestrian walkways between the bumpers of the parked vehicles (Figure 8-6). The walkway is delineated by concrete wheelstops or curbs to prevent vehicles from rolling into the crosswalk. Adding the walkway encourages customers to use the more protected path instead of walking in the vehicle lane. Placement of signage encouraging pedestrians to use these walkways may also reduce pedestrian movement though vehicle traffic areas.

8.3.2 Traffic Calming Measures

A common concern for airport operators is the vehicle shuttlers and rental drivers posing a threat to airport passengers and RAC customers walking in and around the facilities. Traffic calming design and devices can be utilized to force drivers to slow down and be more observant of their surroundings. The measures are meant to combat speeding and unsafe behaviors, especially in areas where vehicles and pedestrians cross. Additionally, strategically placed traffic calming measures can prevent vehicles from reaching the speed necessary to breach fences or barriers.

The vehicle lanes inside RAC facilities are often delineated using concrete, steel, or chain barriers that can be adjusted and moved to meet operational demand. Some RAC facilities have the ability to create tight curves and turns or serpentine lanes (Figure 8-7). Designing the vehicle lanes in this fashion forces the driver to slow down. Placing lane curves near exits will force vehicles to slow down and reduce their ability to gain ramming speed to breach the exit barrier.

Figure 8-7. Traffic Calming Curved Lanes

Speed bumps are low-cost devices used to force vehicles to slow down and discourage speeding. Permanent speed bumps are typically made from asphalt or concrete, but temporary speed bumps made from vulcanized rubber can be attached to the pavement for easier repositioning if needed. Speed bumps are not ideal for low clearance facilities, especially the

concrete and asphalt types, which are typically taller than the rubber versions. The added height could prevent emergency vehicles from accessing the facility.

Placement of speed bumps is key to effectively slowing down vehicles and protecting pedestrians. Ideal locations are around crosswalks, lane intersections, and corners. Temporary rubber speed bumps can be useful to test different locations and the impact to traffic and safety. Speed bumps should always be accompanied by signage to alert drivers and reduce the airport's liability.

8.3.3 Sally Port Exits

Sally port style exits use two sets of vehicle barriers to help control the direction a vehicle can exit the RAC facility. Typically, the customer will stop in front of the first barrier to have the contract verified. If the contract has been verified, the exit booth attendant will release the first barrier and the barrier leading to the exterior of the facility. If the contract cannot be verified, or there is another problem, the exit booth attendant will release the first barrier and the barrier leading back to the return area. This style of exit is highly effective at controlling vehicle access at the exit. The double barriers also prevent unauthorized vehicles from tailgating through the exit behind an authorized vehicle.

The double barriers offer redundancy; should one set need to be repaired, the other two can still help control traffic flow. Additionally, vehicle thieves will find it much more difficult to ram through two sets of barriers without immobilizing the vehicle.

8.3.4 Shuttle Buses

Buses are often required to transport customers to remote RAC facilities. When RAC operators are scattered across the airport campus, several buses are often required—at least one per RAC brand. These large vehicles can cause bottlenecks in traffic and block drivers' views around pedestrian crosswalks. At the terminal curb, this can be alleviated by separating shuttle and bus traffic from other vehicular and pedestrian traffic.

Many RAC facilities have designated entrances and exits for buses. Typically, the bus lane will have access control, such as an arm barrier activated by a vehicle tag, at the entrance and exit to prevent unauthorized vehicles from entering the lane.

Consolidating buses and creating a route that stops at each RAC operator around the airport can significantly reduce the required number of buses, which will alleviate traffic in front of the airport terminal and along the airport roadways. However, this may impact customer service by adding additional travel time.

8.3.5 People Movers

Airport trains and trams are becoming more common as airports expand to more remote locations on their campuses. These allow dozens of passengers to quickly cross the airport to reach various locations, such as consolidated RAC facilities. Typically, the RAC facility is one stop along the people mover's route.

Some city public bus systems have a stop at an on-airport GTC that includes a consolidated RAC facility. This creates a security risk as it allows individuals without business at the airport to loiter at the RAC facility. Airport operators could station a patrol officer on the train or at the stations to identify and interview anyone who does not appear to have business at the airport (e.g., no luggage or employee badge).

8.4 Physical Security Measures

Physical security measures such as traffic spikes, access doors, and vehicle access gates are used to prevent unauthorized pedestrian and vehicular traffic from entering or exiting certain areas of the RAC facilities. These types of measures should be deployed to discourage an attack and impede a threat from execution to allow for law enforcement response.

It is common for airport operators to pay for a consolidated RAC facility design to include the installation of physical security measures, such as barrier gate arms or plate barriers. This allows the airport operators to determine the minimum security standard of the facility upon which the RAC operators can add additional measures. These physical security measures are uniform across all operators, thus reducing vulnerable areas.

Sometimes the airport operator pays for the infrastructure needed to install physical security measures, such as power and in-ground detectors, but requires the RAC operator to furnish the equipment. If the RAC operators have formed a consortium, the consortium will often procure and deploy uniform security measures across the facility. If the RAC operators are furnishing the security measures for their individual spaces within a shared facility, the different levels of security may create areas of vulnerability that could allow for criminal activities.

When RAC operators are scattered around the airport campus, they typically pay for the construction of their own facilities and furnish all their own physical security measures.

8.4.1 Security Booths

Security booths are small structures, only large enough for one or two people, that are typically positioned at the RAC facility exit; they may also be stationed in or near the RAC facility or ready/return area to act as a customer service booth. The RAC operators staff the booths with employees or contract security who are responsible for verifying that the driver and vehicle are authorized to exit according to a rental agreement, customer identification, or employee ID.

The booth attendant can permit the vehicle to exit the facility by deactivating the security measures from inside the booth. Sometimes the booth also includes a duress button that can be activated to quickly alert airport security or police. The booths are typically secured with a standard lock and key.

The structures are often protected by concrete or steel bollards around the perimeter, and can also be constructed on a raised median to further protect the booth and attendant. While not common, ballistic glass in the booths would also offer protection to the booth attendants.

8.4.2 Key Management

RAC operators leave the keys in their vehicles at many locations for ease of business; this challenge is felt by nearly every airport with on-airport RAC services.

> In one instance, an airport operator reported that the practice of leaving keys in the car is commonplace and well known by criminals and persons experiencing homelessness. As a result, a $100,000 Cadillac Escalade was stolen from the RAC facility.

From the RAC operator's perspective, greater customer service and shorter transaction times are more important than the risk of auto theft. For this reason, airports often receive push back on removing the

keys from the vehicles. RAC operations at large airports, in particular, have a large, constantly changing fleet, which makes it difficult to effectively manage a high volume of keys.

Smaller operations and franchise locations may have an easier time managing vehicle keys due to the smaller fleet size. For smaller fleets, key cabinets, safes, and lockers may be options to help manage and organize the vehicle keys. These RAC operators also remove keys from vehicles when the RAC ready/return areas are unsecured.

Many airport operators have appealed to RAC operators for a change in key policies with no success. Some airports have explored the use of procedures and requirements in contract language to eliminate the keys left in vehicles, but this is not a viable option for most airports.

> One airport operator is considering mandating key control in their Airport Rules and Regulations or in their concession lease agreements, if they are able to be amended. This is an area where review is needed by experts from multiple departments responsible for these agreements, including security, legal, and airport business offices.

Compromise is essential to finding a solution. For example, some airport operators have worked with RAC operators to de-key vehicles before the last site manager leaves for the night. Stacking the vehicles in rows and removing the keys from the first and last vehicles is another potential option. However, thieves who are stealing a vehicle for parts may ram into the surrounding vehicles until they have made enough space to drive the vehicle away. Airport operators may find their time and efforts are better spent securing the physical facilities from unauthorized ingress and egress.

KEY CABINETS AND SAFES

Many smaller RAC operations secure vehicle keys in a lockable key cabinet or a safe (Figure 8-11) that requires a PIN or other form of credential. Biometric-activated safes are becoming more affordable and may be options for enhanced security.

Sometimes the key cabinet is the responsibility of a single individual who authorizes the retrieval of every key. This is often a RAC site manager who is the only one with the access code or key to the safe.

> A small RAC operator at one airport had a single person responsible for maintaining the keys, including retrieving, securing, and releasing the keys. This operator had no vehicle thefts during a period when other RAC operators were experiencing a high number of thefts.

KEY LOCKERS

Key lockers contain multiple small compartments that each hold one set of keys, and can be opened individually with a unique code. Apartment complexes and gated communities often use these lockers for residents to leave copies of their keys for couriers, pet sitters, or guests to access their home.

Smart key lockers can be managed remotely through a web-based portal and opened with a mobile app. Using a system such as this could allow the RAC operator to mount the lockers on each row and store the keys for the vehicles in that row in the locker. Customers would be provided with a PIN or QR code that can be scanned by the locker to open the corresponding key compartment.

KEY ORGANIZERS

Key organizers are wall-mounted fixtures designed to hold the vehicle key and rental contract (Figure 8-8). These are less secure than wall cabinets, safes, and lockers, but they offer some expedience for customers in a hurry. Rentals scheduled for pick up that day are stored on the organizer, which is

positioned where all of the counter agents can reach them. The remainder of the keys are stored in a locked safe and brought out when needed.

This method of storing keys behind the counter or on a wall is most commonly seen at smaller airports where RAC operators have a small fleet. However, this method is highly unsecure. Keys stored in this manner cannot be left unsupervised and unprotected as they are open to theft by an opportunistic criminal.

> A RAC operator at a CAT III airport experienced an incident where several gang members rushed the RAC counter and stole multiple key fobs from a key organizer behind the customer counter. The individuals stole several vehicles in this incident.

Figure 8-8. Example of a Key Organizer

Airport operators should discourage RAC operators from utilizing these organizers. Instead, they should be encouraged to secure the keys in a locked box, safe, or room.

KEY RETURN BOXES

Key return boxes are steel boxes that allow the rental customer to drop their rental vehicle keys and rental contract without requiring an employee to be present. The keys and contracts are kept in the locked compartment until the RAC manager retrieves the contents in the morning.

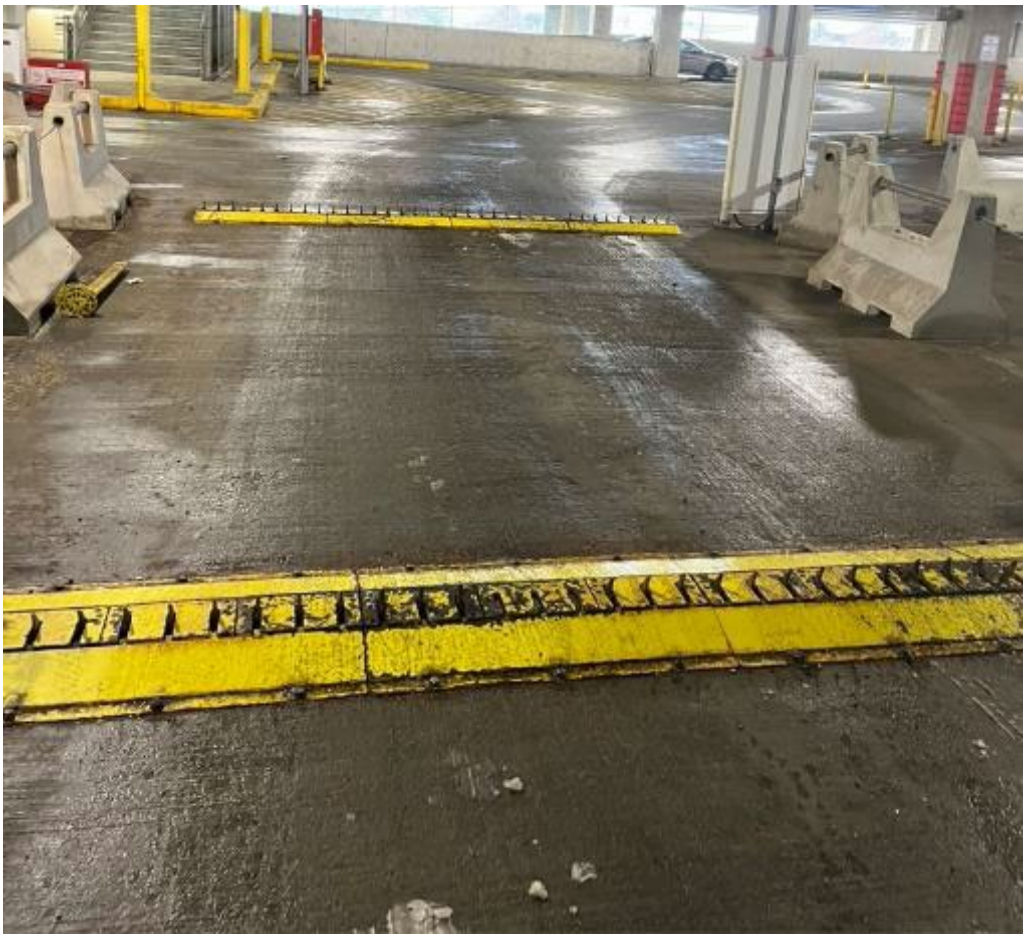
Large and small RAC operations use key return boxes to various extents. Some are only used during closed hours and some are stationed at non-RAC locations, such as before the passenger security checkpoint, to facilitate returning forgotten keys to the RAC operator.

> One airport operator requested the RAC operators install return key boxes at the counters in the baggage claim hall after a few incidents of customers leaving keys on the counter instead of in the return area.

8.4.3 Traffic Spikes

One-way traffics spikes, also referred to as tiger teeth, are very common at the entrances of RAC facilities to prevent vehicles from exiting through the access point (Figure 8-9). They may also be deployed at the RAC facility exit, but that is less common. If a vehicle attempts to roll over the spikes from the wrong direction, the metal spikes will puncture the tires and render the vehicle immovable.

Figure 8-9. Example of Traffic Spikes



Traffic spikes are susceptible to malfunctions and damage due to constant use. Vehicles drive over the spikes constantly throughout the day, and the springs that enable them to lower wear out until they no longer spring back. This can allow a vehicle to pass through the gaps in the spikes and exit. Traffic spikes often require a considerable amount of maintenance and repairs.

Traffic spikes can also be easily bypassed or defeated using bricks, wood planks, floor mats, sign placards, or other materials that cover the spikes and render them useless; many vehicles are stolen from RAC facilities in this way. Regular security patrols through the facility should look for and remove any items that may be used to compromise the traffic spikes.

8.4.4 Plate Barriers

Plate barriers are common at RAC facility exits to prevent vehicle theft. Also called wedge or embassy barriers, these barrier devices lay flat on the ground when deactivated but pivot from the ground to create a wedge when activated (Figure 8-10).

The barriers may be hydraulic or electrically powered. Note that hydraulic systems are notorious for regularly malfunctioning, especially when used in a high-volume environment such as at RAC facility exits. Many legacy plate barriers deployed at airport restricted vehicle access gates were designed with hydraulic systems buried in the pavement, but they easily collected rain, snow, dirt, and debris that made the system inoperable until cleared and repaired. Following the manufacturer's recommended

maintenance schedule can alleviate many of these challenges. Many new RAC facilities use electric plate barriers that are bolted to the surface of the pavement, eliminating many of the challenges of the older systems.

Buried cables in the pavement can be used to detect the presence of a vehicle and activate the barrier to prevent egress. The barrier is then lowered by the booth attendant after the rental contract has been reviewed. In-ground vehicle detectors may also be used to monitor for vehicles traveling in the wrong direction, triggering barriers to pop up and stop a vehicle attempting to exit through the entrance lane.

Figure 8-10. Example of a Plate Barrier and Barrier Arm

Some airport operators have experienced plate barriers that are slow to raise into the locked position. In some cases, this has allowed a second vehicle to piggyback through the exit behind another vehicle. Airport operators should work with the vendor to find the most appropriate activation speed for the equipment and RAC operations.

> Plate barriers are incredibly effective at stopping a ramming or speeding vehicle. One airport's Chief of Police used footage of a vehicle being totaled by a plate barrier to justify the addition of these barriers around their consolidated RAC facility.

Unfortunately, when a vehicle hits an activated plate barrier the vehicle is usually declared a total loss and the plate barrier system has to be repaired and reset; the barrier and possibly the entire exit will be unusable until the barrier is repaired.

Plate barriers are often included as part of the construction of consolidated RAC facilities. Some airport operators install the infrastructure and in-ground detectors required to operate a plate barrier, but have the RAC operator or consortium install the barrier equipment with their operating budget.

8.4.5 Barrier Arms

Barrier arms are one of the most common types of active barriers used at RAC facilities and parking lots. When activated, the arm sits horizontally across the vehicle lane. When the barrier is deactivated by the booth attendant, the barrier arm pivots vertically from one side to allow the vehicle to pass.

Many barrier arms are crash rated to stop ramming and speeding vehicles. Anti-ram models have a pedestal on the opposite side of the lane for the arm barrier to sit and lock in place; this helps reinforce the arm when hit and prevents it from being lifted manually. Anti-ram capabilities are important for barrier arms, especially if not paired with another barrier type because criminals may sacrifice the exterior of a vehicle or sacrifice one vehicle to allow multiple other vehicles to exit the facility.

Like plate barriers, barrier arms are often included in the construction of consolidated RAC facilities before the operators occupy the space. The barriers are most often placed at the RAC exits but may also

be placed at the entrances. Some are activated by in-ground detectors buried in the pavement to detect approaching vehicles or vehicles traveling in the wrong direction.

If the in-ground detectors are placed inside the RAC facility at the entrance, the barrier arms will remain open until a vehicle is detected approaching from the wrong direction; it will then lower into the secure position and prevent egress. When the in-ground detectors are installed outside of the facility entrance, the barrier will remain locked in the horizontal position until a vehicle attempts to enter the facility from the roadway; the in-ground detectors trigger the barrier to raise and allow the vehicle to enter the facility.

Barrier arms at the facility exit are opened by the booth attendant after they have reviewed the rental contract.

One airport LEO reported several incidents of personal vehicles becoming accidentally trapped in the RAC facility after the operators had closed for the night. The entrance to the consolidated facility is close to the entrance of the long-term parking lot, and it is common for vehicles to enter the wrong lane and end up in the RAC facility.

Airport LEOs received multiple calls from lost individuals to be let out of the facility, but the button to deactivate the security barriers was in the locked security booth with no manual override. The airport police had access control pedestals added that allow LEOs to deactivate the barriers with their airport ID.

8.4.6 Concrete Barriers

Concrete barriers, sometimes called Jersey or J-Barriers, are commonly used in RAC facilities to separate RAC operations and prevent vehicles from crossing between the operating areas. The barriers are often included in the construction of consolidated RAC facilities before the operators occupy the space. The blocks can weigh up to 4,000 pounds, but they can be moved if necessary, making them semi-adjustable.

The barriers need to be attached to the pavement or connected together with an anchored cable system to prevent them from being shifted (Figure 8-11). Patrols and inspections of RAC facilities should look for concrete barriers that have been moved or have not been properly secured.

Figure 8-11. Concrete Barrier Attached to the Pavement and Anchored to Other Concrete Barriers

One airport operator discovered one of the barriers had been shifted at some point just enough to let out a vehicle. The blocks were not secured when they were installed, allowing a vehicle or determined individual to push them out of the way.

Criminals interested in vehicle parts will sometimes sacrifice the exterior of a vehicle or an entire vehicle to disable or move these barriers to allow multiple vehicles to pass.

8.4.7 Plastic Barriers

Water- or sand-filled plastic barrels are sometimes used as barriers throughout the RAC facility (Figure 8-12). When empty, the barriers are light enough to move by hand; when filled, they can act as a barrier to vehicles. The ability to empty and refill the barriers makes them highly mobile and flexible to deploy.

Figure 8-12. Example of Water-Filled Plastic Barriers

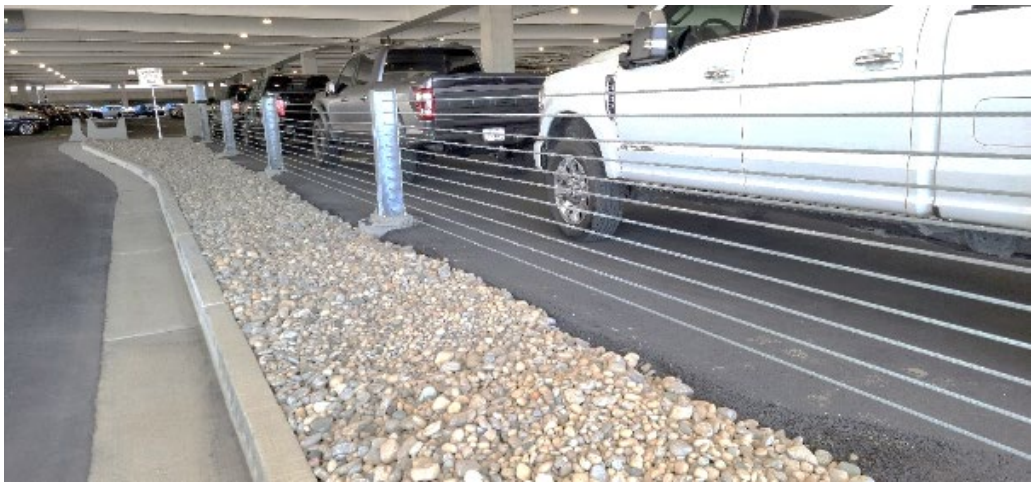
RAC operators using plastic barriers should ensure that they are all full of water or sand and not leaking; bad actors can puncture the barriers to drain them. The barriers should also be cabled or chained together and secured to the pavement to keep them from being shifted.

Even when filled, these plastic barriers are not effective at stopping vehicles at ramming speed, but they can delineate traffic lanes and separate RAC operations. Additionally, water-filled barriers may not be practical in climates where temperatures go below freezing, as the barriers can be damaged when the water freezes and expands.

8.4.8 Cable Systems

Anti-ram cable systems are designed to stop a ramming or speeding vehicle. Many airport operators use cable systems throughout the airport campus, primarily around the perimeter. At RAC facilities, cabling is used along each level's perimeter to prevent vehicles from driving out of the facility or off an upper level (Figure 8-13). They may also be used to separate the RAC operations and separate restricted from unrestricted areas.

Figure 8-13. Cable System



Cable systems that are not properly installed and secured can be easily removed by hand. Additionally, it is possible to cut the cables with a handheld grinder in just a few minutes, allowing vehicles to pass.

Adding an anchored cable system to a chain-link perimeter fence can protect the fence from being penetrated by a ramming vehicle. The cables should be installed on the inside of the fence to prevent criminals from using the cables to climb the fence.

8.4.9 Fences and Walls

Many RAC facilities use perimeter fencing or walls to discourage non-rental customers from entering the facility and to conceal the RAC operations. The most common types of fencing or barriers used are security fencing and brick or concrete walls.

The fence or wall will need to ensure that unauthorized individuals will not be able to jump or climb over. Maintaining a ten-foot buffer (standoff distance) between the perimeter fence or wall and the RAC facility will prevent criminals from using the fence to jump to a higher level.

Figure 8-14. Example of Anti-Climb and Anti-Ram Fencing

Fences and walls can be used in areas other than the RAC perimeter. Many RAC facilities use chain link fences to separate RAC operations. They can also be deployed to prevent access to areas where individuals may try to conceal themselves, such as the space under stairs.

FENCING

Security fences are less expensive to install and replace than solid walls, and they support more open sightlines within RAC facilities to improve situational awareness. However, they also provide clear sightlines of the RAC operations to anyone surveilling the facility, providing them with intelligence on routines and schedules.

RAC facilities are typically equipped with anti-cut and anti-climb security fencing, which also has anti-ram capabilities (Figure 8-14). Fences will be more protected if paired with a cable system or concrete barriers. Anti-ram features are important to prevent criminals from using a sacrificial vehicle to breach the perimeter and allow multiple vehicles to exit.

Figure 8-15. Vertical Bar Fence with Curved Topper

Anti-climb mesh can also be added to the fence if needed. Fencing with vertical bars is good at preventing climbing because it offers no useful footholds (Figure 8-15). Some airport operators add barbed wire or curved and pointed toppers to the top of the fence to discourage climbing.

Although less common, some airport operators add an electric fence to their consolidated RAC facility perimeter. The electric fence is usually accompanied by a non-electrified interior fence to prevent rental customers from touching the electric fence. Typically, the fences are only activated during non-operating hours. Care needs to be taken when

deploying electric fences to prevent customers from getting hurt. Electric fences must always be accompanied by a warning sign.

WALLS

Solid walls made of concrete or brick are sometimes considered more aesthetically appealing than security fencing, but they are also much more expensive to procure and repair. Solid walls will limit RAC operator surveillance of activity outside of the facility except by using exterior facing cameras. However, solid walls can prevent bad actors from surveilling operations in the RAC facility. This can be good for RAC facilities scattered across the airport campus, which often have fewer security measures in place. Additionally, solid walls act as a formidable barrier to stop ramming attempts.

Creating more open sightlines can be challenging in spaces that have already been constructed with solid walls. Some airports may be able to enhance sightlines by replacing brick or concrete walls with fencing or shorter concrete barriers and cable arresting systems.

For more information about perimeter fencing and walls, refer to PARAS 0015: *Guidance for Airport Perimeter Security*.[8]

8.4.10 Bollards

Bollards are commonly used to prevent vehicles from entering restricted areas while allowing for pedestrians to pass between or across traffic lanes. Bollards are commonly constructed of concrete or steel, and they are usually deployed around the RAC lobby building and security booths. Airports typically install bollards around the common areas during consolidated RAC facility construction.

Like any physical security measure, bollards are most effectively deployed when the locations are strategically planned. They are not easily moved once they have been buried or installed in the pavement. When deployed in vehicle operation areas, such as the ready/return areas, bollards should be clearly visible through the use of reflective paint or lights.

> One airport LEO described an incident where a criminal managed to squeeze a vehicle between two bollards at a crosswalk and drive away. The vehicle sustained serious damage to the exterior, but the vehicle was stolen for its parts, not resale. The airport had to install another bollard to close this gap and eliminate the vulnerability.

8.4.11 Vehicles

Many RAC operators utilize shuttle buses and less expensive vehicles to create barriers in front of entrances, exits, and expensive vehicles. This is a cost-effective strategy to protect vehicles overnight, especially if the RAC facility does not have physical security measures or access controls in place.

Some RAC operators stack their cars in rows in the ready/return area. The first car and last car in the row are de-keyed to make it more difficult to steal the vehicles. However, most vehicle thieves are not interested in the appearance of the vehicle but the parts inside. Thieves may drive the cars back and forth, ramming into the surrounding vehicles until they have made enough space to drive the vehicle away.

[8] **PARAS 0015:** https://www.sskies.org/images/uploads/subpage/PARAS_0015.AirportPerimeterSecurity.FinalReport.pdf

8.4.12 Pedestrian Access Doors

Several multilevel RAC facilities have pedestrian doors that provide access to the facility from the perimeter, or provide access to each level. This can be a significant vulnerability, especially when the doors are propped open or left unlocked. Airport operators have developed a few strategies to lower the risk.

New facilities can ensure that the design of the facility limits access points to the bare minimum necessary to meet operational needs and comply with fire codes. Existing facilities can secure unnecessary access doors. The remaining doors should be one-way access. This can be done by removing handles on the outside of the doors, similar to fire door systems. Fire codes and RAC operations will dictate which doors are considered essential.

Full-height pedestrian turnstiles (Figure 8-16) eliminate the possibility of door propping, so they are a good option for employee portals that must be used frequently .

When possible, access controls should be added to pedestrian doors and turnstiles to prevent unauthorized access. Additionally, security patrols should ensure access doors and turnstiles are locked when the RAC facility is closed.

Figure 8-16. Full-Height Pedestrian Turnstile Access Door

One consolidated RAC facility has a stairway core with an access door on the exterior perimeter on each level. The airport was concerned that unauthorized individuals could access the stairs from the exterior on ground level and traverse to any of the levels where vehicles are stored.

They could not remove the stairs or block them because they are considered emergency exits. Instead, the airport operator converted the doors to one-way fire exits on each level. The doors have no handles in the stairwell, so once a person enters the stairwell they can only exit on the top level or the ground level.

8.4.13 Vehicle Access Gates

Separating the RAC operations with concrete barriers or fencing helps minimize vulnerable areas but can prevent emergency vehicles from entering consolidated facilities if not carefully planned. The most common solution is to create a fire access lane that can cross every RAC operator's exclusive area. Rolling gates are installed in the fence line and are typically locked with a cipher lock but may have card swipe access control. Certain authorized individuals, such as first responders, may be given direct access authority through a proximity reader and vehicle tag, but most are required to call ahead to the airport to have the gates opened.

During an inspection, one airport operator found that the red fire padlock used by first responders had been replaced at some point with a regular padlock wrapped in red tape. The airport operator recommends checking the padlocks on emergency gates during routine security patrols and inspections.

Vehicle gates that permit vehicle shuttlers to leave the facility to drive the vehicle to the QTA may require a designated RAC employee to swipe their credentials or enter their PIN to allow the vehicles to exit. This ensures drivers are authorized to leave through the gate.

8.4.14 Future Trend: Security Robots

The practice of augmenting human staff with robots has been gradually increasing as robotic technology continues to improve. Use of robotic technology in airports is also expected to increase as pilot programs prove robots' capabilities.

Several vendors offer security robots designed to patrol areas such as airport terminals and parking lots to help deter criminal activity. These settings are very similar to RAC facilities, suggesting that current robotic technology could support deployment at a RAC facility. Autonomous robots have the ability to perform dozens of functions with a variety of sensors, cameras, and speakers. Many models autonomously navigate and patrol pre-mapped routes using laser, ultrasonic, and bump sensors to determine their location and avoid collisions. They can also be programmed to guard a designated position instead of patrolling. Most security robots perform warning functions such as flashing lights and audible notifications. Security personnel can use the speakers to communicate with individuals from the monitoring room. When necessary, the robot can alert dispatch to send security personnel or LEOs.

Many robots are able to operate indoors or outdoors in moderate temperatures for about three hours before they need to recharge. Improvements in energy storage technology may result in more efficient batteries and longer operating times.

No airport has reported using autonomous security robots to patrol RAC facilities. While some US airports have piloted autonomous robots, the majority of security robots have been deployed at airports outside of the United States. Known robot pilots in the US include:

- In 2018, LaGuardia Airport piloted a robot at its Terminal B arrivals curb. Referred to as B-3PO, the robot was programmed to patrol the entirety of the curb while capturing video footage.
- In 2021, George Bush Intercontinental Airport piloted a robot in its Terminal C parking garage to assist customers with vehicle problems such as dead batteries, flat tires, and lock outs.
- In 2023, Los Angeles International Airport introduced a robot to a major parking structure to deter criminal activity and offer customer support.

Examples of deployments outside the United States include:

- In October 2021, Kansai International Airport in Osaka, Japan, deployed two security robots to patrol Terminal 2 and the airport's railway station (Figure 8-17)
- In July 2023, airline service provider Hong Kong Air Cargo Terminals Limited introduced its first security robot to surveil and patrol the parking areas and export goods handling zones
- In April 2023, the Singapore Police Force added two security robots to patrol Changi Airport

Figure 8-17. Security Robot at Kansai Airport

Source: Kansai Airport

8.5 Lighting and Signage

Lighting and signage are critical to the security of the RAC facility and the perception of security. Lighting is one of the essential elements of the CPTED model. Signage is critical to inform drivers about security systems in use at the facility and traffic safety measures.

8.5.1 Lighting

Effective lighting supports natural surveillance activities, illuminates human activity, deters criminal activity by making it difficult to hide, and facilitates detection of potential offenders and criminals. Strategic lighting design improves the capabilities of surveillance systems and security patrols, enhances wayfinding, and supports normal and emergency operations. Enhancing lighting in RAC facilities can greatly improve the security of the facility without needing to add cameras or other physical security measures.

New lighting systems use Light-Emitting Diode (LED) lamps to improve illumination levels and lengthen the equipment's life cycle. Many airport operators with legacy lighting systems are transitioning to LEDs as the existing incandescent and florescent lamps expire and must be replaced. The LED lamps also provide better illumination, which is key for covered parking facilities. Lighting can be enhanced by painting the ceiling, walls, columns, and the pavement with a bright, reflective white paint.

Uniform lighting is important to minimize shadows where criminals can hide or bright pools of light that can be disorienting to drivers and pedestrians, especially those with low vision or sensitivities to light. The vertical core (elevators, stairwells, escalators) and the exterior of RAC facilities will be the highest risk areas. Appropriate airport personnel and assigned contract security staff, as applicable, should walk through the facility during the day and at night to ensure there is enough lighting in all areas at all times.

Lighting design should consider the difference in light levels when entering and exiting covered RAC facilities. Drivers exiting a dark or dim facility may be momentarily blinded by the bright daylight; alternatively, drivers entering a dark or dim facility from the bright daylight may need a few moments to adjust or to remove their sunglasses. Both of these situations can be hazardous. Lighting designers will be able to create transitional lighting levels to help minimize drivers' visual adjustment period.

Many airport operators indicated that their RAC facilities use dimmable lights that brighten when motion is detected. When no motion is detected, the lights dim to about 25% of their full illumination. The lights being triggered at night can alert airport or RAC security to activity in the facility.

Open-air RAC facilities and strategically designed multilevel RAC facilities are able to use natural sunlight during the day instead of artificial lighting. Open-air RAC facilities and the top levels of multi-level facilities can leave the parking lot lights off until the sun begins to set. Many RAC facilities turn off the perimeter lighting during the day because sunlight illuminates the exterior of the facility and the perimeter.

8.5.2 Signage

Signage informs and alerts potential criminals, customers, pedestrians, and drivers to the safety and security measures used throughout RAC facilities. Effective signage in the RAC facility addresses three main security messages:

- **Installed security measures** – signage informs potential criminals of the surveillance systems and security equipment in place at the facility to discourage criminal activities (Figure 8-18)
- **Alerting and response systems** – signage informs pedestrians of the various alerting and response systems around the RAC facility (e.g., "If You See Something, Say Something®" and security contact numbers)
- **Access control** – signage informs everyone in the facility of the restricted areas (e.g., Employees Only) and the consequences for entering these areas without authorization

Figure 8-18. Security Measure Warning Sign

Where possible, airport operators should ensure that appropriate signage is placed in the proper locations in RAC facilities. It is also important for airport operators to be aware of their local and state laws governing issues such as video monitoring and trespassing, and other relevant laws. Adding signs that reference these laws will alert everyone to the rules and regulations governing the use of the RAC facility and the consequences for violating those rules.

8.6 Landscaping

Landscaping around the RAC facility create a calming and attractive environment while deterring customers and unauthorized individuals from entering certain restricted areas. Well maintained landscaping can signal to potential criminals that the facility is looked after and that criminal activities may be easily observed. It also improves the sense of security for everyone using the facility.

Trees, hedges, plants, and large rocks can be used outside the RAC facility to delineate walking paths and designate areas that pedestrians should not walk. Large trees and hedges can be used to reduce surveillance of the RAC operations and access from outside the facility, but they should be well maintained so that criminals cannot hide amongst the vegetation.

> One airport has a series of trees growing between the long-term parking lot and the RAC operations that create a natural barrier to prevent vehicles from hopping the median and exiting via the RAC facility exit. The natural barrier has been highly effective, but maintenance vehicles must park in the roadway to tend to the trees, which can be a safety hazard. Landscape designers should account for maintenance access in their design.

Hostile landscaping that uses thorny vegetation may keep individuals from getting too close to certain areas, such as the perimeter. Tall trees should not be left to grow too close to a perimeter wall where they could enable criminals to jump over the barrier. Vegetation should be kept trimmed to prevent obstruction of cameras or lines of sight.

> One airport operator reported one tree near the perimeter of the consolidated RAC facility needed to be regularly trimmed because it grew directly in front of a surveillance camera.

8.7 Maintenance

It is important to maintain security equipment in good working order to minimize downtime from equipment or parts failure. Responsibilities for security equipment in the RAC facility can be complex

due to the multiple ownership types. Consolidated RAC facilities typically are divided into several areas, such as exclusive-use areas for each RAC operator, common-use areas that are secured by the airport such as the customer service lobby, and the shuttle bus staging area, which can be owned and operated by the airport or the RAC operators. In general, the entity that owns the security equipment is responsible for maintenance and repairs on that asset. Maintenance in the RAC facility includes repairs, preventative maintenance, and landscaping around the facility.

When a third-party facility manager is contracted, they may care for the facility and security equipment, which may include minor repairs or contracting with vendors. Systems that constantly move (e.g., hydraulic systems, arm barriers) will require more frequent repairs and maintenance. In-ground detectors are particularly susceptible to extreme heat and cold and may require frequent preventative maintenance in certain climates and conditions.

Preventative maintenance on security equipment is based on the manufacturer's recommendations and increases in frequency as the equipment ages. When the manufacturer's warranty has expired, the airport operator should consider contracting with a qualified repair vendor or training airport maintenance to reduce downtime from broken security equipment. Maintaining an inventory of commonly needed spare parts can also reduce the equipment downtime.

8.8 Existing Facility Enhancements

Existing RAC facilities are restricted by the layout that was designed when the facility was built, as it is difficult and expensive to modify the layout of an existing facility. However, there are many options that airports can deploy at their existing RAC facilities without major construction requirements, including:

- Surveillance systems (CCTV, video analytics, LPRs)
- Two-way communication (duress or panic buttons)
- Fraud and counterfeit verification equipment
- Security patrols (LEOs, airport security/operations, contract)
- Lighting and signage
- Traffic lane configurations with:
    - Traffic calming measures (speed bumps, multiple curves)
    - Physical security measures (concrete barriers, plastic barriers, cable systems, fences, bollards)
- Vehicle exits and entrances with:
    - Physical security measures (traffic spikes, plate barriers, barrier arms)
    - Sally ports
- Pedestrian access portals with
    - Access control measures (airport badges, fuel cards)
    - One-way doors or full-height turnstiles
- Maintenance of security equipment and the facility
- Landscaping (improve sightlines, discourage hiding)

The best starting point for airport operators with existing RAC facilities is to conduct a threat and vulnerability assessment (TVA) with a security walkthrough of each facility. The threat assessment portions should include identifying trends in criminal activity locally and nationally. The vulnerability assessment should include a review of the physical features of the location and activities and operational

practices of the RAC operators affected. A walk-through should be performed by the facility renovation architect accompanied by airport security, airport police, and the RAC corporate management, if possible. Because security is dynamic and ever evolving, annual facility walk-throughs or site assessments can help identify gaps in security and opportunities for improvements to security measures.

Many airport operators hire a consultant to perform a TVA of their consolidated RAC facilities every year. This ensures that security facility design, equipment, and policies are consistent and current with industry practices that have evolved since the facility was originally developed.

A list of projects can be created from the TVA and prioritized. Projects that would require the RAC operator to furnish equipment or personnel should be discussed with them to find compromises or alternate options if necessary. If the airport is responsible for additional or enhanced security measures, this can be planned for and built into the airport security budget.

Appendix A includes a case study on the security improvements Minneapolis-Saint Paul International Airport implemented at their existing facility.

8.9 New Construction

Security is most effectively and economically implemented when it is factored into the initial design. Therefore, it is good practice for airport security teams (airport, police, contract security) and RAC operators to work closely with the design teams of new RAC facilities on airport property. This can ensure that security considerations are built into the design and will not need to be retrofitted. This is especially true of any buildings within the terminal area, as these will need increased security measures. Adding security measures and necessary infrastructure is far more time consuming and expensive once the facility is bid, constructed, open, and operating.

Conducting a TVA, or several, during late schematic and early detail design phases can help airport operators identify important security features to include in the new facility design. Risk assessments should consider the crime trends in the surrounding communities and develop solutions to prevent or reduce specific criminal activity and security vulnerabilities.

It is also a good practice to perform a tenant security walk-through/TVA of the facility before final decisions are made regarding security measures. This often includes review of camera installations and placements, security barriers, duress button locations, and other security measures with airport security, the facility planner, and the RAC corporate management or consortium representative. The period to perform this walk-through is after the skeleton of the building is complete but the construction is not so complete that supporting security infrastructure cannot be shifted.

The airport security team and RAC corporate management should walk through the facility during the operational readiness assessment, prior to facility opening, to identify security vulnerabilities.

RAC operators will occasionally hire a security consultant to perform proactive TVAs of their exclusive space in the RAC facility before the operator occupies the space. This allows them to determine what security equipment needs to be furnished in their space.

8.10 Consolidating Facilities

While far from universal, airports of all sizes are increasingly consolidating facilities to accommodate their RAC operations. Consolidating RAC facilities offers several security and public safety benefits to the airport, the RAC operators, and customers:

- **Consolidation of resources:** Flat lots are common at airports but require a designated ready/return area and QTA for each RAC operator. Use of individual flat lots dedicates a significant amount of land for operations spread out across the airport campus and requires airport security and LEO response to travel much farther distances to access and patrol the sites. Consolidating all the RAC operations into a single footprint allows for more efficient use of security resources, such as LPRs, cameras, security patrols, LEO response, and security barriers.
- **Reduced vehicle traffic:** It is common for RAC operators with individual flat lots to also have brand-specific buses to shuttle customers between the RAC counter, RAC ready/return area, and airport terminals. Consolidating the RAC operations into a single location can also consolidate buses, which reduces traffic congestion at the airport terminal curbs and improves safety along the curbs and roadways. In many cases, buses can be eliminated entirely to further reduce the number of vehicles next to the terminal.
- **Decreased pedestrian congestion:** This is a benefit specifically for airports moving the RAC operations from the baggage claim hall to a consolidated RAC facility. RAC operations experience surges in customers throughout the day and year based on flight operations, holidays, and special events. When RAC operations are adjacent to baggage claim operations, there are more opportunities for congestion and bottlenecks where passengers claiming their bags and RAC customers intermingle. Moving the operations out of the terminal reduces the number of individuals crowding the public space of the terminal in the baggage claim area, making the area a less attractive target for potential bad actors.

Fully consolidated RAC facilities—where the RAC operators share ready/return space, storage, lobby, and QTAs—are not an option for many airports for several reasons, including a lack of available space, limited budget, and extended lease agreements already in place with RAC operators. However, airport operators may be able to consolidate certain operational areas to take advantage of some of the benefits listed above. For example, some airports consolidate the QTAs where vehicles are washed, cleaned, serviced, and refueled (Figure 8-19). This can help consolidate costs associated with maintaining security in these areas, improve security resource efficiency, and create space for expanded needs of the RAC operators.

Figure 8-19. Example of a Consolidated QTA

REFERENCES

Brookes, Tim. (2022). "How AirTags Are Being Used to Stalk People and Steal Cars." How-To Geek. https://www.howtogeek.com/784608/how-airtags-are-being-used-to-stalk-people-and-steal-cars/. Retrieved 12 December 2022.

Conrac Solutions. *Problem Solving Airport Lease Requirements*. [Case Study].

Demkovich, Paul. (2011). *Airline and Airline Airport Consortiums to Manage Terminals and Equipment.* ACRP Synthesis 31. Transportation Research Board.

Demkovich, Paul. (2014). *A Guidebook for Airport-Airline Consortiums*. ACRP Report 111. Transportation Research Board.

Federal Bureau of Investigations. "Partners in Prevention: Vehicle Rentals and Vehicle Ramming." [Video]. https://www.youtube.com/watch?v=VpYIIT_LoR0.

Garrison, Robert. (2023). "DIA announces new security measures to tackle staggering car theft problem." Denver7. https://www.denver7.com/news/local-news/dia-announces-new-security-measures-to-tackle-car-theft-problem.

Gibbons, Ronald, et. al. (2015). *Airport Parking Garage Lighting Solutions*. ACRP Report 124. Transportation Research Board.

"Hamad International Airport deploys security robot." (2018). Airport Technology. https://www.airport-technology.com/news/hamad-international-airport-deploys-security-robot/. Retrieved 10 November 2022.

Hawaii Department of Transportation. (2019). "New Kahului Airport Rent-A-Car Center Completed on Time and on Budget." https://hidot.hawaii.gov/airports/new-kahului-airport-rent-a-car-center-completed-on-time-and-on-budget/. Retrieved 10 June 2022.

Hercher, Amy. (2021). "How Midway Car Rental Improved its Lot Security." Auto Rental New. https://www.autorentalnews.com/10141758/how-midway-car-rental-improved-its-lot-security. Retrieved 3 December 2023.

Hirsch, Howard. (2011). "How to Identify and Combat Rental Fraud." Auto Rental News. https://www.autorentalnews.com/146874/how-to-identify-and-combat-rental-fraud. Retrieved 8 December 2022.

International Association of Chiefs of Police. *An Educational Toolkit for Vehicle Crimes for Law Enforcement Agencies.*

International Association of Chiefs of Police. (2019). *It All Starts with a Stolen Car*.

Jacobs Consultancy, et. al. (2009). *Guidebook for Evaluating Airport Parking Strategies and Supporting Technologies*. ACRP Report 24. Transportation Research Board.

Jenkins, Brian Michael, and Butterworth Bruce R. (2019). *"Smashing Into Crowds" -- An Analysis of Vehicle Ramming Attacks*. San José State University.

Joint Counterterrorism Assessment Team. (2019). "Vehicle Rental/Leasing Industry Partnerships: A Force Multiplier." First Responder's Toolkit.

"K5". Knightscope. https://www.knightscope.com/products/k5. Retrieved 10 Nov 2022.

La Vigne, Nancy, et. al. (2011). *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention*. Office of Community Oriented Policing Services, U.S. Department of Justice.

LeighFisher, et. al. (2010). *Airport Curbside and Terminal Area Roadway Operations*. ACRP Report 40. Transportation Research Board.

Lekach, Sasha. (2018). "Facial recognition tech spreads to car rentals." Mashable. https://mashable.com/article/hertz-clear-car-rental-facial-recognition-biometrics. Retrieved 3 December 2023.

LexisNexis. "Detect fraud in real time with autonomous ID authentication." https://risk.lexisnexis.com/products/trueid.

Manzolillo, Nick. "What's a Key Management System & Why Do You Need One?" ButterflyMX. https://butterflymx.com/blog/key-management-system/.

Marsh, Christina. (2022). "Things to Consider When Building a Parking Garage." Airport Business. September/October 2022.

Meyer, Claire. (2022). "Growing a Sense of Ownership with CPTED." Security Management Magazine. May/June 2022 Issue.

Neal, Albert, and Cathy Stephens. (2003). "Defending Your Fleet Against Car Thieves." Auto Rental News. https://www.autorentalnews.com/146456/defending-your-fleet-against-car-thieves. Retrieved 8 December 2022.

New/Media Release. (2022). "Legislation Introduced to Combat Catalytic Converter Thefts." Auto Rental News. https://www.autorentalnews.com/10187431/legislation-introduced-to-combat-catalytic-converter-thefts. Retrieved 3 January 2022.

Richards, Jodi. (2016). "San Diego Int'l Builds $316 Million Consolidated Rental Car Facility". Airport Improvement Magazine. May/June 2016.

Sipe, Corey. (Mar 2022). "Back to Basics: Increasing Security Through Strong Physical Access Control." https://totalsecurityadvisor.blr.com/back-to-basics/back-to-basics-increasing-safety-through-strong-physical-access-control/. Retrieved 12 October 2022.

Smith, Mary. (1996). "Crime Prevention Through Environmental Design in Parking Facilities." Research in Brief. National Institute of Justice.

Tampa International Airport Police Department. *Counterfeit and Credit Card Fraud Investigation*. [Presentation].

Truck Renting and Leasing Association. (2006). *Truck Renting and Leasing Security Awareness and Self-Assessment Guide.*

Underwriters Laboratory. UL 752 Ballistic Standards.

U.S. Department of Defense. (2022). *DoD Minimum Antiterrorism Standards for Buildings*. UFC 4-010-01, change 2.

VPS. (2021). "Security Tips for Airport Parking Lots." https://www.vpslp.com/about/insights/security-tips-for-airport-parking-lots. Retrieved 10 October 2022.

VPS. (2021). "The Future of Airport Consolidated Car Rental Facilities." https://www.vpslp.com/about/insights/the-future-of-airport-consolidated-car-rental-facilities. Retrieved 10 October 2022.

VPS. (2022). "Ways to Improve Design of Car Rental Facilities." https://www.vpslp.com/about/insights/ways-to-improve-design-of-car-rental-facilities. Retrieved 10 October 2022.

Winter, Amy, and Chris Brown. (2013). "Identity Theft and Car Rental." Auto Rental News. https://www.autorentalnews.com/153089/identity-theft-and-car-rental. Retrieved 3 December 2023.

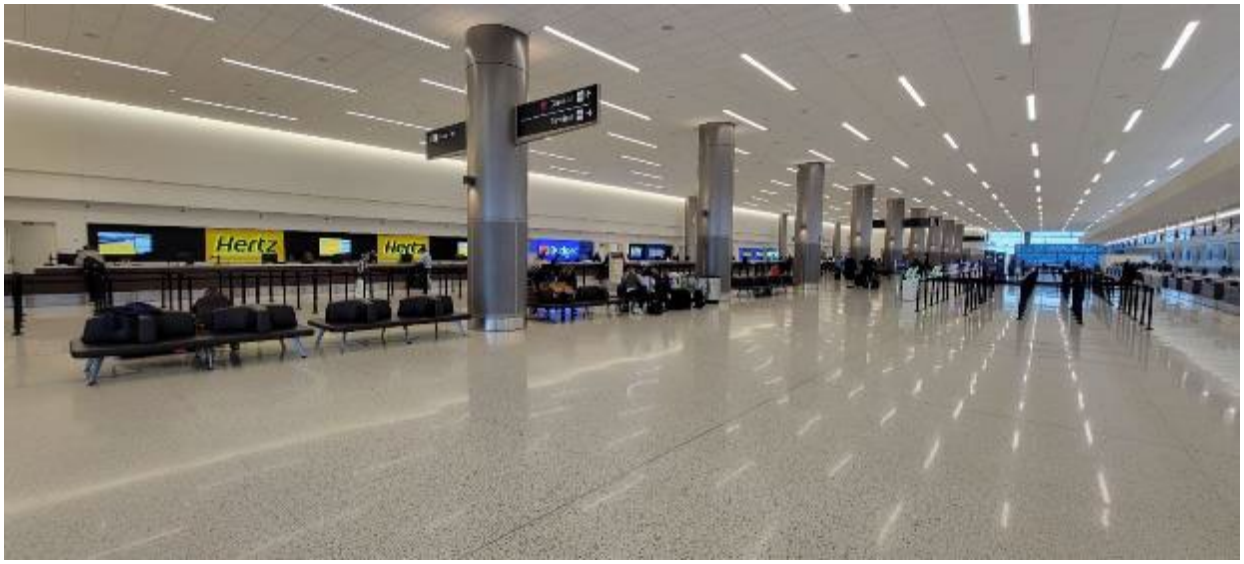
Youd, Frankie. (2021). "Do the robot: Kansai Airport's new autonomous security." Airport Technology. https://www.airport-technology.com/analysis/do-the-robot-kansai-airports-new-autonomous-security/. Retrieved 10 November 2022.

APPENDIX A: AIRPORT CASE STUDIES

SLC Consolidated RAC Facility Design

The consolidated RAC facility at Salt Lake City International Airport (SLC) opened in 2016 and was designed specifically with security as a high priority. Several vehicle-theft incidents occurred at the previous unsecured facility, which prompted physical security enhancements to be incorporated in the new design in addition to operational changes to deter criminal activity and improve public safety. The new facility, with added security enhancements, provides RAC operators with the ability to offer higher levels of customer service while minimizing the risk of vehicle theft.

Figure A-1. SLC's RAC Lobby



SECURITY BARRIERS

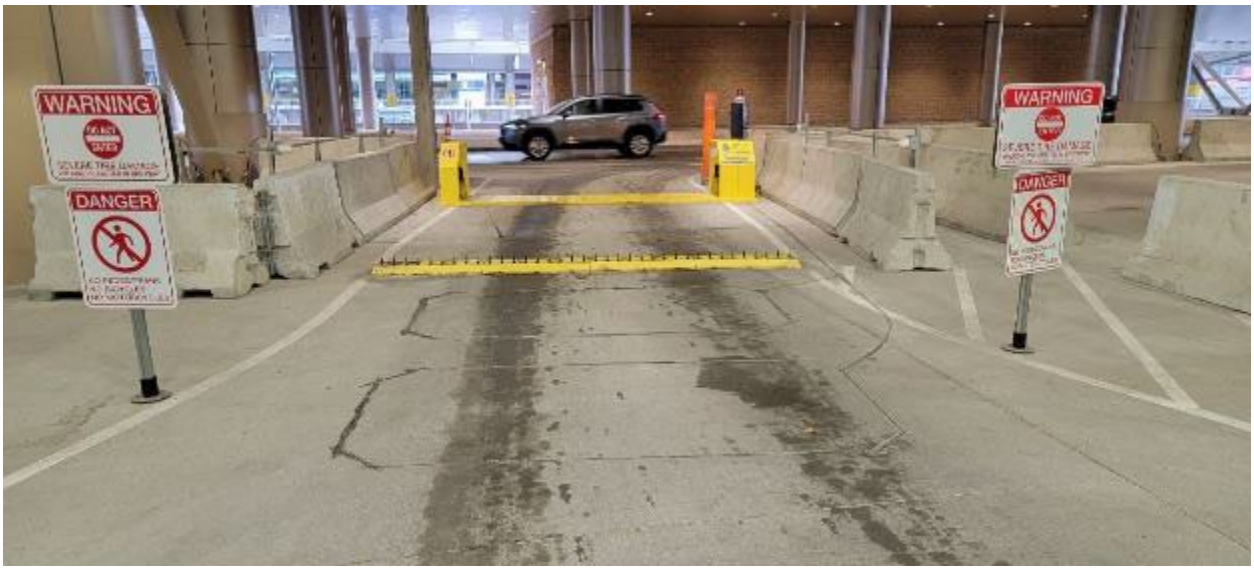
SLC worked closely with RAC operators to design the facility and security features. To ensure consistency in the security measures, the airport provided all the barriers and security booths at the entrance and exits (Figure A-2), as well as the concrete barriers and fencing throughout the facility.

Figure A-2. Identical Security Booths and Barriers at All Exits

The security barriers at the entrance and exits create an enclosed system to prevent unauthorized vehicle egress.

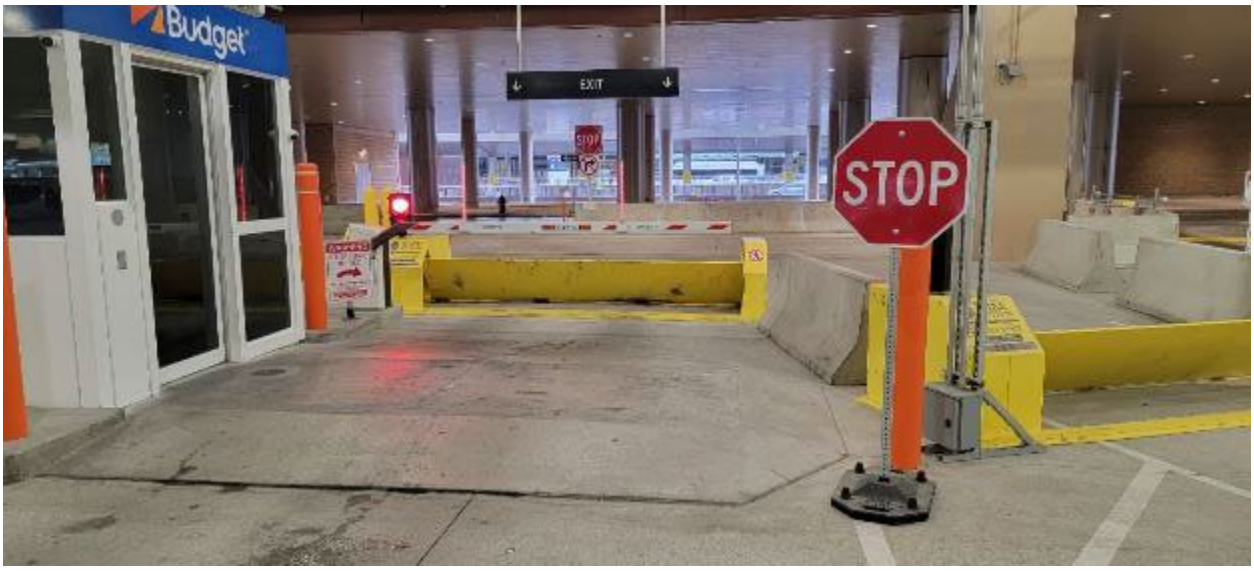
Traffic spikes and a plate barrier are installed at the entrance to the facility with an in-ground detector system to activate the plate barrier when a vehicle passes over them in the wrong direction (Figure A-3). Concrete barriers line the vehicle lanes to prevent vehicles from crossing into the wrong lane.

Figure A-3. Traffic Spikes and Plate Barrier at SLC RAC facility Entrance



The exits have several layers of security. Each RAC operator has exit lanes equipped with a security booth, a barrier arm, plate barrier, and traffic signage (Figure A-4). The barrier arm remains horizontal and the plate barrier remains upright until the employee staffing the booth reviews the driver's rental contract and ID. Once verified, the booth attendant deactivates the barriers, the traffic light turns green, and the vehicle is permitted to exit. The barriers then return to their secured positions.

Figure A-4. Exit Lane Security Measures



The plate barriers are surface mounted on the concrete instead of the buried model often seen at airport restricted vehicle access gates. SLC chose the surface-mounted model because it is less prone to malfunctioning due to snow, inclement weather conditions, and debris than its buried counterpart.

DESIGNATED RAC OPERATOR AREAS

Each RAC operator is assigned their own ready/return areas, vehicle storage area, QTA lanes, and maintenance space based on their original bid share that was part of the RAC operations procurement process. These spaces are separated by concrete barriers and fencing to prevent vehicles from one operator ending up in another operator's space, and to prevent criminals from bypassing the secured exits.

While this helps prevent vehicle theft, it also locks the airport and RAC operators into defined spaces that can be difficult to change. This can negatively affect operations and potentially revenue. In the previous facilities, market-share adjustments to leased stalls occurred annually, ensuring operators with the greatest market share had access to more stalls. In the new facility, the footprint and stall counts remain the same for the entire length of the agreement.

During the design of the facility, there was some concern over first responder access to the facility with so many fences and barriers. To address this, a fire lane with rolling gates at each fence line was added (Figure A-5). The rolling gates can be opened with a call to the control center by an authorized representative of the fire department, police department, or the airport.

Figure A-5. Fire Lane in Fencing

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN

SLC has designed their consolidated RAC facility to minimize vehicle thefts and other criminal activities using several layers of security. In addition to the physical security described above, the facility uses environmental and architectural design principles to deter criminals and create a less inviting target.

Cameras deter and detect criminals at the facility, and SLC has strategically placed their cameras to surveil the most vulnerable areas. Since the airport owns the cameras, it has quick and easy access to the video footage when necessary. Airport police also have access to this footage to assist with investigations.

The garage is well lit throughout all the public areas (Figure A-6). This is especially important for the security of the ready/return areas because much of the natural sunlight is blocked by the nearby terminal

and QTA building. To help increase illumination, all walls, columns, and ceilings in the parking areas are painted in a bright, reflective white.

Figure A-6. Well-Lit Parking Areas

Emergency duress buttons are scattered throughout the public areas of the facility. These are placed in well-trafficked areas and equipped with a blue light so they are easily located. When pressed, the airport control center is notified to pull up the cameras and send a response.

Airport LEOs patrol the facility during their perimeter patrol assignment. The facility is connected to the airport terminal via a skybridge, and officers patrolling the terminal public space also patrol the bridge and the RAC lobby during their shift.

PUBLIC AREA BADGES

SLC requires public area ID badges for the RAC operators' administrative staff. The badge provides no access authority to the restricted areas of the airport, but it requires a background check. SLC would like to badge all RAC employees, but the high turnover of the staff makes this cost and resource prohibitive.

TENANT IMPROVEMENTS

The RAC operators are permitted to add their own security measures. Most of the RAC operators install additional security cameras in their operational areas, especially at the exits and QTA. Some operators also post security guards when the RAC operations are closed for the night. All tenant security measures must conform to SLC's Rules and Regulations and Tenant Improvement Guidelines.

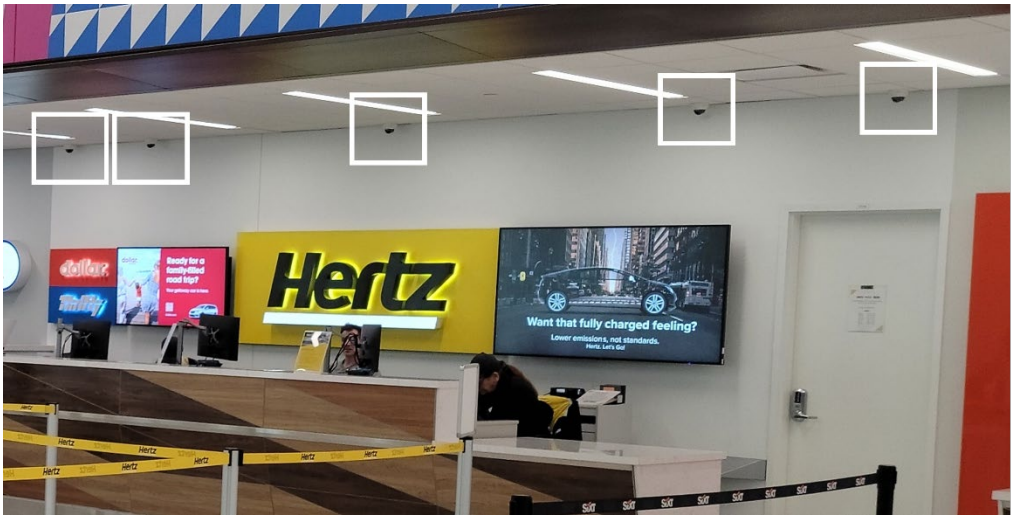
CVG Consolidated RAC and Ground Transportation Center

Cincinnati/Northern Kentucky International Airport (CVG) opened its new rental car and ground transportation center (GTC) in October 2021. One of the first of its kind, the GTC consolidates the RAC operations and provides a centralized location for customers to connect with valet services as well as catch shuttle buses to the airport hotel or parking lots. The GTC was designed to relieve traffic congestion around the terminal and reduce the number of shuttles transiting around the airport.

TECHNOLOGY

The Customer Service Building (CSB) is attached to the terminal by a short hallway and leads directly to the RAC ready/return areas in the GTC. The CSB contains the RAC counters and serves as the RAC lobby space. RAC operators have installed surveillance cameras behind the counters to capture the face of every customer (Figure A-7). This is useful for investigations of fraudulent activities.

Figure A-7. Cameras Behind RAC Counters in CSB



RAC operators own and install their individual surveillance systems on their leased level in the GTC. CVG does not have access to the live feed of these cameras, but the airport operators and police have cultivated a cooperative relationship with RAC operators that results in timely responses to requests for footage. This footage often helps the airport police investigate security incidents on the upper levels of the facility.

Figure A-8. Bollard-Mounted Camera

Some RAC operators have added cameras at their vehicle exits to capture images of every driver exiting the facility (Figure A-8). Posting the camera at vehicle window height provides the greatest visibility inside the car. Police detectives can use the images to identify suspects and establish a timeline of events.

CVG has mounted several surveillance cameras around the perimeter of the GTC, as well as within the facility and CSB. These cameras are integrated into the wider airport CCTV system. CVG has recently examined facial recognition technology that would use existing CCTV footage or LEO body

cameras. Kentucky statutes prohibit certain uses of facial recognition, and the airport police department is required to develop a policy for its use on the airport campus, which they are in the process of developing.

PHYSICAL BARRIERS

Levels 2–4 of the GTC each have a RAC ready/return area, fueling station, and car wash, and a level is leased to each RAC operator. RAC operators have positioned concrete barriers throughout their individual levels to create vehicle traffic lanes. These are connected with vehicle arresting cables and bolted into the concrete (Figure A-9) to prevent vehicles or people from moving the barriers.

Figure A-9. Barriers Separating RAC Operator Exclusive Areas

Vehicle-arresting cables separate the RAC leased areas (i.e., ready/return areas and QTA) from the public and unsecured traffic lanes (Figure A-10). These prevent the vehicles from breaching the fence line and discourage pedestrians from climbing or bypassing the fence line.

RAC operators contract a third-party facility manager to maintain their physical equipment and manage operations on levels 2–5, including security operations.

Figure A-10. Vehicle-Arresting Cable Perimeter

RAC operators are responsible for the security of their individual leased level and many have installed traffic spikes, plate barriers, and gate arms. It is common for operators to install multiple physical barriers (Figure A-11). During construction, CVG requested the designers add the infrastructure necessary for RAC operators to install plate barriers at the entrances and exits.

Figure A-11. Entrance with Double Barriers

TRAFFIC FLOW

The ground level of the GTC is divided into three traffic zones (Figure A-12). Each zone is designated for specific vehicle services on and off airport property. For example, Zone 3 is designated for loading and unloading hotel shuttles. Separating the shuttles greatly contributes to lower traffic congestion and safer crosswalks for pedestrians. All RAC traffic is isolated to the upper levels. This improves the safety of customers and pedestrians by reducing the number of vehicles in active areas.

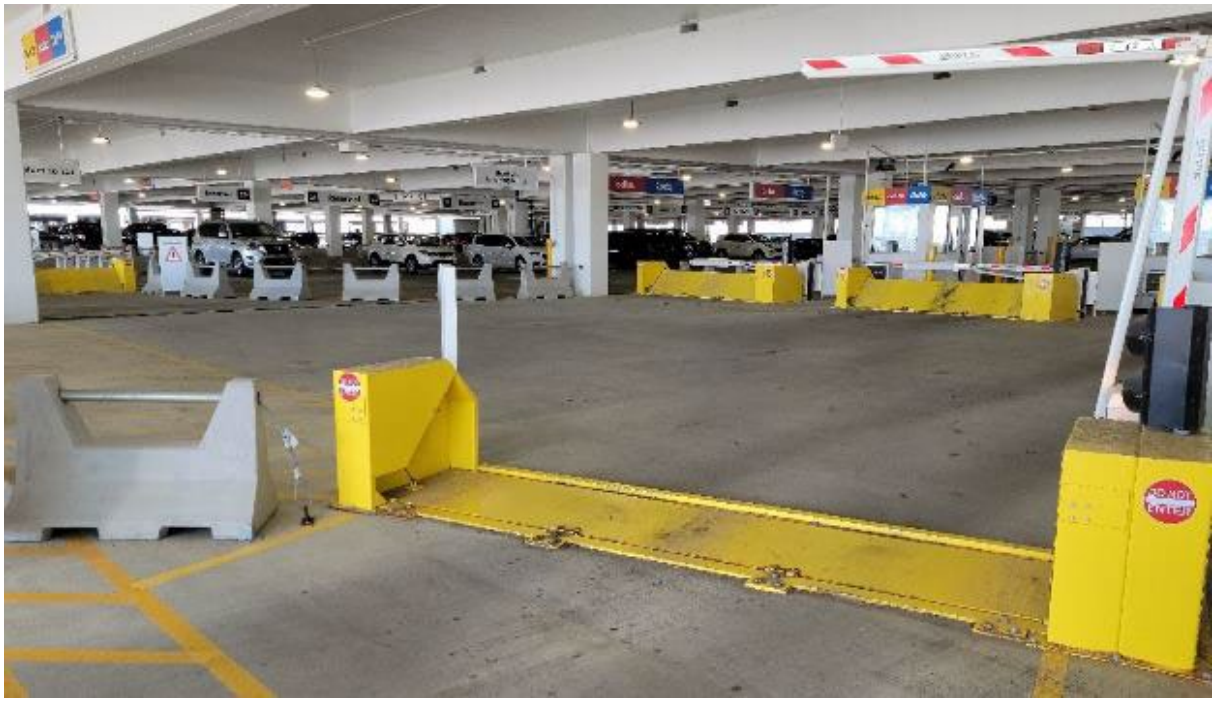
Figure A-12. GTC Traffic Zones

To make space for the GTC, a portion of the garage occupying the designated space was removed and a new roadway was added, which completely altered the flow of traffic around the airport. A common drive was added for non-rental cars to bypass the secured entrance into the return lanes if drivers

accidentally drive into the wrong exit. The common drive reduces the number of unauthorized vehicles in the secured space and reduces the number of calls for response to the airport police to open the access control barriers during off hours.

Some RAC operators created sally-port style exit lanes using plate and concrete barriers (Figure A-13). These exits provide several security benefits. First, criminals attempting to steal a vehicle will need to bypass twice the number of security barriers to exit the lot. This also offers a measure of redundancy if one of the barriers needs to be repaired. Additionally, the attendant in the exit booth is given greater control over security; drivers without appropriate rental agreements for the vehicle can be effectively diverted back to the ready/return area.

Figure A-13. Sally Port Exit



RAC EMPLOYEE TRAINING

In general, CVG's RAC employees are well trained to identify fraudulent activity. Most RAC operators use a driver's license reader to verify document authenticity. RAC employees are encouraged to call the airport police to verify a license if they are unsure of its authenticity. The airport police often share photos of suspects from recent rental crimes with RAC employees. The employees are also encouraged to notify law enforcement of suspicious activity and behaviors.

CVG police held monthly meetings with RAC site managers to discuss security concerns, including fraud. LEOs recommended asking the customers for tickets or itineraries to verify that they are passengers, and scrutinizing individuals without this documentation more carefully during the transaction.

At one time, the CVG police provided training to RAC employees, which included a presentation on red flag indicators and CCTV footage of suspicious activities. LEOs considered this to be an effective training activity. These training events and regular meetings are also excellent opportunities for the LEOs to meet RAC employees.

REPORTING MEASURES

RAC employees have a few options to notify airport security and police of incidents or suspicious activity. Primarily, RAC employees call 9-1-1 to reach the airport police; CVG uses geofencing to redirect any 9-1-1 calls on its campus to CVG dispatch. LEOs frequently patrol the CSB and can be dispatched quickly to the RAC counters to assist with ID verifications or other incidents when necessary.

Additionally, the CVG police initiated a group text between the LEOs and RAC site managers. This allows for mass notification of incidents occurring in the CSB or GTC. Many individuals using fraudulent IDs to attempt to rent a vehicle will repeat this scheme, visiting each RAC operator until an agent accepts the ID. The text group allows RAC site managers to quickly warn the other site managers of this activity and notify LEOs to respond at the same time.

MSP Existing and New Consolidated RAC Facilities

Minneapolis–St. Paul International Airport (MSP) has two consolidated RAC facilities:

- Terminal 2 (T2) RAC facility opened in 2001 as one of the first consolidated RAC facilities in the country. It is located on the south side of the airport. T2's QTA is in a separate facility nearby.
- Terminal 1 (T1) RAC facility opened in 2020. It is located on the east side of the airport in the new Silver Ramp facility. T1's QTA is within the Silver Ramp facility, but is separated from the RAC facility.

The T2 RAC facility experienced several security and auto theft incidents culminating in nearly forty attempted vehicle thefts in 2018. MSP retrofitted the T2 facility with physical security enhancements and incorporated physical, technical, and security design enhancements into the Silver Ramp facility and both QTA facilities. As a result of these enhancements, MSP has experienced a significant drop in overall vehicle theft attempts; only nine attempts were made at both RAC facilities in 2022.

THE T2 CONSOLIDATED RAC FACILITY

The T2 RAC facility (Figure A-14) faced several challenges before the final improvements were completed in 2020 and the QTA improvements were completed in 2022. The facility relied heavily on traffic spikes and arm barriers to control vehicle egress, but poor maintenance of the spikes often rendered them vulnerable or inoperable. As a standalone security measure at the facility entrances, the spikes could be easily thwarted. In some areas, the poor placement of physical barriers allowed vehicles to breach the facility. The QTA was especially vulnerable due to the lack of physical security to restrict vehicular and pedestrian access. Additionally, the RAC facility and QTA both lacked adequate security officers to act as visible deterrence, especially during overnight hours. These factors, paired with RAC operators leaving keys in vehicles for customer convenience, left vehicles highly vulnerable to theft. In some cases, RAC employees used the knowledge of the facilities' vulnerabilities to aid or commit theft of vehicles.

Figure A-14. T2 Consolidated RAC Facility

Source: Google Maps

To reduce the number of vehicle thefts and enhance the security of the T2 facility, MSP worked with RAC operators to cooperatively identify security improvement projects. MSP agreed to install physical equipment such as plate barriers, concrete barriers, guard rails, fencing, concrete work and curbing, gate arms, in-ground detectors, controllers, cameras, and automatic vehicle identification readers. RAC operators provided temporary barriers and contract security to staff the egress lanes while the permanent enhancements were installed.

Figure A-15. Physical Access Control at Egress Portals

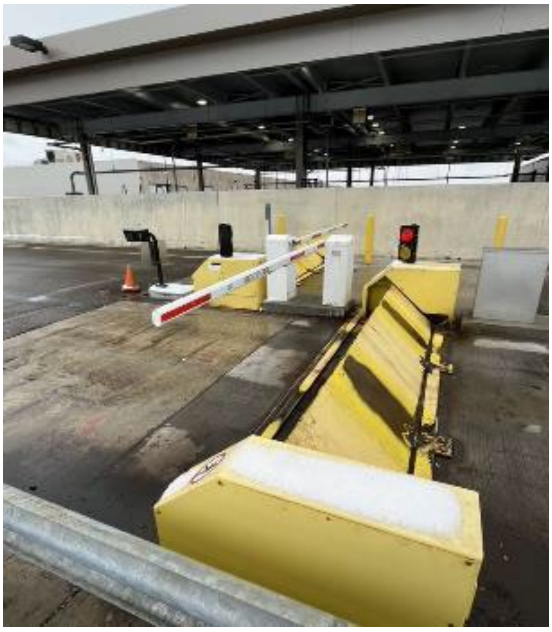


Plate barriers coupled with gate arms and access control (Figure A-15) were installed at the QTA and between RAC operator spaces to enable RAC employees to safely move vehicles while preventing unauthorized access to certain areas. The plate barriers replaced the traffic spikes. The same physical measures were added to the customer exits.

Perimeter fencing was added to restrict pedestrian access to the QTA. A steel crash barrier was installed on the inside of the fence to prevent attempts to ram through the barrier (Figure A-16). A one-way, full height pedestrian turnstile was installed in the fencing to allow RAC employees to exit the QTA (Figure A-17).

Figure A-16. Perimeter Fencing

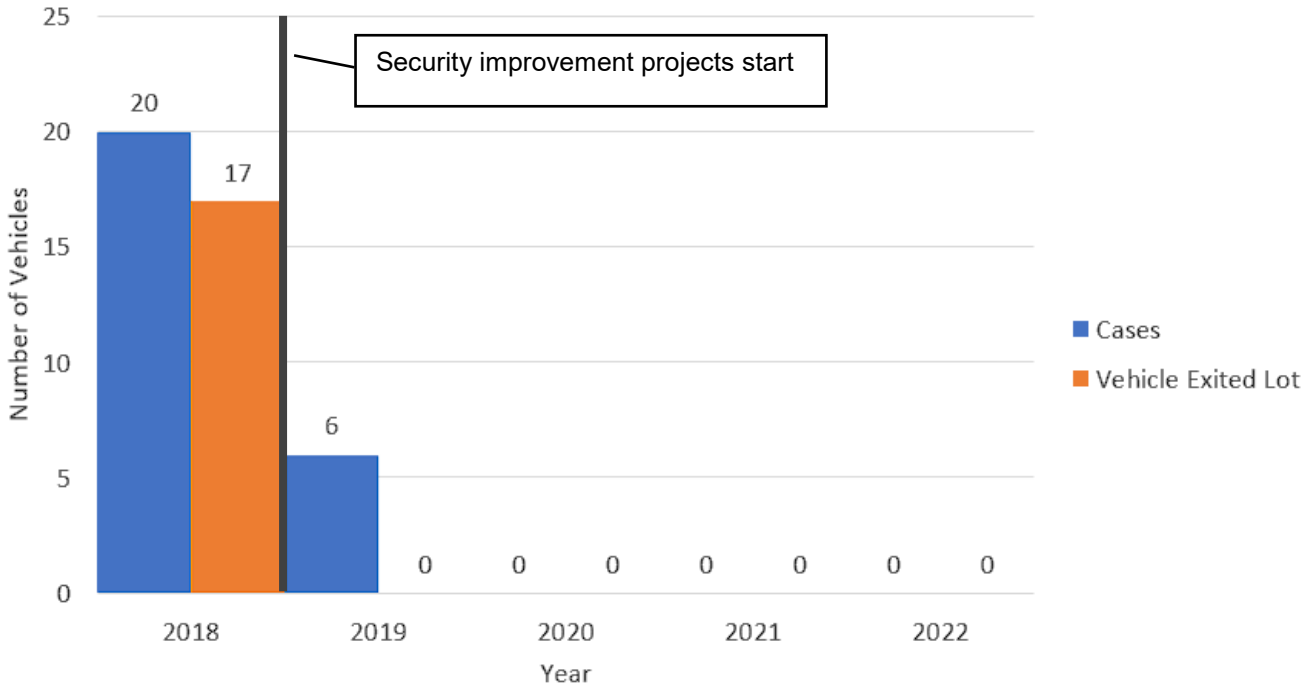
Figure A-17. Full Height Pedestrian Turnstile in Fencing

Figure A-18 shows the decrease in auto theft attempts at the T2 RAC lot after the airport began adding security enhancements. The three successful attempts in 2021 were the result of an incident in which a sacrificial vehicle crashed through the exit plaza and allowed multiple vehicles to exit.

Figure A-18. Attempted Auto Thefts at the T2 RAC Facility

Security improvements and enhancements at the T2 QTA began in 2019. As shown in Figure A-19, the QTA saw an immediate reduction in auto theft attempts and no successful attempts since.

Figure A-19. Attempted Auto Thefts at the T2 QTA Facility



THE SILVER RAMP FACILITY (T1)

Several of the lessons learned from the T2 facility were considered when building the Silver Ramp facility (Figure A-20). The structure is large, which makes it difficult to secure completely, and several security enhancements had to be added during and after construction as vulnerabilities were identified.

Figure A-20. T1 Silver Ramp Facility

Source: Google Maps

Plate barriers, lighted gate arms, anchored concrete barriers, cameras, and staffed guard booths were added to all customer exits (Figure A-21). The airport added in-ground detectors, controllers, cameras, and automated vehicle identification readers to all egress points. Access control measures were added to access points leading to the QTA.

Concrete barriers were added strategically throughout the RAC facility to create vehicle lanes and limit unauthorized movements. Some barriers near the exits are equipped with cameras aimed at the vehicle bumper to capture license plates (Figure A-22). Concrete barriers with steel guardrails are used to create restrictive access and movement of vehicles as well as intuitive lanes for customers (Figure A-23).

Figure A-21. Customer Exit Physical Security

Figure A-22. Concrete Barrier with License Plate Camera

Figure A-23. Steel Guardrails Affixed to Concrete Barriers

Crash-rated perimeter fencing was added around the facility. A fire lane was required for the QTA, so a crash-rated slide gate was also added for first responder access (Figure A-24).

Emergency duress buttons are scattered throughout the public areas of the facility. These are placed in well-trafficked areas and lit with a blue light so they are easily located. When pressed, the control center is notified to pull up the cameras and send a response.

Figures A-25 and A-26 show the drastic decrease in successful auto theft attempts at the RAC facility and QTA after the RAC operators officially moved into the facility in 2020.

Figure A-24. Fire Lane Slide Gate

Figure A-25. Attempted Thefts at the T1 RAC Facility

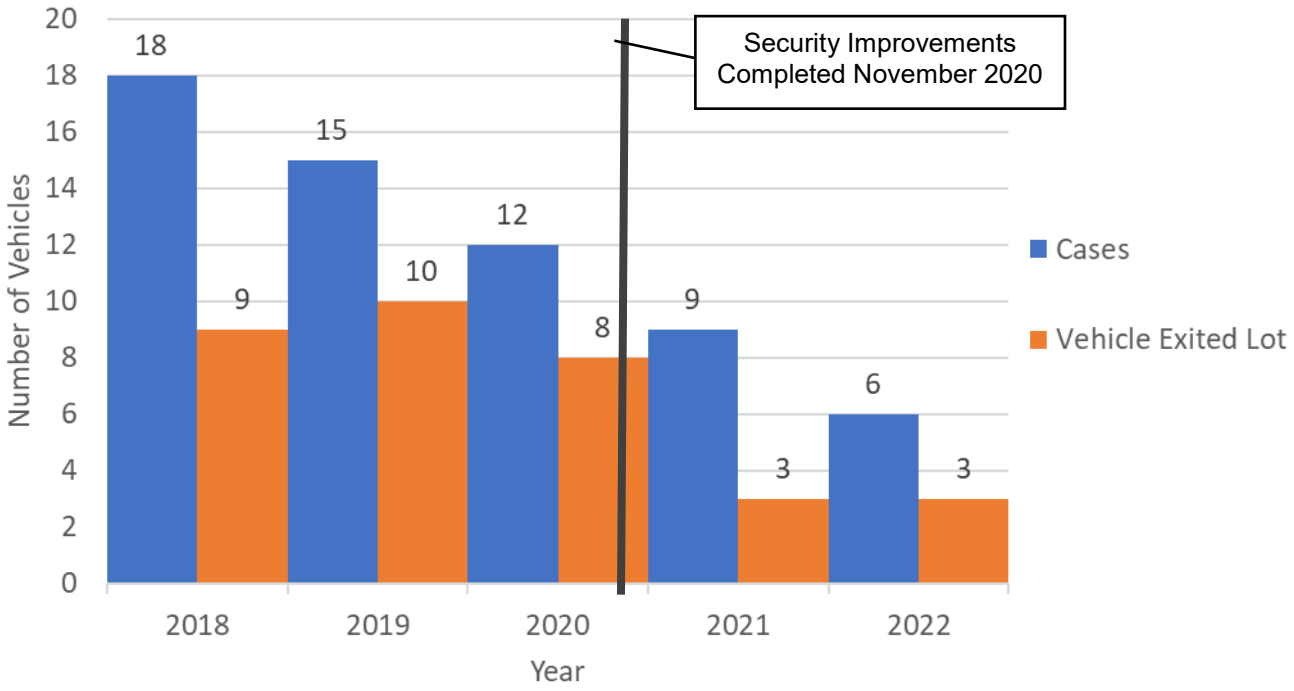
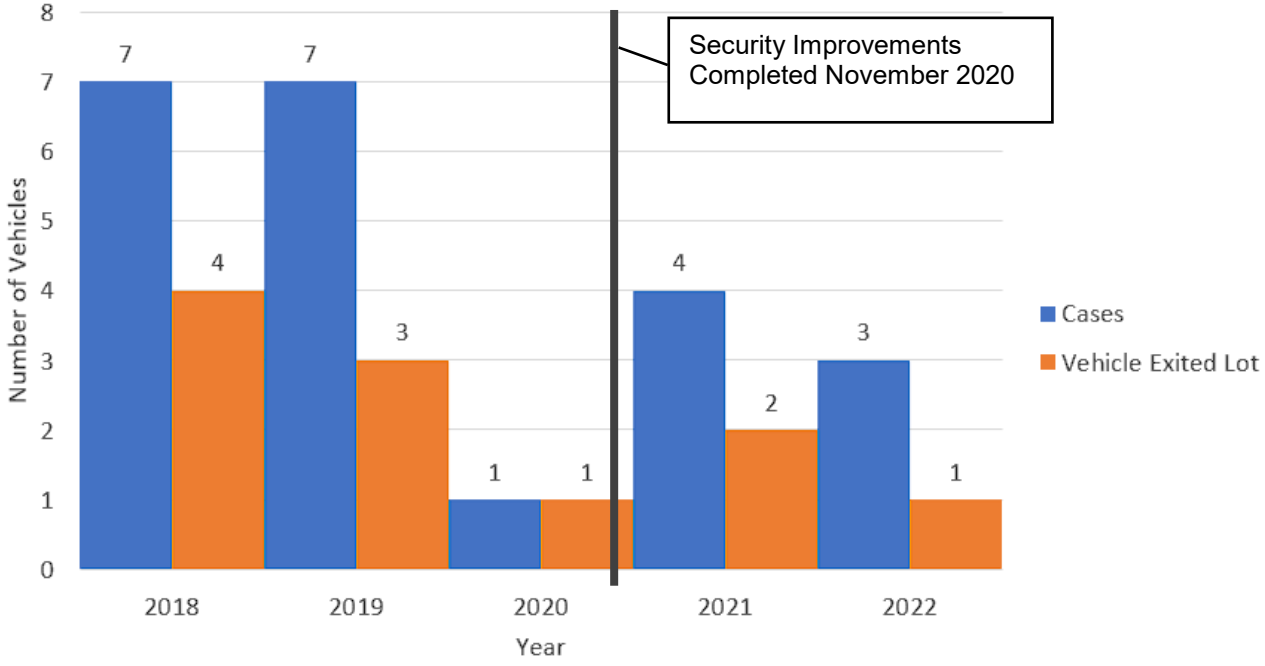


Figure A-26. Attempted Thefts at the T1 QTA Facility



FUTURE IMPROVEMENTS

MSP is continuously looking for measures to further limit vehicle theft at both consolidated RAC facilities. The airport has two projects planned to support this effort.

The first project is to install a full height pedestrian exit turnstile at the Silver Ramp QTA. The fence is currently framed and ready for the turnstile (Figure A-27).

The second project is to create an inventory of key components for the plate barriers. It is typical for parts of the barrier to be damaged when a vehicle crashes into the plate barrier. A strategic inventory of components most commonly damaged during a crash will enable MSP to quickly redeploy the barrier, restoring the physical protective measures of the facility.

Figure A-27. Fence Prepped for Full Height Pedestrian Turnstile