PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0005 October 2016

# Airport Perimeter Breach Classification and Post-Incident Best Practices

**National Safe Skies Alliance, Inc.**

Sponsored by the Federal Aviation Administration

**Ray Garza**
**Trenton Higareda**
CTI Consulting
Gaithersburg, MD

**Dave Fleet**
**Harold Flamenbaum**
Faith Group, LLC
St. Louis, MO



**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 Airport Security Systems Integrated Support Testing (ASSIST) 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 Program for Applied Research in Airport Security (PARAS), 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 for 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 Special Programs Manager*

### PARAS 0005 PROJECT PANEL

**Alan Black** *Dallas/Fort Worth International Airport*
**Colleen Chamberlain** *American Association of Airport Executives*
**Sean Cusson** *Airports Council International – North America*
**Chris Haas** *Oakland International Airport*
**Renee Hendricks** *Ex Officio, Federal Aviation Administration*
**Eric Thacker** *Airlines for America*

# CONTENTS

## SUMMARY

CTI Consulting and Faith Group conducted this research project, on behalf of the National Safe Skies Alliance's Program for Applied Research in Airport Security (PARAS), to develop a guide for all FAR Part 139 airport operators in their efforts to address perimeter security breaches; identify and use best practices to optimize those efforts; and, based on incident consequence, be able to identify the level of severity of any given perimeter breach. Specifically, the project developed a consequence-based classification model for perimeter security breaches that can differentiate the severity and risk of these breaches and enable airports to accurately convey internally, to the public, and to the news media, the severity and types of breaches that occur at their facilities.

This guidance document also provides two main areas of best practices for post-breach activities. The first is the management of activities subsequent to the initial response, including follow-up incident analysis and other processes and stages. The second area focuses on best practices for the prevention of re-occurrences of these types and/or locations of these incidents. The selection of appropriate best practices in this guide must be based on their suitability for airports' respective needs due to such variant characteristics as airport size, configurations, airfield operations, boundaries, environs, available resources, and budgetary considerations.

# SECTION 1: Introduction

CTI Consulting (CTI) and Faith Group conducted a study on behalf of National Safe Skies Alliance (Safe Skies), which included the development of a classification system for perimeter breaches based on their impact and severity. This classification system serves as a guide for airports to assign a category to each breach based on the consequences of the specific incident and, accordingly, be able to use that categorization for efficient response and remediation. This classification system, which will be voluntary, seeks to assist Part 139 airports of all sizes and configurations.

This project also called for a guide to identify best practices developed and used by airports in their management of post-incident activities and the subsequent identification and application of various breach prevention measures and strategies.

## 1.1 Statement of the Problem

A great deal of independent findings and documents are available in the security and aviation industries regarding perimeter breach history, management, and prevention. However, there is no single document that combines this information with a classification system based on severity of consequences to improve real-time responses.

Aviation security professionals throughout the country frequently meet at conferences and other forums (including industry organizations such as AAAE and ACI-NA[1]), share ideas and concerns through formal and informal networks, and research perimeter security issues independently or through consultants. However, the meeting minutes, reference documents, and reports that discuss historical information, best practices, policies and procedures, physical security measures, and perimeter security technologies are sometimes dedicated to only certain breach aspects or types, particular airport sizes or configurations, or are only distributed or available to (or known by) a limited portion of the aviation and security industries.

Airports and aviation professionals do not have a single, up-to-date guidance and classification document that is based on recent airport events, current and upcoming perimeter security technologies, efficient incident management protocols, breach prevention strategies, and first-hand experience recommendations from airports of all sizes across the country.

## 1.2 Need for a Perimeter Breach Classification System

Without a perimeter breach classification system that is based on the severity of consequences of the breach (or the potential of the attempt), airports must independently assess and react/remediate every breach from scratch, based on their limited individual airport or regional histories. This can cost valuable time, personnel, physical resources, and, in some cases, reputations and levels of confidence if an incident is not handled in a fashion deemed prompt or adequate enough for public perception, particularly when compared across the national media. Without a classification system and quick-reference guide, it is difficult for airports to assess quickly and react consistently and uniformly across the country. A single-source breach classification document would meet this need, as long as the classification criteria are broadly acceptable to the aviation industry.

[1] **AAAE:** American Association of Airport Executives
**ACI-NA:** Airports Council International – North America

For broad acceptance by the aviation industry, the perimeter breach classification system must be tailored to the unique airport industry environment and regulations. The system should be based on data and experiences from actual airport perimeter breaches, and should account for airports' specific public safety and national security considerations. The system must also provide uniformity in the process for evaluating breaches, clearly define the protocol for classifying perimeter breaches, and provide the ability to classify an incident based on the consequences of the breach—and not on a possible, ultimate catastrophic scenario. A practical and credible classification system should mitigate confusion and misunderstanding, and instill a sense of confidence to the public, stakeholders, and the media. An appropriate classification system should also be scalable and granular so it can be used by airports of all sizes for every type of incident.

## 1.3 Need for Post-incident Management Best Practices

In addition to an airport's initial response, there are a number of activities, depending on the incident, that the airport should address immediately after the site is secured and there is no longer an urgent risk to the airport, personnel, or public. These activities include documentation of events, mitigation of damages, restoration of security, and offering necessary assurances to tenants, patrons, and the public. A failure to perform these tasks promptly or efficiently can cause unnecessary stress or instability in an airport's recovery from the breach. Having a reference to lessons learned and best practices—established and refined by others in the aviation industry—could provide invaluable information for addressing and resolving these incidents effectively while minimizing the impact on resources and reputation.

## 1.4 Need for Post-incident Breach Prevention Best Practices

Whether in response to a previous breach or as a general security measure, airports have always focused on perimeter breach prevention. As with the breach classification system and post-incident management practices, there have been committees, discussions, research, and communications on methods, technologies, and general best practices for preventing perimeter breaches. However, the body of information has not been put forth in a single document, and certainly not in a combined "one-stop" reference document with a classification system, post-incident management best practices, and breach prevention best practices.

While airports have become adept in dealing with the immediate vulnerability of perimeter breaches and in finding and removing the risk (i.e., the intruder), determining how to prevent future similar or different breaches in a cost-effective fashion is not as straightforward. Whether airport operators are remediating an existing risk, or being proactive to prevent a potential breach that has occurred at another airport or facility, the use of available current information and best practices from other aviation industry professionals can save valuable time, conserve resources, and increase success. Breach prevention best practices include coordinated discussion of stakeholders, policies and procedures, potential tactical and strategic solutions, physical security improvements and technologies, integration of systems for detection and response, and measures to mitigate risks.

## 1.5 Goals and Objectives

This project's goal was to produce a guide for the airport industry that provides a perimeter breach classification system and best practices for both post-incident management and perimeter breach prevention. The source data for the document was collected from historical incidents, recommendations, and best practices identified by airport personnel from airports of all sizes, classifications and configurations, and inputs from a variety of aviation security industry personnel.

The applicability of the guidelines is to enhance assessment and response to real-world incidents, improve remedial actions, allow categories of risk to be added to an airport's security program if desired, prevent future incidents, and provide best practices that assist airports in maintaining their reputation, economic stability, and general public sense of aviation security. The study findings and recommendations will provide security professionals with analyses of incidents, workable solutions to deficiencies, and a base document to support the application of perimeter breach solutions. As new and improved best practices are identified, and additional members of the airport community provide inputs, this classification system and best practices can be improved and updated.

## 1.6 Scope of the Study

The study is limited to security breaches through the airport perimeter fence, gates, and other barriers that result in accessing any part of the airfield, and the effects of these breaches on security of aircraft, assets, employees and other stakeholders, and the public. Breaches occurring through airport terminals or other secured buildings were not designated as part of this study and, therefore, were not addressed. However, some of the post-incident management of breaches discussed in this project may apply to non-perimeter fence/barrier breaches.

Information presented in this document is grouped into two areas. The first is the development of a security breach classification system. This system is based on airport areas deemed to be critical due to their assets, and also on the severity of the actual consequences of the breach.

The second area of the study is the identification of best practices for post-incident management. These best practices are based on lessons learned from airports regarding activities that were undertaken after the initial response to an incident. They include methods to address working with the news media, communicating with the public, and preventing further similar breaches.

## 1.7 Project Research Methodology

The research methodology for the project consisted of three basic strategies. The first was the study and review of practices, manuals, literature, media reports, articles and papers, plans and related regulatory requirements, government reports, and congressional hearings records regarding airport perimeter fence breaches. The second was the distribution of questionnaires to solicit input from airport operators on practical and acceptable types of breach classification systems, as well as best practices in the management of post-breach activities and breach prevention measures. The third involved conversations with airport professionals on the classification model and vetting of practices.

An additional factor is the experience of the CTI team members' work with airports over the past 30 years regarding perimeter security threat and vulnerability; tactical and technical preventative measures; design and implementation oversight of integrated technology systems; design and construction oversight of perimeter fencing, barriers, and gates; vetting of security procedures and measures at over 20 client airports; working with the Federal Aviation Administration (FAA) and Transportation Security Administration (TSA) on vulnerability and breach mitigation; and upgrading airport security programs (ASPs) based on target hardening needs. The team ensured that these best practices and lessons learned are still used by airports and other secured facilities.

## 1.8 Format of Report

The major parts of this report and guide document are divided into the following sections:

- General findings address what is happening with security breaches on a national level, including background information, past and current events, current trends and concerns, findings from media investigations, industry and government concerns, and examples of breaches over the past 15 years.
- Specific findings and conclusions describe how the general findings and conclusions impact the proposed breach classification system, the identification and implementation of recommended best practices for post-breach activity management, and implementation of breach prevention measures.

Appendices A and B contain, respectively, the Perimeter Breach Classification System and the Best Practices Guide for Management of Post-Incident Activities and Breach Prevention in a format that allows the readers to present this guidance independently of the other narratives included in this report.

# SECTION 2: General Findings and Conclusions

The following sections describe the general findings and conclusions related to the classification of breaches, and the best practices for managing post-incident actions and preventing subsequent breaches. They focus on the status of airport practices in dealing with perimeter breaches, and how breaches are currently covered in the media.

## 2.1 Security Breaches

An airport's physical security systems and programs become vital to the integrity of security areas, and the protection of the public, employees, and airport assets. The TSA and the airports' Airport Security Program (ASP) requirements regarding perimeter security must be met for an airport to be fully compliant in its security mission. Airport security professionals support airports in meeting this need through technology, innovative engineering solutions, sound security procedures, airfield enforcement programs, and proactive auditing programs of system usage. In mitigating the terrorist threat and the threat from others, they have assisted in developing target hardening strategies and maintaining regulatory compliance.

However, the security paradigm in today's environment is continuously evolving. Many threats that were once considered remote (e.g., armed attacks, use of improvised explosive devices, and active shooters) have moved to the forefront of security considerations. Measures that were once considered adequate are now, in many cases, deemed subpar. Security processes and countermeasures must be in place to safeguard facilities, operations, and personnel from criminal acts, natural emergencies, and acts of terrorism. Airports must adapt these processes and security technologies to meet the new challenges.

Airport operators must contend with regulatory changes, and perimeter breaches, both intentional and accidental, on a constant basis. The severity of each breach may range from a person merely in the wrong place at the wrong time, to sabotage of an aircraft, or a deliberate runway vehicle incursion. The consequences may range from minimal property damage to loss of life.

Specific to perimeter intrusions, it is the opinion of some security professionals that the actual intrusion (i.e., the penetration of the fence) is not a breach until the person penetrates the first level of security. The thought is that the fence is not intended to be a viable barrier for protecting the airport. In their opinion, it serves primarily as a reminder to a potential trespasser that the airport is protected property and they should not enter. The majority of airport professionals, however, hold the view that such an intrusion constitutes a breach, that the result may be significant, and the severity of the consequences should determine the appropriate category of the breach.

U.S. airports differ from each other in a variety of ways, including locations, their environs, and their inbuilt characteristics. Some may be located in urban areas, remote areas, industrial areas, adjacent to military bases, or may even be a dual commercial/military-use airport. They may have water boundaries or public roadways adjacent to or ending at right angles to the perimeter. Many airports in urban areas have sidewalks alongside the perimeter fence that may result in more spur-of-the-moment breaches. Airports also vary in the configuration of the airfield and the designations of Secured Areas and Air Operations Area (AOA). Some perimeters have fence lines in single digit miles, while others may have more than 30 miles of perimeter to be protected.

Airports adjacent to military bases, especially military recruit training facilities, may have more incidents of recruits jumping the perimeter fence to get to the terminals. Airports with public roadways may have more vehicle breaches at certain points where the roadways are in close proximity to fence

lines. Similarly, vehicle penetrations, due to reckless, inebriated, or police-pursued drivers, are more likely to occur where public roadways end or make a right-angle turn at a fence line. Many airports have public roadways that cross the airport and cannot be closed to the public. These roadways—which in some cases are major roadways—require fencing along the route, which may increase the vulnerability of airports' fence lines.

Airports with water boundaries have incidents of persons beaching their watercraft due to malfunctions or fuel issues. For practical reasons, these water boundaries may not have perimeter fencing or other barriers. In a similar vein, many airports have streams crossing through a portion of their airfield, often with barrier gates that have to be raised and lowered at certain times to clear them of debris. Some airports have cemeteries that, although they have an inner fence, have to be accessible to certain members of the public.

Security professionals admit that 100% protection against breaches is not possible. Raising the fence and enhancing the top guard[2] may not prevent a breach, and may only delay it by a few seconds or minutes, depending on the agility of the trespasser. Moreover, many airports have areas that are remote and do not have power connectivity for surveillance cameras and perimeter intrusion detection systems.

### 2.1.1 Importance of Perimeter Patrols

A Part 139 airport's use of perimeter and airfield patrol is an important element of its ASP. Perimeter patrol serves as a deterrent to breach attempts, allows identification of persons on the airfield who may have breached the perimeter, and enables inspection of the perimeter fence to locate where breaches occurred or were attempted. It is a common practice for perimeter patrol to be carried out by security personnel, law enforcement personnel (LEP), airport operations staff, maintenance staff, or any combination of these groups. In some airports, operations staff may carry out perimeter and airfield patrol duties, while in others, security staff and LEP are trained on and carry out some operations duties. CTI staff members have found airports where LEP are trained and certified as emergency medical technicians, and also trained in confined space rescue.

Airports are always seeking to optimize the patrol mission, and often use increased frequency, reconfiguration, and unpredictability of patrol tours in their efforts. The patrol of large airports may take several hours and require getting in and out of the vehicle to ensure perimeter integrity. In some cases where airports use fencing that allows a vehicle to breach under the fence, the fence may return to its normal position so that a breach may not be noticeable**.** In some cases, portions of perimeter fencing must be inspected from landside due to factors such as wetlands and wooded areas. Also, inspection of fencing around terminals and other busy areas where cargo containers and other equipment are parked may require patrol observation from landside. In some very small airports, LEPs are required to be present at the passenger screening checkpoint, to patrol inside the terminals, enforce the challenge program, monitor vehicles at terminal curbsides, and patrol the Secured Area, which leaves little time for accomplishing multiple perimeter patrols during an individual shift.

Airport security staff members agree that, where possible, the availability of video cameras at certain perimeter areas, and the use of video analytic systems, when monitored, are a tremendous force multiplier for the perimeter patrol program.

[2] **Top Guard:** the overhang of three or four strands of barbed wire along the top of a fence, commonly facing outward and upward at an angle of approximately 45 degrees.

## 2.2 Findings of Associated Press Study of 31 Airports

The Associated Press (AP) created a very comprehensive account of perimeter security breaches from January 2004 through January 2015, at the nation's 30 busiest airports, plus one more airport where a stowaway incident had occurred. The information about the 31 airports was obtained through public records requests, news archives, searches, and interviews.

The list of 268 breaches of the 31 airports in the study is indicative of perimeter breaches across the spectrum of the 450 commercial airports in this country. The types of intrusions are similar, as are the various types of locations, environs, natural boundaries, and intruders.

A review of the AP report revealed the commonality of the breaches among the airports. As noted above, the similarity in locations included urban or remote areas; proximity to military bases; and boundaries that include residential, commercial, industrial, wooded, and wetland areas, as well as bodies of water. None of these breaches included a terrorist attack. The majority of these incidents were what would be called "nuisance" breaches.

At least 44 times in those 268 breaches, intruders made it to runways, taxiways, or to gate areas where planes park to refuel or load passengers. In seven cases, they got to aircraft. Few airports revealed how long it took to apprehend suspects, saying this detail could show security vulnerabilities. The available information showed most arrests happened within 10 minutes.

It does not appear that there were many prosecutions of violators, or that there was a legal disposition of the violations. In the AP study, one of the airports had approximately 34 breaches during the 10 years, which seems like a lot; however, it amounts to less than 4 per year. Several other airports had incident counts in the 20s, and others in the teens or fewer. One airport had eight breaches in one year from the same man, who was mentally disturbed and managed to reach the stairs to an aircraft twice. Eight breaches by one person in a 1-year period indicates that there may not have been a serious judicial disposition for at least seven of the breaches. He was ultimately placed in a treatment facility by a court.

There were a number of breaches caused by intruders who crossed the airfield because it offered a shortcut to their jobs. It seems like a weak reason for committing the breach until one considers that these airports are enormous, and the intruder is cutting off additional miles of walking. These types of violations indicate that persons who commit them may not appreciate their seriousness and the risks present on an airfield. Other reasons for breaches actually involved persons trying to get to terminals by walking across the airfield. Similarly, there have been cases where drivers crash through a fence and try to drive across the airfield to get to the terminals. The report indicated only a few intrusions where a vehicle rammed manned gates to enter the airfield.

Airport perimeter breaches, unfortunately, are not uncommon. Intrusion through the perimeter fence is probably the easiest way for an unauthorized person to access the airfield. Moreover, a top guard of barbed or razor ribbon wire cannot keep all persons from scaling the fence. In remote areas, persons can bring ladders or other climbing aids to facilitate access. Making the fence higher or adding a top guard would only slow down a person, and not necessarily stop an intruder.

### 2.2.1 Issue of Stowaways

There have been two stowaway incidents in the past 6 years where the transgressors hid in the wheel wells of the planes (indicating that they most likely accessed the planes via the perimeter fence). One incident was in 2010 where the stowaway died, and another in 2014 where the person survived.

Although these incidents may not have presented a security risk to the aircraft, a stowaway could pose a risk to the landing gear or plane overall. The result of this type of incident is the loss of public confidence in the airport's ability to secure the facility and the aircraft—if a person can hide in the wheel well, malicious devices can potentially be hidden in the same location.

A concern about these two incidents is that the persons got into the terminal ramp/apron area, went under the aircraft, and then climbed into the wheel well without anyone noticing these actions. One of these persons was 15 years old. Terminal ramps/aprons are very busy places, with tight timelines for servicing the aircraft, and ramp workers taking heed of all the moving parts and hazards in their work areas. Still, these employees and aircrews conducting preflight aircraft inspections need to be aware of potential stowaways, as they are the last line of defense once intruders enter the terminal ramp/apron area.

### 2.2.2 Focusing on Specific Areas

Focusing on the use of protective measures at specific vulnerable areas of the perimeter, rather than the whole perimeter, is more feasible for airports. The best practices of airports are often contingent on the nature of the vulnerability that needs to be addressed. Airports look at their most vulnerable areas and use the most cost-effective measures to deal with those sites. For example, in the case of vehicle penetrations of the perimeter, if a public roadway ends or makes a sharp turn at the point it meets the perimeter, guard rails or pre-cast concrete barriers (similar to jersey barriers) at that point may be needed to prevent accidental or intentional penetration of the fence. Speed bumps may also be used to reduce the speed of vehicles approaching the perimeter.

## 2.3 Categorization of Breach Incidents

Airports know from experience that the majority of perimeter breaches are more of a nuisance than a threat against planes, passengers, or assets critical to the operation of the airport. Moreover, even when intruders have intended to go near the aircraft, they do not have the capability to attack, sabotage, or hijack an aircraft. There were no terrorist plots discovered nor attacks carried out in any of the 268 breaches noted in the AP study or the over 1,300 breaches of all airports from 2001 to 2011 listed in the publically available TSA report.

A major concern of the airport community, however, is that the public, and perhaps the media, may not know that most of these intrusions pose a minor risk to the airports, and have not resulted in severe consequences to persons or assets. What is needed, therefore, is a classification system through which the airports can assess breach incidents and categorize them based, not necessarily on all the possible eventualities stemming from the breach, but on the actual results of the breach. The severity of the consequences of a breach is very important as a criterion. Otherwise, every person who scaled a perimeter fence could be deemed as capable of accessing a parked aircraft and flying it across the country.

Circumstances surrounding breach incidents raise many questions. If a person or persons armed and intent on attacking an aircraft were stopped and arrested upon entering the airfield, should the lack of severe consequences categorize the breach at the lower end of the scale? In another example, if a person with no malintent accesses a plane, but is discovered and detained, and subsequently determined to lack the capability to do harm or damage, is the incident classified at a lower severity, and if so, by how much? An effective classification system should take these and many other factors into consideration.

If a classification system is objective, transparent, and based on sound criteria, it is more likely to be accepted by the public as a fair evaluation of perimeter breach incidents. Still, the key point is that the affected airport has to make the judgment as to the classification of a breach. The airport staff and stakeholders know the airport better than anyone else. They know the configuration and layout of the airport, the environs and potential security hazards, designated Secured Areas and AOAs, aircraft movement areas, non-movement areas, assets, and overall airport operations. They also know vulnerable perimeter areas, open areas with no camera coverage, time and distance between various points around the airfield, pathways to critical areas and important assets, and the day-to-day operational routines. These factors underline the need for the airports to determine the classification assessments.

## 2.4 Best Practices for Post-Breach Management Activities

There are various practices in dealing with the different types of breaches with various levels of severity, intent, capability, and characteristics of the intruders. The initial response—securing the perimeter and any related vulnerabilities—is only one part of the overall response and analysis of the breach. Depending on the severity and complexity of the breach, there may be a great deal of follow-up work to ensure that the airport identifies the basics of the breach (the who, what, where, when, why, and how of the incident) and determines what short- and long-term security solutions can be implemented. Some incidents will be very basic, and extensive follow-up actions may not be necessary.

Since there are many types of breaches, inherent factors, and severity levels, it is very difficult to deal with all the possible best practices for all the breaches and every type of circumstance. This guide will provide a comprehensive menu of practices that can be applied to deal with any type of incident. This list can provide viable options for best practices for the breach review group.

## 2.5 Breach Prevention Best Practices

The whole airfield security program is based on the mandate: *The perimeter must be protected at all times.* The airport security plan lays out the baseline for perimeter security, and provides the requirements for perimeter fences, the need for frequent patrols, and challenge/escorts programs. As described in the *New York Daily News*' report of the 2015 AP study, "The TSA said that from 2010 through 2014, it issued $277,155 in fines for 136 breaches."[3] While many incidents were non-threatening, other intruders posed greater dangers. Some airport officials assert that perimeters are secured and that an intruder being caught is proof that their system works. Others have said that it is neither financially nor physically possible to keep all intruders out, and that there are no fences that cannot be penetrated.

The TSA stresses the fact that the most vital part of the airport is the aircraft, as the 9/11 attacks have demonstrated. Thus, a perimeter breach close to parked aircraft is more serious than a similar intrusion in a remote part of the airport. The lesson learned is that perimeter breaches cannot be prevented with 100% certainty. Therefore, airports constantly search for the most effective ways to reduce breaches through deterrence, enhanced security measures, security training and awareness programs, and policies and procedures.

All airports, regardless of size, have these three basic elements of a security plan: a challenge program that requires all employees to question suspicious persons on the airfield or notify security of the

[3] AP, 9 April 2015

person's presence; a program for inspections and patrol of the perimeter and other areas of the airport; and a camera system, no matter how small, to monitor important areas of the airport.

Use of camera surveillance is relatively inexpensive when compared to other more expansive and expensive technologies, and is a very effective force multiplier for airports. These systems were praised by respondents to this project's questionnaire who said that they are critical in identifying breaches and unauthorized persons, and are used whenever possible for critical and/or vulnerable areas. Unfortunately, the miles of airport perimeters and the amount of large open spaces inside the perimeter often preclude the expansion of surveillance programs to cover all these areas. The costs of installing and maintaining large surveillance systems, lighting, and power connectivity, impede comprehensive camera coverage for an entire perimeter and remote areas.

Best practices for prevention or mitigation of breaches focus on three main security areas: policies and procedures, physical security measures, and security technology systems.

### 2.5.1 Policies and Procedures

Policies and procedures are important because they provide the framework for the security program and are the base for physical and technology security. The elements covered by the policies and procedures include the following:

- Patrol supported by security, LEP, operations, maintenance, other departments and stakeholders
- Search procedures for locating reported trespassers
- Challenge procedures and programs
- Security training of stakeholders
- Security awareness programs for stakeholders
- Reward programs for discovering breach suspects
- Use of community groups to assist with patrol of perimeter and public observation venues
- Security signage
- Name/nomenclature for areas of the perimeter
- Clear zones for perimeter, inner/outer perimeter roads

All breach prevention security measures are important; however, two programs stand out among these: perimeter patrol and inspection, and the challenge program.

#### 2.5.1.1 Perimeter Patrol Program

The perimeter patrol program is carried out for several reasons. One is to help in deterring persons from trespassing; another is the possibility of catching an intruder; and a third (and very critical) reason is the inspection of the fence to assess its condition, discern if certain intrusions such as those involving vehicles have occurred, and determine whether the fence has been damaged. Law enforcement patrols are also a key part of this effort. In some airports, it is solely airport LEP who perform the patrol function. Whether conducted by security, law enforcement, operations, and/or other units, patrols are important to airports' breach prevention programs.

Commonly, airports have a baseline for the number of perimeter patrols per 24-hour period, which are documented in a log. At times, the airport may not achieve their patrol goals, but generally they try to stay on schedule. The times of the patrol tours are often varied to eliminate predictability. One of the most common security solutions used after a perimeter breach is enhancement or increase in the number of perimeter patrols, or a greater focus on certain locations at issue. The greatest hindrance to better

patrols is the lack of staff, so airports' patrol programs often include the assistance of other entities such as law enforcement, operations, maintenance staff, and TSA.

#### 2.5.1.2 Challenge Program

The challenge program at airports is a very important part of the perimeter protection program; once an intruder enters the AOA, the designated Secured Area, or the terminal ramp/apron area, airport employees play a critical role in discerning unauthorized persons and challenging them or notifying security. For this reason, and due to regulatory requirements, all airports establish challenge programs as directed in their ASP, and train employees on the procedures and the importance of challenging. Airport badge holders are trained as part of the security identification display area training program, and through continuous challenge awareness programs. Many airports also establish reward programs to encourage employees to challenge persons who are not properly displaying an identification badge or do not seem to belong in the airfield. These reward programs, operating under various names, have been successful in encouraging employee vigilance. Some of the airports publicize the cash award to promote participation by all employees. Another program involves sending persons without badges to see if they are challenged, and then writing up employees who failed to challenge the decoys.

### 2.5.2 Physical Security Measures

Physical security measures include gates, locks, high-security fencing, guards, crash-resistant barriers, buried and embedded fencing, anti-penetration cable, closing or re-routing of public roadways, speed bumps, gate arresting cable, sally port gates, simple motion sensors at vehicle gates that will annunciate when a pedestrian walks through, and even convex security mirrors that allow guards to see the blind side of a truck being processed at a gate.

Two other factors that assist in preventing trespassing are warning signs and clear zones required on either side of the fence. Although not always a deterrence, for some people, the no trespassing signs and the potential risk of exposure in clear zones are sufficient to stop them from breaching the perimeter fence.

Lighting is also an asset for perimeter security. Unfortunately, the cost of implementing electrical power and lighting for an entire perimeter can be prohibitive for individual airports. This means that the airports prioritize perimeter lighting for areas that are most critical and vulnerable whenever possible, especially areas close to the terminal ramp/apron.

A drop-arm gate with an arresting cable just inside a busy vehicle gate might allow the guards to leave the rolling gate open and thereby process the vehicles faster and expedite the air carriers' operations. Also, speed bumps at vulnerable gates, where vehicles can build up ramming speed, present an effective security measure.

At locations where the fence is at risk from an adjacent public roadway, arresting cable threaded through fencing at the proper height can stop a ramming truck or automobile, and at the same time provide a life-saving measure to occupants.

### 2.5.3 Security Technologies

Security technologies for preventing breaches vary among airports regarding which systems are used, how they are integrated, the amount of area or perimeter covered, system age, life cycle stage, deployment, and efficiency. Cost and budgetary issues are major factors in determining which systems

an airport buys and uses. Although the systems may be expensive, their capabilities in detecting intrusions and intruders on a 24/7 basis is a great aid to the airports. The following technology types comprise the systems that airports utilize. Detailed descriptions of the systems are found in Appendix B.

- Closed Circuit Television (CCTV) camera coverage
- Video analytics
- Sensor wires/cables/contacts on fence or in-ground
- Microwave sensors
- Radar intrusion detection
- Automated gate barriers
- Solar power panels
- Integrated systems that include combinations of fence hardening measures, such as sensor wire/cable intrusion detection systems, microwave, video analytics, or thermal imaging video

# SECTION 3: Specific Findings, Conclusions, and Recommendations

The following are the principles, categories, methodologies, and factors involved in the proposed breach classification system. The information in this section is repeated in Appendices A and B for ease of reference.

## 3.1 Classification of Security Breaches

The following describes the perimeter fence and gate breaches classification model developed for use by airport operators who will categorize their airports' breach incidents based on the facts and actual consequences of the incident. Since the airports vary in configuration, operation, designation of secured, movement, and non-movement areas Security Identification Display Area (SIDA), and AOA, the airport operator is best able to factor in all the variables and the consequences of the incident and determine its rating.

### 3.1.1 Underlying Principles

This system is intended for classifying perimeter breach incidents only, and is based on the following principles:

- The system model contains categories designated as 1 to 5, with category 5 being a breach with the most severe consequences, and category 1 having the least severe incidents.
- Each incident should be evaluated for severity based on the consequence of the incident, and not on what may possibly have occurred.
- Passenger aircraft are the most critical asset of an airport and require the greatest protection. For this reason, the non-movement area, (i.e., the terminal ramp/apron where aircraft load and unload passengers and baggage) becomes the airport's most critical area.
- Aircraft in the terminal ramp/apron area, whether they are operational or not, must be protected from the vulnerability to immediate or delayed sabotage, the placement of weapons in the aircraft, or other actions that may result in a hijacking.
- Cargo, charter, and hardstand-parked aircraft based in the terminal ramp/apron are deemed a higher criticality than those based outside the ramp/apron.
- A combination of factors such as violator intent, time in unauthorized area, observation of trespasser, detainment, trespasser mental capacity and capabilities, location of unauthorized access, and consequence of breach should be considered in determining the appropriate category.
- Individual airports should determine the amount of increase or decrease of category level based on situational factors.
- Flexibility in using the model is essential, and airports may adapt the model to suit their respective needs.

### 3.1.2 Factors in Designating Categories

The following factors will affect and determine the categories for perimeter breach incidents:

- Perimeter breach incidents resulting in aircraft passengers being successfully attacked, hijacked, or sabotaged will be classified as category 5, absent other possible mitigating factors.
- In cases where persons are injured, shots are fired, explosives detonated, or vehicles are used to attack aircraft with passengers anywhere in the airport, the severity of the incident should be raised.

- The immediate or reasonably quick apprehension of trespassers reduces the severity of the incident in any area.
- Identification and observation of an intruder by stakeholders until the person is apprehended or otherwise detained reduces the severity of an incident.
- Breaches resulting in access to other airfield areas, exclusive of movement areas, by persons with clear, non-malevolent intent reduces the classification category.
- Intruding persons and vehicles in the proximity of, but not on, active runways, taxiways, and their access ramps reduces the severity.
- The severity of an incident based on the length of time before an intruder is discovered is contingent on criminal intent, location, capability and opportunity to do damage to persons and assets, and other factors discovered by post-incident investigation.

### 3.1.3 Classification System Category Criteria

The following is the classification system and the individual category criteria that provide guidance on the process of classifying perimeter breaches according to their actual consequences. Each category definition includes a general description followed by a list of potential examples to be used in the classification process.

**Category 5:** Addresses intentional criminal actions that include successful attacks, sabotage, or hijacking of a passenger aircraft in the critical terminal ramp/apron area; it may also include cargo or charter aircraft and hardstand-parked planes in the critical area.

Examples of this category may include:

- Any perimeter breach that results in a successful attack, sabotage, or hijacking from within the critical terminal ramp/apron area.
- Incidents where persons are injured, shots are fired, or explosives detonated, even if the attack of aircraft failed.
- Similar successful attacks of passenger aircraft in the process of taking off, landing, or taxiing to and from the runways.

**Category 4:** Addresses intentional criminal actions that include unsuccessful attempts to attack, sabotage, or hijack passenger aircraft in the terminal ramp/apron, and those landing, taking off, or taxiing to or from the runways. It also addresses successful attacks on assets that if sabotaged could affect essential air and ground operations.

Examples of this category may include:

- Unauthorized access to the terminal ramp/apron area that results in an unsuccessful attempt to attack, sabotage, or hijack a passenger, cargo, or charter aircraft in that area.
- Unsuccessful attempts to attack passenger aircraft landing, taking off, or taxiing to or from the runways.
- Successful attacks, sabotage, and other intentional destructive acts against assets that may affect essential flight or ground operations, such as fuel farms, heating and cooling utilities, power utilities, fuel lines and hydrants, fire stations and fire personnel, and other facilities deemed important by the airport. *An unsuccessful attack on these critical assets would lower the event to a category 3 or lower depending on the progress of the attack effort when it was prevented.*

**Category 3:** Addresses criminal intent that results in successful attacks, sabotage, or damage to non-essential assets and buildings whose damage or destruction would not disrupt airport air or ground operations.

Examples of this category may include:

- Successful attacks, sabotage, or damage to non-essential assets and buildings whose damage, although costly, would not disrupt airport air or ground operations.
- Theft of expensive materials and equipment.
- Incursions on active runways and taxiways where the incursion from breach vehicles or pedestrians momentarily affect the flight operations of landed aircraft or aircraft intending to land or take off. These incidents would include vehicles evading pursuit that may endanger aircraft and passengers.

*An incident should be included in category 2 or 1 when areas containing these assets are accessed by unauthorized persons who lacked criminal intent, did not cause damage or injury, were quickly arrested or were observed until detained, or did not have the ability or capability to do harm to persons or assets.*

**Category 2:** Addresses breaches by persons who intentionally trespass through the perimeter fence with clear intent of committing criminal, terrorist, or other serious malevolent acts, but who are prevented by immediate detainment or who were observed and monitored throughout their presence before being detained.

Examples of this category may include:

- Remote areas where perimeter breaches are made by persons with intent to attack, sabotage, or hijack aircraft or other significant assets, and who are in possession of weapons and/or explosive devices, but who are intercepted/apprehended before reaching those assets.

**Category 1:** Addresses persons who accessed, or attempted to access, areas on the airfield with or without bad intentions, and who were detained before committing a more serious violation.

Examples of this category may include trespassers who:

- Accessed the critical terminal ramp/apron or other secured locations, but could not or did not commit a greater violation before apprehension.
- Did not have the intent, opportunity, mental capacity, capability, or time to commit a greater violation.
- Had intention of commiting a criminal act such as theft or vandalism, but were apprehended before commiting that act.
- Accidentally breached the perimeter fence in a vehicle (e.g. were lost, confused, or intoxicated).
- Progressed into a critical or other security area, but was under observation.

## 3.2 Best Practices in Management of Post-Incident Activities

A number of activities need to be carried out subsequent to the immediate response to a perimeter breach. In certain cases and depending on the type, severity, and factors of the incident, the security staff or a small group of security staff and other employees may undertake these activities. The following are the stages, phases, and best practices in the management of post-breach incidents.

- Ensure that the breach site and/or the existing vulnerability is secured. These actions will be dependent on the type of breach and the status of the perimeter fence or gate.
- Search for and find the intruder if he or she has not been yet detained.
- Identify and interview witnesses for descriptions, numbers of intruders, accounts of what occurred, areas accessed, identification/verification of the intruder if necessary, and other relevant information.
- Question the intruder; run a National Crime Information Center (NCIC) check
- Determine access to critical areas, the depth of the access, and any critical assets reached.
- Determine the intent of the intruder.
- Decide if intruder will be charged and, if so, ensure LEPs have the necessary information for the charges, to include comments and declarations made by the intruder.
- Identify short-term solution(s) for the vulnerability.
- Determine category of breach per the classification system for media and stakeholder dissemination.
- Notify appropriate airport stakeholders.
- Prepare to brief and assist the public information spokesperson with key information on the incident, and to ensure the protection of Sensitive Security Information (SSI).
- Identify, if necessary, preventative policies and procedures, physical security, and/or technology actions that will address the breach.
- Conduct a “hot wash” meeting of security, law enforcement, persons involved in the incident, and stakeholders who will be involved in follow-up meetings. Analyze breach factors, including method of intrusion; consequence of the breach; response and investigation by the airport; questioning of the intruder; other interviews conducted; methods of improving handling of the incident; whether additional changes to the perimeter, policy and procedures, physical security, or technology are needed; and if further meetings to discuss and plan for those changes are necessary.
- Monitor category of breach for changes in classification for media and stakeholder dissemination
- Hold a meeting of the breach review group to address the breach incident and its result, response and other actions of the airport; decide if changes in response protocols and practices are needed; and identify the most practical and cost-effective preventative measures
- Identify possible long range solutions for this type of breach for consideration by the breach review group.
- Ensure that airport staff knows that interviews and information dissemination are centralized in the airport owner’s designated public information spokesperson, and that inquiries must be directed to that person.
- Reinforce that no SSI information should be revealed.

## 3.3 Working with the News Media

One of the tasks in post-incident management is dealing with the news media, which entails preparing a statement that is based on a comprehensive investigation and discussion of the incident. The airport’s security staff will not be the major actor in dealing with the news media, but its assistance will be needed. The office of the Airport Director, the public relations staff, or a public information officer (PIO) will likely interface with the media, prepare all written and oral comments, and possibly lead a press conference. However, security staff can assist the spokesperson by providing information, ensuring the investigation is thorough and promptly conducted, and by determining the classification of the incident.

Working with the news media is a process that can be beneficial to the missions of both the airport and media. The media needs to gather the facts of an event—in this case a breach—to present the news to the public, while the airport needs to ensure that the public gets an accurate account of what occurred. Working together increases the chances of both parties reaching their goals. Some basic principles for any spokesperson addressing the news media include:

- Maintain credibility
- Maintain objectivity
- Respond to inquiries on a timely basis
- Prepare an appropriate message
- Accept responsibility
- Know the ultimate audience: the public, through the press
- Do not guess; focus on what is known
- Keep in mind SSI issues, and be candid and firm regarding security information that should not be divulged

### 3.3.1 Primary Considerations

Many, if not all, airports have had experience in working with the news media on positive public relations stories, such as new air carriers coming to the airport, new construction, openings of new facilities, increased holiday passenger traffic, and other similar occasions. They have dealt with inquiries from the media regarding what the airport is doing about security in view of incidents at other airports and the "could that happen here?" thread. It is a safe assumption that these airports have also dealt with inquiries regarding an incident at their venue, and that they have a designated spokesperson to deal with the press, and a protocol, written or unwritten, on how to respond to, and work with, the media.

Though the person who will most likely interact with the media will be someone from the public relations office, the security staff, should be ready to provide any necessary information and assistance to the public relations staff. Main points to keep in mind are:

- In any case involving a security breach, the incident may or may not get the attention of the news media. Be prepared for the former.
- The original news story may raise further attention on the internet.
- Questions regarding details of the incident may come from various news entities.
- Inquiries may take place when the airport is still trying to deal with the vulnerability, investigate the incident, and assess the information still being gathered.
- The media works on a hurried timeline, while the airport may be trying to conduct a thorough and methodical investigation.
- The wrong information on an incident can sometimes be worse than no information at all.
- Delayed information from the airport may cause speculation on the details and severity of the incident.
- If incident information is limited, the airport should provide known information, say the incident is still under investigation, and explain that the public is not at risk.
- Information on steps or measures being taken must be weighed against the SSI restrictions.
- The designated media liaison must correct inaccurate information, and provide clear information to the media regarding the facts of the incident, the breach classification, and the reason for that classification.
- The airport, law enforcement, and airlines should agree on the facts of the breach before speaking to the media.

## 3.4 Best Practices in Prevention of Security Breaches

After post-incident activities have been completed, the airport security breach working groups can focus on strategies for mitigating future breaches. These prevention categories are Policies and Procedures, Physical Security, and Prevention Technology.

### 3.4.1 Policies and Procedures for Perimeter Breach Prevention

The security breach working groups should evaluate what, if any, policies and procedures need to be added, changed, or expanded:

- **Patrols:** Review and assess the perimeter patrol program, assure patrols stay up-to-date with latest industry breach news and detection methods, develop random rotations on patrol routes and schedules, and execute enhancements and changes based on current trends and needs.
- **Searching and Locating:** Develop and regularly review search procedures and methods that would be applicable to situations (potential breaches) where there is an unauthorized person within the perimeter whose location is unknown. Consider occasional limited-area search/locate training exercises to familiarize responders with search conditions and potential areas of concealment.
- **Training and Awareness:** Develop, execute, and perform routine training and security awareness programs for stakeholders, including identification of suspicious persons, challenge program, key stakeholder responsibilities, and security notification procedures/contacts.
- **Challenge & Reward Program:** Execute and reinforce a strong airport challenge program. When possible, include random challenge exercises, and recognition and/or reward for successfully challenging a test individual or an actual unauthorized individual/intruder.
- **Community Support/Awareness:** Develop a contact network and periodic briefing/awareness program for adjacent tenant and community groups (neighborhood/business associations, church/activity centers, and major nearby industries/businesses) to assist with airport security protection/notification, as well as indirect monitoring of shared perimeter boundaries and general airport perimeter conditions, suspicious persons/vehicles, and general public security observations. Communication should be a two-direction pathway to assist the airport's awareness of adjacent community events that may impact area traffic, pedestrian activity levels, or indirect airport security measures.
- **Signage and Deterrents:** Develop signage and deterrent standards (reflectivity, lighting, and/or barrier), as well as schedules/means for regular inspection and maintenance.
- **Location Names/Nomenclature:** Employ standard nomenclature/addresses and navigational terms for quick and knowledgeable identification of perimeter areas and sections during breaches, exercises, or inspection events.
- **Clear Zones:** Develop schedules and criteria for maintaining clear zones for the perimeter and inner/outer perimeter patrol roads, to include not only vegetation, vehicle, and obstruction clearing, but also maintenance of key lines of sight to drainage crossings, access points, key airfield equipment, critical assets and utilities, and other locations of concern that should be regularly and easily inspected.

### 3.4.2 Physical Security Prevention Measures

The physical security systems and measures listed below are commonly used by airports to protect the perimeter and perimeter gates. The fact that these measures currently are used and accomplish their purpose make them best practices for the airports using them, and thus potential best practices at other airports. As each airport's needs are unique, the cost of the systems, construction, maintenance, and sustainability should always be considered against the benefit to perimeter security improvement.

- **Guards:** Although guards are typically only assigned to frequently used staffed gates, they may be necessary for damaged fence locations or areas in need of persons to prevent unauthorized entry. The presence of a guard or periodic random patrol may also be a valuable detection method and deterrent in remote areas, or during high-threat or construction periods that do not warrant permanent measures.
- **Fence Protection Barriers:** These barriers serve to minimize the potential of a breach or prevent/deter a breach, as well as protect the perimeter fence line itself, when implemented outside the fence line, by making the perimeter inaccessible by vehicle or drastically reducing the speed/force of an intrusion. They may include natural or manmade berms and drainage ditches, jersey barriers, bollards, guardrails, or cable barriers. Even if these protection measures cannot be installed outside a perimeter fence due to right of way or clearance issues, they can still be valuable breach minimization measures that can decrease the intrusion distance of a breach or disable a vehicle.
- **Gate Protection Barriers:** Similar to fence protection barriers, gate protection barriers are most useful when placed outside (landside) of the gate to prevent actual intrusion or damage to the gate itself. Examples include strengthened roll gates, sally port gates, wedge and similar barriers that raise and drop into the ground, drop arm beams with or without arresting cable, and permanent or portable barriers that can be located in a fashion to slow a vehicle's approach, limit vehicle size, or narrow the available perimeter opening. As noted in the technology section below, some of these barriers can also be integrated or automated to enhance everyday functionality, detection, and/or response efficiency.
- **Safety Fences:** These structures are intended to absorb some energy caused by a vehicle and realign the vehicle to move parallel to the fence. They include deflection rail guards and cable guards and are most useful for specific, vulnerable portions of fences that are conducive to intentional or accidental car crashes.
- **Special Fence Construction:** Breach-resistant special fence construction includes anti-climb fences (such as those with one-inch spaces that mitigate scaling the fence), use of arresting cable to stop or to deflect a vehicle crashing into the fence (while also increasing life safety protection to the occupants, if appropriately installed), buried/embedded fencing to prevent digging under the fence (or slow a vehicle), or fences mounted on/to concrete walls or barriers to make vehicle and/or pedestrian breach more difficult.
- **Sally Port Gates:** The use of a dual-gate sally port system, although more effective to prevent a breach to the actual security perimeter line, increases the time for throughput. However, they can also prevent vehicle piggybacking, and can certainly provide added visual deterrence and detection/response time.

- **Speed Bumps:** Movable or permanent speed bumps placed prior to a gate location are effective in slowing down vehicles (minimizing breach speed and potential), and can close openings under cantilever gates to minimize pedestrian breaches.

- **Roadway Design:** Where possible, re-routing of adjacent public roadways, particularly those that 'T' or dead-end at fences/gates, can be effective in stopping accidental and intentional vehicular fence breaches. Where roadway design changes (or efforts to reduce head-on angle) cannot be implemented due to existing conditions, efforts towards other measures, such as fence protection barriers, landscaping barriers, reflectivity, signage, lighting, and other recommendations within this section, should be maximized to reduce accidental breach risk and breach speed/angle.

- **Perimeter Reflectivity and Signage:** Reflective lights, tape, and signage placed at vulnerable parts of the perimeter can, during hours of darkness, alert and deter public roadway drivers to prevent accidental vehicle breaches. Reflective tape woven into the fence and gates at these locations, reflective markers or blinking red lights (solar, battery, or powered), solar lighting, reflective signage, or any other measures designed to increase the visibility of the often remote, dark, unlit, and sometimes undetectable fence/gate fabric could make a great difference in preventing breaches, as well as enhancing public safety and avoiding injuries.

- **Increased Gate Visibility/Detection:** Economical measures such as convex security mirrors can be used at staffed gates to cover the blind side of trucks or semi-trailers stopped for processing, allow visibility of concealed areas adjacent to guard posts, or provide additional coverage area for CCTV cameras to detect and deter pedestrian breaches through vehicle portals. Photocell sensor systems (with local alarm annunciation), which are relatively inexpensive, can also be used at staffed gates to detect a person attempting to enter the airfield on the blind side of a large vehicle.

### 3.4.3 Breach Prevention Technology

Various technologies can be used to assist in breach prevention and deterrence. The technologies listed below are some of the typically available measures. But, new technologies, creative use of existing technologies, and the integration of technologies should be considered.

- **CCTV:** Cameras for assessment, detection, or monitoring are one of the most common security technologies at airports, aside from automated access control and badging systems. However, appropriate deployment, repurposing, and/or expansion of an existing or new system can greatly improve an airport's perimeter breach prevention. The mere visible presence of a fixed camera observing (and presumably recording) the events at a perimeter gate or fence location can deter an intentional breach attempt at that location (as well as capture for record and resolution the events of an actual breach). In addition, fixed-view cameras in remote and infrequently used locations can be set to video-level motion detection to alarm (whether integrated with access control or not) on activity within the camera's field of view, and allow prompt dispatch or response to potential breach activity.

  Many airports already have CCTV on a priority basis to cover fencing at critical areas such as the terminal apron/ramp areas, gates, and locations of vital facilities, either to monitor access points or general activity. Moreover, the existing infrastructure in these locations can allow for cost-effective additional fixed cameras with breach-specific purposes. Coverage of other perimeter areas will depend on the airport's budget, the ability to provide power and

communications connectivity, and other local factors. However, with the costs of solar power and wireless technology decreasing, this becomes a viable perimeter enhancement. Some airports may also be able to add the capability to monitor tenant cameras that cover perimeter locations, based on agreement, or could enact agreements to use them for investigative purposes.

- **Video Analytics:** Technology for the use of video analytics has greatly expanded in recent years, while costs have decreased, making it a more viable breach prevention measure. As with basic CCTV, the general visible presence can be a deterrent; however, video analytic technology can allow for much wider coverage by being able to use analytics to minimize basic motion-detection false alarms, create unique detection areas, and customize deployment to focus on only objects of a specific type/size in each location. As with expansion of existing CCTV systems for breach prevention purposes, this solution can also leverage existing resources for cost-effectiveness, while providing a technology with other non-breach capabilities (such as wildlife control and access control monitoring/piggybacking detection).

- **Physical Sensors:** For decades, the military has used sensor wires/cables/contacts on fences, structures, or in-ground for cost-effective perimeter breach detection, and the improved ability to respond to and prevent attempts. Visible measures or notification signage deters intentional attempts and, if attempts are made, the decreased response time may minimize the impact of the breach or prevent it entirely. As such, the ideal sensor placement may be outside the fence for early notification. Technology has also been developed to incorporate some joint-purpose physical security (arresting cables) or communication devices (fiber optics) into sensor applications to increase functionality and additional technology capabilities, as well as detect and prevent breaches in a cost-effective fashion.

- **Remote Sensors:** The use of a remote sensor technology (such as microwave or radar) is less of a visual or physical deterrent, but can be just as effective in detecting or preventing a breach, particularly in remote areas where infrastructure or terrain is limiting. Remote sensors are also useful as a supplemental measure to notify security personnel of an intruder approaching a critical area (such as between security areas of an airfield). A microwave sensor pair can be placed thousands of feet apart and still detect person- or greater-sized motion between the two units, without the need for physical structure or connections. Radar systems can cover a wide area and, with filtering capabilities, can be tailored to objects of a certain size and limit false alarms on authorized movement within the area. Also, unlike CCTV, most remote sensor technology is not as sensitive to light and weather conditions.

- **Portal Barriers:** Whether automatically or manually activated, perimeter gate barriers not only deter but can stop an actual breach attempt if deployed appropriately. On frequently used portals, automatic/powered barriers can be automatically retracted/deployed if an authorized/unauthorized vehicle approaches (or a gate attendant activates). On after-hours or infrequently used gates, barriers can remain deployed and be either manually retracted or integrated with an access control or timer system for use only during times of increased risk.

- **Remote Power/Communications Technology:** As noted above, advances in both cost-effective solar power capabilities and wireless and distributed communication technologies are making both conventional and new technologies available for perimeter security. As parks, cities, and areas around urban airports, as well as facilities within an airport, become networked with wireless communication capabilities and solar and alternative energy, the possibilities for expanding the technology to airport perimeters for breach detection and prevention grow as well.

- **Future Technology:** While aspects of physical security have been discussed previously, constant advances in materials technology and new ways to design for lightweight strength should not be discounted in their potential application and advances to perimeter security and hardening. Strong, lightweight gates and barriers that can still withstand and absorb impact are under development. Conductive touch-sensitive materials, which could provide new sensor capabilities for detecting fence climbers or breaks, could be forthcoming. Viable deployment of security patrol drones, or incorporation of military and industrial technology is also possible. In terms of breach preventative technologies, these future advancements could be airports' next best practices.

# REFERENCES

http://www.homelandsecuritynewswire.com/dr20140528-airports-resist-bolstering-perimeter-security-because-of-cost

http://www.nationaldefensemagazine.org/archive/2013/May/Pages/USAirportPerimeterSecurityMarketinDecline.aspx

International Foundation for Protection Officers article: Evolution of airlines Security Since 911; Alycia B. Taylor and Sara Steedman.

National Strategy for Airport Perimeter and Access Control Security – Commercial Airport Innovative Security Measures

**Perimeter Breaches**

*Airport Police Concerned by Airport Perimeter Breaches; Advocates 24/7 Police Patrols of Perimeters*. Rep. Los Angeles: American Alliance of Airport Police Officers. Web. http://laapoa.com/docs/AAPO-12232015.pdf

Associated Press (AP). "AP Investigation Details 8 Denver Airport Perimeter Breaches." *The Denver Post*. Associated Press, 09 Apr. 2015. Web. 02 Mar. 2016.

———. "AP Investigation Details DC-Area Airport Perimeter Breaches." *NBC Washington*. Associated Press, 12 Apr. 2015. Web. 29 Feb. 2016.

———. "AP: Philly Airport Had 25 Perimeter Breaches over 11 Years." *6abc Philadelphia*. Associated Press, 09 Apr. 2015. Web. 02 Mar. 2016.

———. "Major American Airports Report 268 Perimeter Security Breaches since 2004 – Though NYC Data Withheld for 'security concerns'." *New York Daily News*. Associated Press, 9 Apr. 2015. Web. 29 Feb. 2016.

Garbers, Jan. "Issues in Airport Perimeter Security." *TMG Consulting*. Word Press, 10 Oct. 2013. Web. 02 Mar. 2016. https://tmgconsulting.wordpress.com/2013/10/10/issues-in-airport-perimeter-security/

Klimas, Liz. "Airport With the Most Perimeter Breaches in a Decade Blames Most on Proximity to Homeless Shelter." *The Blaze*. The Associated Press, 10 Apr. 2015. Web. 29 Feb. 2016.

Peters, Justin. "It Is Shockingly, Terrifyingly Easy to Breach Perimeter Security at Most Airports." *Slate*. Slate, 20 Feb. 2013. Web. 02 Mar. 2016.

Richards, Anne L., ed. *Transportation Security Administration's Efforts to Identify and Track Security Breaches at Our Nation's Airports (Redacted)*. Rep. Web. https://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-80_May12.pdf (Appendix F is useful in particular)

**Best Practices**

*Airport Police Concerned by Airport Perimeter Breaches; Advocates 24/7 Police Patrols of Perimeters*. Rep. Los Angeles: American Alliance of Airport Police Officers. Web. http://laapoa.com/docs/AAPO-12232015.pdf

Barry, Ann S. "Airport Perimeter Security: Where we've been, Where we are, and Where we're going" *2008 IEEE Conference on Technologies for Homeland Security*. (2008): 57-62. Web. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4534423&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4534423

Dimoff, Timothy. "What Can Be Done About Airport Perimeter Security Breaches." *SACS Consulting & Investigative Services Inc*. SACS Consulting, 30 July 2015. Web. 02 Mar. 2016. http://sacsconsulting.com/2015/07/30/what-can-be-done-about-airport-perimeter-security-breaches/

Montanari, Mirko, Roy H. Campbell, Krishna Sampigethaya, and Mingyan Li. "A Security Policy Framework for eEnabled Fleets and Airports." *2011 IEEE Aerospace Conference* (2011): 1-11. Web.

Olivier, James. “Airport Perimeter Security: Finding the Right Fit For Your Airport.” *Airport Magazine* Aug/Sept 2014: 10-12. Web. http://www.airportmagazine-digital.com/airportmagazine/aug_sept_2014?pg=14#pg14

Ott, Jonathan, Jutta Hild, and Alexander Bauer. "Decision Support to Facilitate Cost-Optimal Response in Time- and Safety-Critical Situation", 2009.

Pita, James, Milind Tambe, Christopher Kiekintveld, Shane Cullen, and Erin Steigerwald. "GUARDS - Innovative Application of Game Theory for National Airport Security." *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence* Three (2011): n. pag. *USC Viterbi School of Engineering: Teamcore Research Group*. USC. Web. 2 Mar. 2016.

Sampigethaya, Radhakrishna G., Mingyan Li, and Timothy M. Mitchell. Airport Security System. The Boeing Company, assignee. Patent US 20120210387 A1. 1 July 2014. Web.

Weiss, William E. "Dynamic security: an agent-based model for airport defense." Simulation Conference, 2008. WSC 2008. Winter. IEEE, 2008. http://www.edgestone-it.com/papers/158.pdf

## ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

| | |
|---|---|
| **AAAE** | American Association of Airport Executives |
| **ACI-NA** | Airports Council International – North America |
| **AOA** | Air Operations Area |
| **AP** | Associated Press |
| **ASP** | Airport Security Program |
| **CCTV** | Closed Circuit Television (Cameras) |
| **FAA** | Federal Aviation Administration |
| **LEP** | Law Enforcement Personnel |
| **NCIC** | National Crime Information Center |
| **PARAS** | Program for Applied Research in Airport Security |
| **PIO** | Public Information Officer |
| **SIDA** | Security Identification Display Area |
| **SSI** | Sensitive Security Information |
| **TSA** | Transportation Security Administration |

# APPENDIX A: Airport Perimeter Breach Classification System

The following describes the perimeter fence and gate breaches classification model developed for use by airport operators who will categorize their airports' breach incidents based on the facts and actual consequences of the incident. Since the airports vary in configuration, operation, designation of secured, movement, and non-movement areas SIDA, and AOA, the airport operator is best able to factor in all the variables and the consequences of the incident and determine its rating.

## Underlying Principles

This system is intended for classifying perimeter breach incidents only, and is based on the following principles:

- The system model contains categories designated as 1 to 5, with category 5 being a breach with the most severe consequences, and category 1 having the least severe incidents.
- Each incident should be evaluated for severity based on the consequence of the incident, and not on what may possibly have occurred.
- Passenger aircraft are the most critical asset of an airport and require the greatest protection. For this reason, the non-movement area, (i.e., the terminal ramp/apron where aircraft load and unload passengers and baggage) becomes the airport's most critical area.
- Aircraft in the terminal ramp/apron area, whether they are operational or not, must be protected from the vulnerability to immediate or delayed sabotage, the placement of weapons in the aircraft, or other actions that may result in a hijacking.
- Cargo, charter, and hardstand-parked aircraft based in the terminal ramp/apron are deemed a higher criticality than those based outside the ramp/apron.
- A combination of factors such as violator intent, time in unauthorized area, observation of trespasser, detainment, trespasser mental capacity and capabilities, location of unauthorized access, and consequence of breach should be considered in determining the appropriate category.
- Individual airports should determine the amount of increase or decrease of category level based on situational factors.
- Flexibility in using the model is essential, and airports may adapt the model to suit their respective needs.

## Factors in Designating Categories

The following factors will affect and determine the categories for perimeter breach incidents:

- Perimeter breach incidents resulting in aircraft passengers being successfully attacked, hijacked, or sabotaged will be classified as category 5, absent other possible mitigating factors.
- In cases where persons are injured, shots are fired, explosives detonated, or vehicles are used to attack aircraft with passengers anywhere in the airport, the severity of the incident should be raised.
- The immediate or reasonably quick apprehension of trespassers reduces the severity of the incident in any area.
- Identification and observation of an intruder by stakeholders until the person is apprehended or otherwise detained reduces the severity of an incident.
- Breaches resulting in access to other airfield areas, exclusive of movement areas, by persons with clear, non-malevolent intent reduces the classification category.
- Intruding persons and vehicles in the proximity of, but not on, active runways, taxiways, and their access ramps reduces the severity.

- The severity of an incident based on the length of time before an intruder is discovered is contingent on criminal intent, location, capability and opportunity to do damage to persons and assets, and other factors discovered by post-incident investigation.

## Classification System Category Criteria

The following is the classification system and the individual category criteria that provide guidance on the process of classifying perimeter breaches according to their actual consequences. Each category definition includes a general description followed by a list of potential criteria to be used in the classification process.

**Category 5:** Addresses intentional criminal actions that include successful attacks, sabotage, or hijacking of a passenger aircraft in the critical terminal ramp/apron area; it may also include cargo or charter aircraft and hardstand-parked planes in the critical area.

Examples of this category may include:

- Any perimeter breach that results in a successful attack, sabotage, or hijacking from within the critical terminal ramp/apron area.
- Incidents where persons are injured, shots are fired, or explosives detonated, even if the attack of aircraft failed.
- Similar successful attacks of passenger aircraft in the process of taking off, landing, or taxiing to and from the runways.

**Category 4:** Addresses intentional criminal actions that include unsuccessful attempts to attack, sabotage, or hijack passenger aircraft in the terminal ramp/apron, and those landing, taking off, or taxiing to or from the runways. It also addresses successful attacks on assets that if sabotaged could affect essential air and ground operations.

Examples of this category may include:

- Unauthorized access to the terminal ramp/apron area that results in an unsuccessful attempt to attack, sabotage, or hijack a passenger, cargo, or charter aircraft in that area.
- Unsuccessful attempts to attack passenger aircraft landing, taking off, or taxiing to or from the runways.
- Successful attacks, sabotage, and other intentional destructive acts against assets that may affect essential flight or ground operations, such as fuel farms, heating and cooling utilities, power utilities, fuel lines and hydrants, fire stations and fire personnel, and other facilities deemed important by the airport. *An unsuccessful attack on these critical assets would lower the event to a category 3 or lower depending on the progress of the attack effort when it was prevented.*

**Category 3:** Addresses criminal intent that results in successful attacks, sabotage, or damage to non-essential assets and buildings whose damage or destruction would not disrupt airport air or ground operations.

Examples of this category may include:

- Successful attacks, sabotage, or damage to non-essential assets and buildings whose damage, although costly, would not disrupt airport air or ground operations.
- Theft of expensive materials and equipment.
- Incursions on active runways and taxiways where the incursion from breach vehicles or pedestrians momentarily affect the flight operations of landed aircraft or aircraft intending to

land or take off. These incidents would include vehicles evading pursuit that may endanger aircraft and passengers.

*An incident should should be included in category 2 or 1 when areas containing these assets are accessed by unauthorized persons who lacked criminal intent, did not cause damage or injury, were quickly arrested or were observed until detained, or did not have the ability or capability to do harm to persons or assets.*

**Category 2:** Addresses breaches by persons who intentionally trespass through the perimeter fence with clear intent of committing criminal, terrorist, or other serious malevolent acts, but who are prevented by immediate detainment or who were observed and monitored throughout their presence before being detained.

Examples of this category may include:

- Remote areas where perimeter breaches are made by persons with intent to attack, sabotage, or hijack aircraft or other significant assets, and who are in possession of weapons and/or explosive devices, but who are intercepted/apprehended before reaching those assets.

**Category 1:** Addresses persons who accessed, or attempted to access, areas on the airfield with or without bad intentions, and who were detained before committing a more serious violation.

Examples of this category may include trespassers who:

- Accessed the critical terminal ramp/apron or other secured locations, but could not or did not commit a greater violation before apprehension.
- Did not have the intent, opportunity, mental capacity, capability, or time to commit a greater violation.
- Had intention of commiting a criminal act such as theft or vandalism, but were apprehended before commiting that act.
- Accidentally breached the perimeter fence in a vehicle (e.g. were lost, confused, or intoxicated).
- Progressed into a critical or other security area, but was under observation.

# APPENDIX B: Best Practices

## Post-Breach Management of Activities

A number of activities need to be carried out subsequent to the immediate response to a perimeter breach. In certain cases and depending on the type, severity, and factors of the incident, the security staff or a small group of security staff and other employees may undertake these activities. The following are the stages, phases, and best practices in the management of post-breach incidents.

- Ensure that the breach site and/or the existing vulnerability is secured. These actions will be dependent on the type of breach and the status of the perimeter fence or gate.
- Search for and find the intruder if he or she has not been yet detained.
- Identify and interview witnesses for descriptions, numbers of intruders, accounts of what occurred, areas accessed, identification/verification of the intruder if necessary, and other relevant information.
- Question the intruder; run an NCIC check
- Determine access to critical areas, the depth of the access, and any critical assets reached.
- Determine the intent of the intruder.
- Decide if intruder will be charged and, if so, ensure LEPs have the necessary information for the charges, to include comments and declarations made by the intruder.
- Identify short-term solution(s) for the vulnerability.
- Determine category of breach per the classification system for media and stakeholder dissemination.
- Notify appropriate airport stakeholders.
- Prepare to brief and assist the public information spokesperson with key information on the incident, and to ensure the protection of SSI.
- Identify, if necessary, preventative policies and procedures, physical security, and/or technology actions that will address the breach.
- Conduct a “hot wash” meeting of security, law enforcement, persons involved in the incident, and stakeholders who will be involved in follow-up meetings. Analyze breach factors, including method of intrusion; consequence of the breach; response and investigation by the airport; questioning of the intruder; other interviews conducted; methods of improving handling of the incident; whether additional changes to the perimeter, policy and procedures, physical security, or technology are needed; and if further meetings to discuss and plan for those changes are necessary.
- Monitor category of breach for changes in classification for media and stakeholder dissemination.
- Hold a meeting of the breach review group to address the breach incident and its result, response and other actions of the airport; decide if changes in response protocols and practices are needed; and identify the most practical and cost-effective preventative measures.
- Identify possible long range solutions for this type of breach for consideration by the breach review group.
- Ensure that airport staff knows that interviews and information dissemination are centralized in the airport owner’s designated public information spokesperson, and that inquiries must be directed to that person.
- Reinforce that no SSI information should be revealed.

## Working with the News Media

One of the tasks in post-incident management is dealing with the news media, which encompasses preparing a statement that is based on a comprehensive investigation and discussion of the incident. The airport's security staff will not be the major actor in dealing with the news media, but its assistance will be needed. The office of the Airport Director, that of the public relations staff, or a PIO will very likely be the interface with the news, prepare all written and oral comments, and possibly lead a press conference. However, security staff can assist the spokesperson by providing information, ensuring the investigation is thorough and promptly conducted, and by determining the classification of the incident.

Working with the news media is a process that can be beneficial to the missions of both the airport and media. The media needs to gather the facts of an event—in this case a breach—to present the news to the public, while the airport needs to ensure that the public gets an accurate account of what occurred. Working together increases the chances of both parties reaching their goals. The following are some doctrines that should guide the airport, and that represent the best practices for working with the news media based on the response from airport operators, related literature, and professional experience of the project staff. Some basic principles for any spokesperson addressing the news media include:

- Maintain credibility
- Maintain objectivity
- Respond to inquiries on a timely basis
- Prepare an appropriate message
- Accept responsibility
- Know the ultimate audience: the public, through the press
- Do not guess; focus on what is known
- Keep in mind SSI issues, and be candid and firm regarding security information that should not be divulged

The person who will most likely interact with the media will be someone from the public relations office or anyone that the Airport Director assigns. The security staff, however, should be ready to provide any necessary information and assistance to the public relations staff. Main points to keep in mind are:

- In any case involving a security breach, the incident may or may not get the attention of the news media. Be prepared for the former.
- The original news story may raise further attention on the internet.
- Questions regarding details of the incident may come from various news entities.
- Inquiries may take place when the airport is still trying to deal with the vulnerability, investigate the incident, and assess the information still being gathered.
- The media works on a hurried timeline while the airport may be trying to conduct a thorough and methodical investigation.
- The wrong information on an incident can sometimes be worse than no information at all.
- Delayed information from the airport may cause speculation on the details and severity of the incident.
- If incident information is limited, the airport should provide known information, say the incident is still under investigation, and explain that the public is not at risk.
- Information on steps or measures being taken must be weighed against the SSI restrictions.
- The designated media liaison must correct inaccurate information, and provide clear information to the media regarding the facts of the incident, the breach classification, and the reason for that classification.

## Policies and Procedures for Perimeter Breach Protection

After post-incident activities have been completed the airport, security breach working groups can focus on strategies for mitigating future breaches. These prevention categories and their respective areas are Policies and Procedures, Physical Security, and Prevention Technology:

- **Patrols:** Review and assess the perimeter patrol program, assure patrols stay up-to-date with latest industry breach news and detection methods, develop random rotations on patrol routes and schedules, and execute enhancements and changes based on current trends and needs.
- **Searching and Locating:** Develop and regularly review search procedures and methods that would be applicable to situations (potential breaches) where there is an unauthorized person within the perimeter whose location is unknown. Consider occasional limited-area search/locate training exercises to familiarize responders with search conditions and potential areas of concealment.
- **Training and Awareness:** Develop, execute, and perform routine training and security awareness programs for stakeholders, including identification of suspicious persons, challenge program, key stakeholder responsibilities, and security notification procedures/contacts.
- **Challenge & Reward Program:** Execute and reinforce a strong airport challenge program. When possible, include random challenge exercises, and recognition and/or reward for successfully challenging a test individual or an actual unauthorized individual/intruder.
- **Community Support/Awareness:** Develop a contact network and periodic briefing/awareness program for adjacent tenant and community groups (neighborhood/business associations, church/activity centers, and major nearby industries/businesses) to assist with airport security protection/notification, as well as indirect monitoring of shared perimeter boundaries and general airport perimeter conditions, suspicious persons/vehicles, and general public security observations. Communication should be a two-direction pathway to assist the airport's awareness of adjacent community events that may impact area traffic, pedestrian activity levels, or indirect airport security measures.
- **Clear Zones:** Develop schedules and criteria for maintaining clear zones for the perimeter and inner/outer perimeter patrol roads, to include not only vegetation, vehicle, and obstruction clearing, but also maintenance of key lines of sight to drainage crossings, access points, key airfield equipment, critical assets and utilities, and other locations of concern that should be regularly and easily inspected.
- **Signage and Deterrents:** Develop signage and deterrent standards (reflectivity, lighting, and/or barrier), as well as schedules/means for regular inspection and maintenance. Included within these standards and related training should be standard nomenclature/addresses and navigational terms for quick and knowledgeable identification of perimeter areas and/or sections during breach, exercises, or inspection events.

## Physical Security Preventative Measures

The physical security systems and measures listed below are commonly used by airports to protect the perimeter and perimeter gates. The fact that these measures currently are used and accomplish their purpose make them best practices for the airports using them, and thus potential best practices at other airports. As each airport's needs are unique, the cost of the systems, construction, maintenance, and sustainability should always be considered against the benefit to perimeter security improvement.

- **Guards:** Although guards are typically only assigned to frequently used staffed gates, they may be necessary for damaged fence locations or areas in need of persons to prevent unauthorized entry. The presence of a guard or periodic random patrol may also be a valuable detection method and deterrent in remote areas, or during high-threat or construction periods that do not warrant permanent measures.

- **Fence Protection Barriers:** These barriers serve to minimize the potential of a breach or prevent/deter a breach, as well as protect the perimeter fence line itself, when implemented outside the fence line, by making the perimeter inaccessible by vehicle or drastically reducing the speed/force of an intrusion. They may include natural or manmade berms and drainage ditches, jersey barriers, bollards, guardrails, or cable barriers. Even if these protection measures cannot be installed outside a perimeter fence due to right of way or clearance issues, they can still be valuable breach minimization measures that can decrease the intrusion distance of a breach or disable a vehicle.

- **Gate Protection Barriers:** Similar to fence protection barriers, gate protection barriers are most useful when placed outside (landside) of the gate to prevent actual intrusion or damage to the gate itself. Examples include strengthened roll gates, sally port gates, wedge and similar barriers that raise and drop into the ground, drop arm beams with or without arresting cable, and permanent or portable barriers that can be located in a fashion to slow a vehicle's approach, limit vehicle size, or narrow the available perimeter opening. As noted in the technology section below, some of these barriers can also be integrated or automated to enhance everyday functionality, detection, and/or response efficiency.

- **Safety Fences:** These structures are intended to absorb some energy caused by a vehicle and realign the vehicle to move parallel to the fence. They include deflection rail guards and cable guards and are most useful for specific, vulnerable portions of fences that are conducive to intentional or accidental car crashes.

- **Special Fence Construction:** Breach-resistant special fence construction includes anti-climb fences (such as those with one-inch spaces that mitigate scaling the fence), use of arresting cable to stop or to deflect a vehicle crashing into the fence (while also increasing life safety protection to the occupants, if appropriately installed), buried/embedded fencing to prevent digging under the fence (or slow a vehicle), or fences mounted on/to concrete walls or barriers to make vehicle and/or pedestrian breach more difficult.

- **Sally Port Gates:** The use of a dual-gate sally port system, although more effective to prevent a breach to the actual security perimeter line, increases the time for throughput. However, they can also prevent vehicle piggybacking, and can certainly provide added visual deterrence and detection/response time.

- **Speed Bumps:** Movable or permanent speed bumps placed prior to a gate location are effective in slowing down vehicles (minimizing breach speed and potential) and can close openings under cantilever gates to minimize pedestrian breaches.

- **Roadway Design:** Where possible, re-routing of adjacent public roadways, particularly those that 'T' or dead-end at fences/gates, can be effective in stopping accidental and intentional vehicular fence breaches. Where roadway design changes (or efforts to reduce head-on angle) cannot be implemented due to existing conditions, efforts towards other measures, such as fence protection barriers, landscaping barriers, reflectivity, signage, lighting, and other

recommendations within this section, should be maximized to reduce accidental breach risk and breach speed/angle.

- **Perimeter Reflectivity and Signage:** Reflective lights, tape, and signage placed at vulnerable parts of the perimeter can, during hours of darkness, alert and deter public roadway drivers to prevent accidental vehicle breaches. Reflective tape woven into the fence and gates at these locations, reflective markers or blinking red lights (solar, battery, or powered), solar lighting, reflective signage, or any other measures designed to increase the visibility of the often remote, dark, unlit, and sometimes undetectable fence/gate fabric could make a great difference in preventing breaches, as well as enhancing public safety and avoiding injuries.

- **Increased Gate Visibility/Detection:** Economical measures such as convex security mirrors can be used at staffed gates to cover the blind side of trucks or semi-trailers stopped for processing, allow visibility of concealed areas adjacent to guard posts, or provide additional coverage area for CCTV cameras to detect and deter pedestrian breaches through vehicle portals. Photocell sensor systems (with local alarm annunciation), which are relatively inexpensive, can also be used at staffed gates to detect a person attempting to enter the airfield on the blind side of a large vehicle.

## Breach Prevention Technology

Various technologies can be used to assist in breach prevention and deterrence. The technologies posed below are some of the typically available measures, but new technologies, creative use of existing technologies, and the integration of technologies should be considered.

- **CCTV:** Cameras for assessment, detection, or monitoring are one of the most common security technologies at airports, aside from automated access control and badging systems. However, appropriate deployment, repurposing, and/or expansion of an existing or new system can greatly improve an airport's perimeter breach prevention. The mere visible presence of a fixed camera observing (and presumably recording) the events at a perimeter gate or fence location can deter an intentional breach attempt at that location (as well as capture for record and resolution the events of an actual breach). In addition, fixed-view cameras in remote and infrequently used locations can be set to video-level motion detection to alarm (whether integrated with access control or not) on activity within the camera's field of view, and allow prompt dispatch or response to potential breach activity.

  Many airports already have CCTV on a priority basis to cover fencing at critical areas such as the terminal apron/ramp areas, gates, and locations of vital facilities, either to monitor access points or general activity. Moreover, the existing infrastructure in these locations can allow for cost-effective additional fixed cameras with breach-specific purposes. Coverage of other perimeter areas will depend on the airport's budget, the ability to provide power and communications connectivity, and other local factors. However, with the costs of solar power and wireless technology decreasing, this becomes a viable perimeter enhancement. Some airports may also be able to add the capability to monitor tenant cameras that cover perimeter locations, based on agreement, or could enact agreements to use them for investigative purposes.

- **Video Analytics:** Technology for the use of video analytics has greatly expanded in recent years, while costs have decreased, making it a more viable breach prevention measure. As with basic CCTV, the general visible presence can be a deterrent; however, video analytic technology can allow for much wider coverage by being able to use analytics to minimize basic motion-detection

false alarms, create unique detection areas, and customize deployment to focus on only objects of a specific type/size in each location. As with expansion of existing CCTV systems for breach prevention purposes, this solution can also leverage existing resources for cost-effectiveness, while providing a technology with other non-breach capabilities (such as wildlife control and access control monitoring/piggybacking detection).

- **Physical Sensors:** For decades, the military has used sensor wires/cables/contacts on fences, structures, or in-ground for cost-effective perimeter breach detection, and the improved ability to respond to and prevent attempts. Visible measures or notification signage deters intentional attempts and, if attempts are made, the decreased response time may minimize the impact of the breach or prevent it entirely. As such, the ideal sensor placement may be outside the fence for early notification. Technology has also been developed to incorporate some joint-purpose physical security (arresting cables) or communication devices (fiber optics) into sensor applications to increase functionality and additional technology capabilities, as well as detect and prevent breaches in a cost-effective fashion.

- **Remote Sensors:** The use of a remote sensor technology (such as microwave or radar) is less of a visual or physical deterrent, but can be just as effective in detecting or preventing a breach, particularly in remote areas where infrastructure or terrain is limiting. Remote sensors are also useful as a supplemental measure to notify security personnel of an intruder approaching a critical area (such as between security areas of an airfield). A microwave sensor pair can be placed thousands of feet apart and still detect person- or greater-sized motion between the two units, without the need for physical structure or connections. Radar systems can cover a wide area and, with filtering capabilities, can be tailored to objects of a certain size and limit false alarms on authorized movement within the area. Also, unlike CCTV, most remote sensor technology is not as sensitive to light and weather conditions.

- **Portal Barriers:** Whether automatically or manually activated, perimeter gate barriers not only deter but can stop an actual breach attempt if deployed appropriately. On frequently used portals, automatic/powered barriers can be automatically retracted/deployed if an authorized/unauthorized vehicle approaches (or a gate attendant activates). On after-hours or infrequently used gates, barriers can remain deployed and be either manually retracted or integrated with an access control or timer system for use only during times of increased risk.

- **Remote Power/Communications Technology:** As noted above, advances in both cost-effective solar power capabilities and wireless and distributed communication technologies are making both conventional and new technologies available for perimeter security. As parks, cities, and areas around urban airports, as well as facilities within an airport, become networked with wireless communication capabilities and solar and alternative energy, the possibilities for expanding the technology to airport perimeters for breach detection and prevention grow as well.

- **Future Technology:** While aspects of physical security have been discussed previously, constant advances in materials technology and new ways to design for lightweight strength should not be discounted in their potential application and advances to perimeter security and hardening. Strong, lightweight gates and barriers that can still withstand and absorb impact are under development. Conductive touch-sensitive materials, which could provide new sensor capabilities for detecting fence climbers or breaks, could be forthcoming. Viable deployment of security patrol drones, or incorporation of military and industrial technology is also possible. In terms of breach preventative technologies, these future advancements could be airports' next best practices.

## AUTHOR ACKNOWLEDGMENTS

CTI Consulting and Faith Group, LLC wish to acknowledge the assistance of the various airports and their staffs that participated through written and oral responses to our questionnaire. Their responses and observations provided not only best practices, but also identified other measures and technologies that could benefit their respective airports if attainable. The team is also appreciative of the Safe Skies PARAS 0005 panel for its guidance and contributions during the development of this document.