AIRPORT PERIMETER SECURITY

ACI-NA TALKING POINTS

May 2016

ACI-NA POSITION

Maintaining the safety and security of the traveling public is the top priority for airports. Airports, in full compliance with federal requirements, continually work with their federal government, law enforcement and airline partners to examine, test, and improve upon the multi-layered, risk-based security system to provide for the safety and security of travelers.

HIGH LEVEL POINTS

- Maintaining the safety and security of the traveling public is the top priority for airports.
- Airport perimeter security involves multiple layers of integrated processes, procedures, and technologies to detect and mitigate breaches.
- While there is no perfect perimeter security system, the multiple layers of security – which airports routinely enhance – provide an effective system to deter and detect potential intruders.
- Although perimeter fencing and controlled access gates are the most outwardly visible features, numerous other systems – both seen and unseen – are in place at airports to reinforce perimeter security.
- Airports are committed to ensuring effective security and implementing enhanced measures based on current and emerging threats and in response to assessments.
- Airports work in continual collaboration with federal, state, and local law enforcement agencies, their airline partners and the Transportation Security Administration (TSA), to routinely conduct risk and vulnerability assessments to identify potential weaknesses and guide the application of resources to further enhance perimeter security.
- On-going research and development of promising new technology is essential. To evaluate the effectiveness of new technology in the operational environment, TSA should commission the National Safe Skies Alliance to pilot test promising technologies identified through the R&D process at airports. These pilot

programs would provide valuable information about additional cutting-edge technologies that could be used by airports to further enhance perimeter security.

- DHS and TSA should establish an airport security-focused grant program. Such a program would provide needed funding to support perimeter and other security-technology projects at airports.

SUPPORTING POINTS

Because of the unpredictable nature of security threats, airports often go above and beyond baseline security requirements, implementing additional processes, procedures, and technologies that are adapted to each airport's unique geographic locations and facility designs.

- **Shared Responsibility**

  Maintaining the safety and security of the traveling public is a responsibility that is shared by airports, airlines, airport partners, federal agencies, law enforcement, and the traveling public. Airport personnel are trained to spot and report suspicious behavior. The traveling public is always encouraged to report suspicious activities.

- **Seen and Unseen Security**

  While passengers may see chain link fences topped with barbed wire and security checkpoints, they do not see the fully integrated, multi-layered approach to airport perimeter security that happens behind the scenes.

  Airports have established systems – independently and in compliance with TSA security regulations – to prevent, detect, and respond to the unauthorized entry, presence, and movement of individuals and vehicles in secure airport areas.

  Examples of airport actions for securing perimeters include:
  - Fencing and other visible barriers like bollards, reinforced structures, and controlled access areas
  - Active perimeter intrusion detection systems, measures, and technologies
  - Frequent patrols of public and secure areas by airport, airline, and local law enforcement officers
  - Deployment of closed circuit television, video analytics, and smart fencing

  In the event of a potential breach, these systems identify the location of an intruder and alert law enforcement.

- **New Approaches to Security**

  Airports are always looking for new and innovative methods to enhance security. In addition to presenting their security initiatives at industry forums, airports routinely hold security peer reviews and invite their counterparts to participate in discussions and provide feedback on security programs in place at the host airport. Such initiatives facilitate an unbiased evaluation of existing systems as well as opportunities to benchmark on processes, procedures, and technologies in place at other airports.

  In partnership with TSA and the FBI, airports conduct joint vulnerability assessments of facilities, systems, and perimeters. These assessments, along with the latest intelligence, are used by airports to direct the application of resources to enhance individual security layers.

- **National Safe Skies Alliance**

  The National Safe Skies Alliance, in partnership with airports, supported by funding through the Airport Improvement Program, conducts testing and operational evaluations of security technologies designed to further enhance perimeter security. Many airports have deployed the systems tested and evaluated by the National Safe Skies Alliance. These evaluations, which are available to all airports through a TSA secure site, provide specific details about the application and functionality of technologies tested under the program and contain incredibly valuable information for airports as they make decisions on which technologies may work best at their facility.

OPPOSING VIEWS

- **The Associated Press report highlights a significant gap in airport security.**

  The AP investigation into airport perimeter breaches contains some misleading information about alleged breaches of perimeter security systems in place at U.S. airports. For example, the report compares a wide variety of breaches using inconsistent and incomplete data. Additionally, local law enforcement may define "breach" differently and the situations are all very different. Some airports provided data on all recorded events, even if an actual breach did not occur. Simply put, airports may have over-reported and, absent a uniform definition of a breach, there can be no apples to apples comparison. If an individual scales a fence and is promptly challenged, escorted out of the area and/or arrested, that is not a breach. Rather, it is an example of how the multi-layered system works.

- **Any breach of the airport perimeter is a failure in security.**

  The individuals involved in many of the breach reports were promptly apprehended. Rather than presenting a gaping vulnerability, this is clear evidence of the effectiveness of the layered security system in place at airports.

FREQUENTLY ASKED QUESTIONS

- **Is the issue of perimeter security a major issue or is it a minor issue?**

  Airport perimeter security is certainly something that airports focus on, but it is just one of a number of things that airports do to provide the highest level of safety and security for the passengers, airport employees, and airport facilities.

- **If someone jumps a fence, did the system work or did the system fail? Isn't someone getting over or through a fence a failure of the system?**

  There is no fence that is impenetrable. Every perimeter fence is different because of different considerations by each airport. Safety also plays into fence height. We cannot build fences that might become an obstruction for aircraft. That is why airports apply a multi-layered, risk-based approach to security. If someone jumps a fence and gets through one layer but is stopped by the second layer, that is an example of the system working.

- **In the AP report, 300 breaches over a 10 plus year period were self-reported by airports. Is that number high, low, or concerning?**

  In many cases, the individual was promptly apprehended and/or arrested, which demonstrates the effectiveness of the multi-layered system. It is impossible to comment on the number of alleged breaches. Each and every detail of each circumstance is different. The local definition of breach may also be different. There are many different ways to look at the data and that is impossible to do without a uniform, consistent data set.

- **Should passengers be worried about the security of airports in the United States? Should passengers be worried that perimeter security is inadequate in the United States?**

  No. Passengers should not be worried that perimeter security is inadequate. Airports have taken considerable steps to enhance airport security, including perimeter security, through a multi-layered, risk-based approach.

- **Is there a nexus between airport perimeter breaches and terrorism?**

  To date, there has been no nexus between reported perimeter breaches and terrorism. At the same time, airports understand that just because something has not happened does not mean it can be discounted. That is why airports continue to look for innovative ways to enhance airport security, including perimeter security. They constantly coordinate with federal partners, airlines and law enforcement and conduct vulnerability assessments at their locations.

- **Is there a challenge to obtain funding for airport security?**

  Airport operators have limited funding available that must be prioritized across a multitude of safety, security and operational projects. Although the Department of Homeland Security (DHS), through its Homeland Security Grant Program, dispenses billions of dollars annually for systems and technology to bolster state, tribal and local preparedness and improve security and resilience, such a robust program is not currently available to airports. To provide readily available funding to support perimeter, access control and other security enhancements at airports, ACI-NA recommends that DHS and TSA establish an airport security-focused grant program.

- **Why can't you tell me more about your security rules and regulations?**

  Federal regulations (49 CFR Part 1520) prevent airport operators from disclosing sensitive security information (SSI) due to transportation security concerns. You can learn more about SSI regulations here.

- **What improvements/changes have airports made over the last year since the AP story on perimeter breaches broke? How much has been invested?**

  There continues to be a constant focus on airport security because an airport's top priority is maintaining the safety and security of the travelling public, airport workers, airport tenants, and airport facilities. Perimeter security is just one part of overall airport security.

  Over the last few years, many airports have worked with the National Safe Skies Alliance to test and evaluate new – both active and passive – technology, systems, and procedures based on threat assessments. Specific examples include new kinds of fencing, video analytics, and intruder detection systems.

  It is difficult to say how much airports have directly invested in airport security because of the way money is apportioned across different systems. Individual airports would have to respond based on their own systems.

- **While it is difficult to break out specific funds spent to enhance security, is there federal money available? Has more money been made available?**

  Unfortunately, no new money has been designated for airport security. Airport operators have limited funding available that must be prioritized across a multitude of safety, security and operational projects. Although the Department of Homeland Security (DHS), through its Homeland Security Grant Program, dispenses billions of dollars annually for systems and technology to bolster state, tribal and local preparedness and improve security and resilience, such a robust program is not currently available to airports. To provide readily available funding to support perimeter, access control and other security enhancements at airports, ACI-NA recommends that DHS and TSA establish an airport security-focused grant program.

- **Does ACI-NA have a definition of a breach? What constitutes a breach?**

  ACI-NA does not have a definition of a "breach" because definitions vary greatly from jurisdiction to jurisdiction. TSA also has no stated definition in its regulations. If someone gets over a fence but they are immediately challenged, that is an example of the multi-layered system working. No system is perfect. That is why airports use a multi-layered system.

- **Can't an intruder being stopped by a multi-layered system still be considered a breach? Are the terms mutually exclusive?**

  If you look at each layer individually and one fails, then it can be considered a breach. But that is the entire point of the multi-layered system. It is multiple layers and risk based, and if someone is prevent from getting in or challenged after they get in, the system worked. It goes back to the time it takes to challenge an intruder and the individual failures of the various active and passive systems (including surveillance) in place to determine if a breach occurred.

- **Does ACI-NA track incidents?**

  No.

- **Where does the perimeter breach fall on the hierarchy of concern/security priorities for airports?**

  To date, there has been no nexus between a perimeter event and terrorism. At the same time, airports understand that just because something has not happened does not mean it can be discounted. Airport perimeter security is certainly something that airports focus on, but it is just one of a number of things that airports do to provide the highest level of safety and security for the passengers, airport employees, and airport facilities.

- **There have been some ASAC recommendations on perimeter security. Where do those recommendations stand?**

  Perimeter security was discussed at the September 5, 2015, ASAC meeting. At that meeting, the ASAC made several perimeter-security related recommendations. Minutes are available on the TSA website.

- **Is TSA fair in its application of SSI to protect data?**

  TSA is responsible for the enforcement of clear definitions as part of TSA regulations. TSA can speak to the application of SSI to the release of data.

- **Are airports safer by the public not being made aware of SSI information?**

  If released, security sensitive information could provide a roadmap to terrorism. Protecting that information is integral to the entire security of the transportation system. We need to prevent the release of that type of information.

- **Do you think perimeter security at our nation's largest airports to keep passengers safe?**

  Passengers are safe because of the multilayered approach to security. Each airport develops its own systems based on its own needs, like geographic location and unique boundaries.

- **Do our nation's largest airports have a problem with perimeter security breaches?**

  An airport's top priority is ensuring the safety and security of the travelling public, airport workers, airport tenants, and airport facilities. Based on their on-going risk assessments, they provide the highest level of security. There is not a gaping vulnerability in aviation security because of perimeter breaches.

CONTACTS

Media

Scott Elmore
Vice President, Communications and Marketing
selmore@aci-na.org
301-676-3304

Policy

Chris Bidwell
Vice President, Security
cbidwell@aci-na.org
202-293-8500