FLIGHT SAFETY FOUNDATION
Airport Operations
Vol. 17 No. 6 *For Everyone Concerned with the Safety of Flight* November/December 1991

U.S. Airport Access Control Moves Slowly

Passenger screening is only one spoke in the wheel of airport security. Airport access control of personnel is required for an integrated effort to close the door to perils, and the United States is discovering that the door does not fit as well as expected.

by
Frank G. McGuire
Editor & Publisher
Security Intelligence Report

At one o'clock in the morning on September 6, 1991, the State of South Carolina, in the United States, executed Donald "Pee Wee" Gaskins.

The electrocution of Pee Wee Gaskins may not, at first, seem significant to airport interests, but the murder of Rudolph Tyner in 1982 by the late Pee Wee Gaskins is very significant, indeed. Gaskins, 58, had actually murdered 14 people and had stabbed, shot or drowned all but Tyner, the last of his victims, who died by another method. Rudolph Tyner was killed by a bomb disguised as an intercom unit and passed between jail cells.

At the time that Gaskins designed the bomb, acquired its materials, and then built and delivered the device to Tyner, both men were inmates on death row in the state penitentiary. Most people would have described such an event as impossible.

On December 7, 1987, David Augustus Burke, a recently discharged USAir employee with a history of unprosecuted petty crimes, used his illegally retained employee identification (ID) card to bypass security at Los Angeles International Airport and board a Pacific Southwest Airlines flight. Over the San Luis Obispo area, he drew a pistol, shot a passenger and the PSA crew, then himself. The crash killed the remaining people aboard for a total of 43 dead. Within hours, the U.S. Federal Aviation Administration (FAA) issued orders that no one may bypass security at airports.

Pee Wee Gaskins and David Burke personify a real challenge to airport security, just as much as do acknowledged terrorists like Abu Nidal or Ahmed Jibril. Officials responsible for effectively controlling access at public airports used by millions of honest people annually should consider people like Gaskins and Burke to be a challenge because, in appearance, they could have presented themselves as ordinary citizens; they did not look like the stereotypical terrorists described in books and articles. Gaskins was creative. If a bomb can be built and delivered on death row and a discharged employee with an apparently valid ID card can board flights, what recourse does the airport operator have to safeguard the public?

There is certainly no lack of technological effort in bomb detection or the variety in security access control systems; neither is there any lack of control on death row. A logical answer to this puzzle was provided by Bill Jackson, security director of the Airport Operators Council International (AOCI). He said, "True, you can't stop it, but you can make a gallant effort at it if you screen everybody. Our estimates are that we'll spend about a billion dollars for security access control at our 274

major airports in the United States, based on one incident [the PSA case] in our 60-year history of commercial aviation. Is it ever going to happen again? Probably not, but I wouldn't bet my paycheck that it's not going to happen this afternoon."

The FAA has a program underway that requires airports to install access control systems under Part 107.14 of the U.S. Federal Aviation Regulations (FAR). The advance draft of the proposed change was sent to FAA regional offices in May 1989; the change subsequently became U.S. law. By late 1991, the first airport access control system has yet to be fully operational.

The airport access control program was prompted specifically by the PSA case. The goal of the program is to secure every gate or door that provides access to critical areas of civil airports to deny opportunities to those who should not be allowed into those areas. Ideally, all the security systems that would control this access would be computer-based.

"We have to live with the FAA program," observed Bill Jackson, who admits to the moral responsibility to make a "gallant effort," but who is not convinced that actual security will become any better. "It's going to cost us around a billion dollars," he said. "We're not really going to accomplish that much with it. An access control system is a wonderful way to control your doors, but it doesn't add a lot of depth to your security. It will keep Joe Stranger from wandering out on your ramp, and it will tell you which employee went through which door and when. It will do a lot of those things. Do we need to pay a billion dollars for that? It will solve the problem of lost keys and replacing locks, but it will solve few genuine security problems."

The Real World Is a Jumble of Independent Efforts

The FAA's regulatory solution to access control eventually encounters the real world of airport and airline operations. This is composed of numerous types of access points, varying levels of priority, many transient air crews of competing airlines, joint use of airports, available budgets and resources, as well as rapidly changing daily situations dictated by weather, peak traffic periods and emergencies. In this world, political and bureaucratic processes play havoc.

"Security integration at airports simply is not taking place," said Jackson. "The FAA has ordered that everybody put in a security access control system. That really is a regulation designed to take care of yesterday's employee. He was relieved of his job, or his authority changes and we want to make sure he is unable to get to the ramp."

A major technical reason that airport security integration is not being fully implemented is because the technology of access control is so varied that making choices is a major challenge. There are barcode cards of the type familiar to supermarket shoppers and an array of others: magnetic spot cards; magnetic stripe cards (three types of this technology are used by banks and others); optical cards (three types); Weigand-effect cards (a form of tamper-proof card); proximity cards (can be waved at the card reader up to a foot away); and, smart cards (which include other than security information, such as blood type and payroll data). Each has advantages and disadvantages. Airports have chosen various technologies for their own reasons. Some are more difficult to falsify than others, some are cheaper and some cannot be programmed by the airport but must be encoded by the manufacturer.

Airport Access Controls

"There are quite a few airports that are late in getting the hardware to comply with the regulation. FAA is allowing them to institute alternative interim measures which will elevate the level of security until they reach the sought-after degree of automation. FAA expects them to install the systems as soon as hardware is available. Most airports are late. There was a high level of demand on an industry that wasn't ready to meet that demand."

Fred Farrar, spokesman
U.S. Federal Aviation Administration
October 1991

Weigand-effect cards have been chosen by some, and magnetic stripe cards by most. Dallas/Fort Worth International Airport, Texas, U.S., chose a proximity card. The problem with this card is that there is no national uniformity. Consider how many cards each member of an air crew must carry in order to gain access to his or her own company's areas at every airport in the system?

It is this last point, as well as others, that is seen by the industry as the most significant security aspect that the FAA has failed to properly address. Instead of mandating a nationally uniform system (after appropriate field tests), the FAA told every airport to go its own way. The result has been varied local systems.

For FAA policy reasons and not technical reasons, said Jackson, "We have an open door at airports and we're not doing a whole lot to close that door. If you look at the airport in its entirety, the FAA wants you to secure the whole thing. There's no way that can be done. An airport the size of Washington-Dulles International Airport (IAD)

encompasses 18,000 acres. A Marine rifle battalion couldn't completely secure it. Even at Baltimore-Washington International Airport (BWI) with only 3,500 acres or San Diego International Airport with 800 acres, you still can't defend the perimeter of the airport. We can't do what they do in Tel Aviv — put an electronic fence around the airport and when it's disturbed you send out a patrol armed to the teeth. It's not feasible and not cost-effective, nor do we have a reason yet to do so in this country."

Pros and cons of Jackson's argument notwithstanding, the fact is that the installation of access control systems is an FAA requirement whose merits may be debated, but it does exist.

The FAR 107.14 change requires airport managements to deal with numerous items not previously encountered in any serious fashion. What is a "secure area" and is one area more "secure" than another? The entire terminal may be secure from an access control standpoint, or just the boarding gate areas or only the air carrier ramp area. The FAA has its specifications for some, but not all of these areas, leaving some to the local authority. What about general aviation, cargo areas and all that grass extending out to the perimeter fence? Secure, yes, but less secure than the air carrier ramp area.

… what procedures must be in place to immediately deny access by an ex-employee to any part of the airport?

If the David Burke case can be considered a benchmark scenario, what procedures must be in place to immediately deny access by an ex-employee to any part of the airport? What if the employee is fired by the night supervisor at two o'clock in the morning? How are other users of the system, airport tenants, airport police and airline security interests, not to mention the FAA, to be quickly notified of this action? Who is responsible for seeing that the notification is made?

What if the arrangement of doors in the airport secure area does not enhance security because of traffic patterns? Where do new doors have to be installed and previous doors have to be closed? How does all this mesh with local building and fire codes?

The Billion-dollar Check List Adds Up

While most people could think of a few obvious problems in securing all access points, only the security director of an airport must deal with every possible situation. Just to give the basics of what is involved, an initial set of considerations for access control systems are these points developed by AOCI, with other considerations applying to special circumstances:

- What type of identification medium is to be used, i.e., magnetic stripe, barcode, etc.?
- How many wood doors and frames will have to be replaced with metal?
- What is the default condition when the system fails, i.e., all locks open, all locks closed, etc.?
- Is there a need for multiple systems at each security point so a personal identification number (PIN) can be used to validate a card reading, and so lost or stolen cards cannot be used by others?
- Is there a need for multiple media at one airport for varying levels of security, i.e., card readers at ramp doors, lock and key at perimeter gates, visual clearance in administrative areas?
- Is there a need for flexible computers to handle mixed systems and communicate with other systems?

Once those criteria are determined, the airport operator must work out the system problems, such as:

- Which are the "essential" doors, as required under the FAA rule?
- How personnel access must be prioritized, i.e., which personnel must have access to which doors? What priorities are given to contractors, transient crews, tenants and others? What happens during overtime hours, emergencies, crash-fire-rescue (CFR) universal access and other non-standard situations?
- What is the most effective placement of ID card readers, i.e., both sides of doors? How can the system comply with fire codes? Is there enough capacity for peak hours? Are there special problems such as baggage carousel entry ports, catering and fuel service access, and others?
- What requirements exist for access to non-ramp areas, such as cargo areas, general aviation, joint civil-military facilities (some of which have higher security than the civil facilities), industrial buildings, parking areas, navaids, perimeter fences, hangars, maintenance facilities and non-aviation tenants that require no ramp access.
- What qualifications and staff will be required to operate and maintain the new system?

Procedural details must be worked out after the physical elements of the system are in place. Some of these procedural items require the establishment of criteria which include:

- Scheduled domestic and international crew access arrangements must be established.

- Transient, cargo and general aviation access, as well as unscheduled access during non-business hours, must be considered.

- Accommodation must be made for personnel who require multiple-point access, repeated access at one site, or access to more than one airport (e.g., a port authority with several facilities).

- The decision must be made regarding whether a single operator which operates several airports (i.e., a port authority or a city) may have a merged system for all facilities or must these be totally separated. (Examples are New York's LaGuardia, John F. Kennedy International and Newark International, and Chicago-O'Hare International, Chicago Midway and Merrill C. Meigs Field.)

- The access control database must be updated and maintained. Data must be integrated into personnel management files. Will the first and last security access of the day be considered a time-card record? An employee's security access must be determined, i.e., will it be validated at the start of a shift before further same-day access is authorized?

- Card accountability must be determined so that expired, duplicate or otherwise invalid cards which are still outstanding must be tagged or purged from the system.

- Compatibility standards for data communications must be determined so the system may be linked to a network with other systems nationwide.

Daily operations of any access control system require hundreds of decisions to be made on routine situations, such as these:

- Security personnel response procedures and times must be established for various threat levels, i.e., international boarding gate vs. a distant cargo ramp, or a door problem due to forced entry vs. a faulty card reader.

- Responsibility for responding to a system failure, either partial or total, must be established.

- Procedures for clearing personnel through access points during system failure, either by redundant electronic systems or manual systems must be established, as well as determination be made regarding how computer data will be recovered following a system failure.

- A supervisory clearance or police response must be developed to deal with cancelled ID cards, lost or stolen ID cards, attempted illegal breaches of security, damaged cards, new hires and temporary IDs, transient personnel and legitimate system errors.

How Long Are Your Arms?

"What we really need to do, in my opinion," said Jackson, "is to guarantee the airline that the ramp area is secure. With the new Part 107.14 requirements, we call it the 'secure working ramp area' [SWRA]. The SWRA is the area that you can figuratively put your arms around."

At some airports, said Jackson, it is very easy to isolate that area because everything else is some distance away. At other airports, it is virtually impossible to totally isolate it. At Boston General Edward Lawrence Logan International Airport (Boston-Logan), for example, there is a cargo ramp immediately contiguous to the air carrier area. The same thing is true at Albuquerque International Airport and at some other airports, but at BWI and IAD, security can totally isolate the air cargo area from the air carrier area. Jackson noted this should be done. "Everything entering the SWRA should be screened," he said, "but we're not doing that.

"What we really need to do … is to guarantee the airline that the ramp area is secure."

"We're not screening cargo, we're not screening mail, we're not looking at the catering operation, we're not even looking at today's employee. He uses his card to come into this area from the unsecured world and, because he has an ID card, we assume he's a good guy. I just don't subscribe to the idea that we're all good guys. We're going to have to screen today's employees," said Jackson.

Jackson has proposed that airports, especially new ones, have a separate employee entrance/exit plaza. There would be turnstiles that would be operated by employee access cards with PIN numbers, and there would also be someone from security to selectively and randomly have employees go through a screening line to have lunch con-

tainers checked. Employees would come to work without knowing whether a briefcase or lunch box would be sent through the X-ray machine for screening. Employees would be more hesitant to bring in contraband because they could be discharged or even jailed. Until such procedures are implemented, Jackson said security efforts will be ineffective in screening employees.

"We're putting a lot of effort into screening passengers," he said. "We're looking at their carry-on luggage, even though it's been a long time since we've had a suicidal martyr take a bomb on an airplane. When is the last time somebody tried to take over an airplane with a weapon? It's been a long time. So maybe that's not where our threat is. Maybe our threat is having somebody put something on the airplane and blowing it out of the sky. That sort of thing does not come through the screening point with the passengers," he said.

Jackson foresees U.S. airports within the next five years becoming a series of funnels, noting that everyone who gets into the SWRA is going to be screened somehow. What he has to say about the consequences of any failure to stop the potential bomber is frightening, and is based on his observations after six years as operations director at BWI, and aviation experience in many other places.

"Maybe everybody will not be screened every day, but it's going to be the kind of situation where the guy who comes to work in the morning will not know if he's going to be screened or not. It will be an arbitrary thing. Every piece of equipment that goes on an airplane will be screened, whether by X-ray, hand search or whatever. I see no reason why this shouldn't take place, because if a terrorist organization has the wherewithal and the desire to knock down an airplane, why can't they do it by putting something with the catering equipment? Why can't they pay someone a few thousand dollars to come in as a worker and load something on the aircraft, right next to a fuselage stringer. It could be in his lunch box. There are people who would do it.

We're telling the traveling public it can rest assured that everything is OK. Well, it's not."

"We know that drugs are the backdrop for so much evil in the world. So I just think that one of these days somebody is going to do it. The drug cartels have already bombed an Avianca flight. [A Boeing 727-100 was destroyed by a bomb seven minutes after takeoff from Bogota, Colombia, on November 27, 1989, with the loss of 101 passengers and six crew members, plus three persons on the ground.] You take a cross-section of any group of workers and you'll find some that are shaky. Maybe they're doing cocaine after working hours or sometimes during working hours. Why can't somebody lure them with a few thousand dollars or get them into an extortion or blackmail box and say: 'Put this on an airplane or your family is going to suffer.'?

"So there is nothing that's helping me sleep well and believe that nothing is going to happen to an airplane in the United States. I just don't think our airports are any more secure than some of the foreign airports. I keep looking at the reports on the Pan Am 103 investigation [A Boeing 747 that was destroyed by a bomb over Lockerbie, Scotland, in December 1988], and I see absolutely nothing that we're doing today — had it been done in Frankfurt and London in 1988 — that would have had one bit of effect on the Pan Am 103 disaster. I could set five tape players down on this table and neither you nor I could pick the one that had the bomb in it.

"My point is that we're really not closing the door," concluded Jackson. "We're making a lot of noise. We're telling the traveling public it can rest assured that everything is OK. Well, it's not."

Why Are There So Many Systems?

One reason everything is not OK, Jackson and many others in the industry maintain, is that FAA forced the access control issue on a very fast track. The industry wanted a "lead-airport" approach, where four different kinds of facilities would be selected to test different hardware and software systems for access control. Although at first agreeing to the idea, the FAA later reversed itself in 1989 and ordered all airports to begin installing their own choice of access control system immediately, with no coordinating effort except for the voluntary work of industry associations.

"We knew we were going to have a problem because we were going to have as many different kinds of systems as we have airports. We warned the FAA that if it ever decided we needed a national system, we'd be so far down that diverse trail of everybody inventing his own wheel that we won't economically be able to create a unified national system. So here we are nearing the end of 1991 — we don't even have the [largest airport installations] completed yet and we realize we need a national system for our flight crews [that is compatible from one airport to another]. It's going to cost a bundle, an absolute bundle," said Jackson.

"Some airports are so far behind schedule they are getting waivers for as much as a year," said Jackson. "The industry told the FAA at the outset that even if airports had all the equipment on hand and the access system design completed, they could not get the biggest airports

on line in a year and a half no matter how it was done. The FAA did not believe it, so the agency gave airports six months to send in proposed changes to the security plan to FAA for approval. Then airports had 18 months to implement their access systems from the day the security plan was returned to the airport with the approval.

"Los Angeles International, for example, is a huge airport," said Jackson. "[Management personnel] don't have the first item completed yet and they've got less than six months to go. JFK was due in June 1991 and hasn't finished yet. You can't put in a massive computer-based system like that and expect to turn the switch and have it function. The software will have glitches, the hardware will allegedly have been thoroughly tested, and I can tell you from experience that parts of it won't work."

Chicago-O'Hare has 1,500 doors, noted Jackson, plus two or three systems that they must coordinate. This is also occurring at JFK, where the Pan American World Airways terminal has its own system and the Trans World Airlines terminal has a different system. Some airline systems are not on the airport system, and they require various modems and software interfaces. If someone takes an employee's name out of an airline's computer, that name must also come out of the main computer serving the airport. Such multiplicity of systems, some industry sources say, are not minor, are not cheap, do not get implemented overnight — and are not necessarily effective.

"The FAA idea is not bad," acknowledged Jackson, "and it may benefit the airports in some subsidiary ways, but whether it will benefit security to the tune of a billion dollars is questionable. The FAA was dreaming on the time frame — totally unrealistic."

Two things are clear from this discussion: access control problems at civil airports are so numerous and complex they could easily fill a book, and the airport access control book is being written by more than 200 U.S. airport operators as each invents his own wheel. They each must "make a gallant effort" to invent that custom-tailored wheel very effectively so as to do the near-impossible and prevent another tragedy.

Remember Pee Wee Gaskins and David Burke. ♦

About The Author

Francis ("Frank") G. McGuire has been a journalist writing and editing almost exclusively about aviation, law enforcement and security for more than 30 years. He is founding editor & publisher of Counter-Terrorism and Security Intelligence, *a biweekly newsletter focused on ideological and political violence around the world.*

McGuire's first published article on industrial security was in "Law and Order" *magazine. A past president of the Aviation/Space Writers Association (AWA), he has been an accredited correspondent to the U.S. Congress for more than a dozen years.*

In 1985, he won a national award from the Newsletter Association for investigative reporting after a series on aircraft safety.

A revised edition of his standard reference work Who's Who in Terrorism: A Security Intelligence Sourcebook *was published in 1989 and included profiles of terrorist groups and leaders, areas of operation, tactics, links with other groups, statistics on terrorism and other data.*

His 100-page report Aviation Security — Strategies for the 1990s *was published in 1989 by McGraw-Hill Information Systems Division.*

What's Your Input?

Flight Safety Foundation welcomes articles and papers for publication. If you have an article proposal, a completed manuscript or a technical paper that may be appropriate for *Airport Operations* please contact the editor. Submitted materials are evaluated for suitability and a cash stipend is paid upon publication. Request a copy of "Editorial Guidelines for Flight Safety Foundation Writers."

AIRPORT OPERATIONS

 • Subscriptions : $55 U.S. (U.S. - Canada - Mexico), $60 Air Mail (all other countries), six issues yearly. • Staff: Roger Rozelle, director of publications; Arthur H. Sanfelici, senior editor; Ashton Alvis, production coordinator; Sandra Mitchell, editorial assistant • Request address changes by mail and include old and new addresses. • Flight Safety Foundation, 2200 Wilson Boulevard, Suite 500, Arlington, VA 22201-3306 U.S. • telephone: (703) 522-8300 • telex: 901176 FSF INC AGTN • fax: (703) 525-6047