

Aviation Security – Filling the Gaps

By Ray Bernard, PSP

Where do we stand with regard to civil aviation security? It is impossible to provide a short or complete answer to this question. There is no security model against which the various components of the civil aviation system—the airlines, airline service companies, airports, airport business tenants, local airport security forces and the TSA screener force—can be rated. (The Israeli model of security doesn't scale up. El Al's 30 planes provide only 90 flights per day, the same as The Eastern Iowa Airport in Cedar Rapids, a tiny fraction of the approximately 25,000 daily flights from U.S. airports.) There are no scorecards by which, from one year to the next, we can formally rate security progress.

Nonetheless there are thousands of people with security responsibilities in aviation system jobs, and millions more who are also stakeholders in aviation security—the flying public and the employees whose jobs, directly or indirectly, depend upon the successful future operation of the civil aviation system. Regardless of how difficult the job is, we have no choice but to improve aviation security. Too much depends upon it. The key question is whether we will do it poorly or well.

Security Gaps

On February 11, 2004 Congressman Edward J. Markey introduced bill HR 3798, to amend the Homeland Security Act of 2002 to improve aviation security. The bill calls for seven specific reforms:

- Mandatory, physical inspection of all cargo transported on passenger airplanes
- Prohibition of foreign flights from taking off or landing in the U.S. unless air marshals of a foreign country are onboard, if requested by the Department of Homeland Security
- Authority for U.S. Federal Air Marshals to travel on cargo planes
- The requirement that the Department of Homeland Security develop a plan to improve coordination with foreign counterparts, particularly in the area of air marshals and improved perimeter security at airports abroad
- Establishment of uniform security standards for airport workers with access to sensitive areas, including screening for metal objects and hazardous substances and background checks that verify Social Security numbers and query terrorist watch lists
- Requirement that the Department of Homeland Security issue regulations mandating that air carriers train pilots on how to maneuver passenger planes safely in the event that the plane is hit by a surface-to-air missile
- The requirement that flight attendants have a secure, wireless means to communicate to the cockpit crew, Federal Air Marshals and authorities on the ground regarding the existence of a terrorist threat, even if the intercom system is disabled

Regarding the bill, called the Secure Existing Aviation Loopholes (SEAL) Act, Congressman Markey says, "Repeated disruptions in airline service and exploitation of the cargo screening loophole have demonstrated that we must take a comprehensive approach to improving the level of security across the aviation system." These reforms, if enacted, would indeed close

Aviation Security – Filling the Gaps

some major existing security gaps. But much more is needed in order to reach the higher levels of security that are obtainable.

Comprehensive Security

One phrase in Markey’s comment will strike a chord with many security practitioners: *comprehensive approach*. The Merriam-Webster online dictionary provides two definitions for *comprehensive*: 1. covering completely or broadly; 2. having or exhibiting wide mental grasp. Mark Denari, Director of Public Safety and Security for San Diego International Airport, says, “Our civil aviation system was built to support a complex and open society. The primary challenge for aviation security practitioners is to establish a comprehensive security program, given the huge breadth of aviation system activities and the finite scope of resources. The civil aviation system is not a single business or organization. It’s composed of a multitude of local, national and international businesses and organizations, working together to provide a workable air transportation system. Each organization has to remain viable and achieve its mission, in order for the civil aviation system to work. It’s not just passengers and planes that we have to secure. We have to protect the operations of the entire system—a system built to be open, and to provide high volume services at a very fast pace. The nature of the system contributes to its vulnerability.”

In its publication *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, the National Research Council (NRC) states, “Our society is too complex and interconnected to defend against all possible threats.”¹ Thus the same can be said for civil aviation.

Following the NRC report, the Transportation Research Board published Special Report 270 titled, *Deterrence, Protection, And Preparation: The New Transportation Security Imperative*, which explains why a comprehensive approach to security is an absolute necessity:

The nation’s vast air, land, and maritime transportation systems are marvels of innovation and productivity, but they are designed to be accessible, and their very function is to concentrate passenger and freight flows in ways that can create many vulnerabilities for terrorists to exploit. Prospects for defending against each of these vulnerabilities through traditional means, such as “guards, guns, and gates,” are dim. The transportation sector is simply too large and the threats faced too diverse and ever-changing for such blanket approaches to work. Moreover, if applied in the large and diffuse transportation sector, these approaches run the risk of creating a diluted and patchwork collection of poorly connected defenses that disperse security resources while leaving many vulnerabilities unprotected against a terrorist attack.

Transportation security can best be achieved through coherent security systems that are well integrated with transportation operations and are deliberately designed to deter terrorists even as they selectively guard against and prepare for terrorist attacks. In particular, layered security systems, characterized by an interleaved and concentric

¹ National Research Council’s Committee on Science and Technology for Countering Terrorism, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (The National Academies Press, 2002), p. 2. The book is available online at <http://books.nap.edu/books/0309084814/html/index.html>.

Aviation Security – Filling the Gaps

set of security features, have the greatest potential to deter and protect. Layered systems cannot be breached by the defeat of a single security feature—such as a gate or guard—as each layer provides backup for the others, so that impermeability of individual layers is not required. Moreover, the interleaved layers can confound the would-be terrorist. Calculating the odds of breaching a multitiered system of defense is far more difficult than calculating the odds of defeating a single, perimeter protection.

The Transportation Research Board special report also states:

The dangers of not taking such a coherent, systems approach to security were manifest in the aviation sector on September 11. Commercial aviation has been the subject of hostile attacks for more than 30 years. Each new attack has prompted the advent of more technologies, procedures, and rules—each superimposed on those previously introduced, and designed mainly to prevent a recurrence of similar attacks. Aviation security has not been provided through truly systematic means, but rather through a collection of mostly unrelated measures that have hinged on a very high and sustained level of performance from each, with little or no backup and redundancy. By overcoming a single perimeter defense, such as a metal detector, an attacker could, in effect, overcome the entire security regime.

Technology Deployment Is No Small Issue

Federally mandated security technology initiatives continue to roll forward airport by airport. These initiatives are lengthy and expensive initiatives, whose schedules are measured more in years than in months. The security industry continues to strive to develop new technologies to help fill the security detection and prevention gaps that still remain; there can be no schedule for those results.

The Faith Group, headed by Faith Varwig, is a planning and consulting firm whose mission with regard to their aviation clients is to help unfold the complex issues surrounding continued operational changes, including those brought about by new security and baggage inspection requirements. Varwig says, “Perimeter security is one example of an issue that seems simple at first thought, but in reality is far from simple. There is no ‘one-size-fits-all’ approach, and for most airports just defining ‘the perimeter’ is a complex issue. For example, many airport properties have water boundaries. Portions of some airport perimeters are not under direct airport control, because tenants occupy perimeter buildings. Some have endangered animal species that live on the perimeter land. What’s more, the FAA and TSA regulations have no clear cut definition of what is meant by ‘airport perimeter.’”

Paul Foster is Manager, Aviation Security and Special Systems at San Francisco International Airport. Foster says, “If part of your airport perimeter is water, who monitors it? How far out does the airport authority extend? Who responds to water-based threats? Is it the Airport Police, the Harbor Patrol, the Coast Guard or all of them? And how do they respond—by helicopter, by boat, or by jeep? The situation is often one of cross-jurisdictional issues touching upon city, county and other regulations.” These kinds of issues have to be resolved,

Aviation Security – Filling the Gaps

and security plans and procedures developed, before you can begin to identify technology that will work to support your security objectives.

Aviation’s Most Underutilized Security Asset

A recent airport experience gave me additional insight into what is probably the most underutilized security asset for civil aviation security: the people in and around the civil aviation system. While many organizations glibly state “our people are our most important asset”, a look at the training plans and budgets of most organizations reveals that people are often the most neglected asset—especially from a security training perspective.

In mid 2003 I spent several days performing an airport perimeter photo survey for an urban regional airport. In a few spots I took photos from inside my car; mostly I walked around the streets outside of the airport. Since it was 2-½ years after September 11, I wasn’t expecting the magnitude of response from people not employed by the airport or by an airport business. Each day several non-airport individuals called the police to report my taking photos of the airport. Two drivers circled around to note my license plate, as I snapped pictures of the airport from inside my car at the side of the road. Each day I was directly confronted by several non-security people, who asked what I was doing or who stated, “You can’t take pictures of the airport.” One hi-lo driver who was unloading a truck waved me forward, shut off his hi-lo, and asked me what I was doing. In each instance I showed my airport ID badge and a letter from the airport explaining what I was doing. That wasn’t enough for most individuals, who contacted the airport or the police to verify my story.

I’m hoping that these individuals were commended. When ordinary citizens go out of the way to provide helpful specifics to the authorities, a “thank-you” letter or note is probably warranted, and will go a long way to support local awareness of airport security.

Expanding the Scope of Airport Security

The responses to the airport perimeter survey highlight the role that individual initiative can play. Enhancing the security role of people already on the job at airports would be a tiny cost compared to most other security initiatives, yet it holds much greater potential for filling in security gaps—especially the gaps that technology just can’t fill.

George Teebay, former Federal Security Manager for San Francisco International Airport, points out that existing regulations and procedures can be leveraged to increase security for airside operations. Teebay explains, “Before September 11, many airports found it beneficial to minimize their SIDA [Security Identification Display Area]. These days, airports would be well advised to expand the SIDA to include everything inside the perimeter fence except for FBO² ramps. This triggers Criminal History Records Checks (CHRC) and SIDA training for employees in those areas. The CHRC gives the airport assurance that people who are in there on a daily basis have no disqualifying convictions, and thus reduces insider threat. By training the workforce and sensitizing them to aviation security issues, you expand the challenge area, and have additional trained security ‘eyes and ears’ who may be able to interdict a field side

² FBO - Fixed Base Operator, a commercial enterprise that has entered into a lease agreement with the Department to provide services such as aircraft fueling and oil dispensing; aircraft parking, tie-down and hangar storage; Airframe, power plant and accessory service; air charter services and flight instruction.

Aviation Security – Filling the Gaps

penetration of the Secured Area from other areas of the airport.” To minimize unbudgeted costs and ID office workload, this can be phased in over perhaps a year.

A multi-layered security system includes layers composed of policies and procedures, which define required personnel behavior as well as aspects of individual security awareness. Traditional personnel-based security measures, such as a rotating “buddy system” (no single person can occupy sensitive areas or perform sensitive tasks), can be applied on an airport-specific basis to strengthen security where there is risk of insider threat, such as for some aspects of baggage handling. An additional 15 minutes or so of security awareness and procedure training can easily be added to the TSA-required SIDA training classes, and can be tailored for the particular category of attendees. Certainly it’s a bother to go beyond the mandated generic training, but it’s also a low-cost and low-effort means of adding additional layers to existing security.

The great potential of personnel-based security actions is that people are in every part of the civil aviation system. There is no other resource that is as pervasive and flexible as people are. People can be deployed much more quickly than just about any type of technology—all that’s required is their willingness and a bit of training or instruction.

Paul Foster mentions one example of where the security awareness of individuals is vital: “It’s always an ongoing battle to keep the airport perimeter ‘clear zone’ clear. Technology can help somewhat, but ultimately it depends upon the initiative of the many people involved.”

The increased utilization of existing personnel is probably the most cost-effective and universally available resource for filling many of the existing gaps in aviation security. Across the boards in aviation security, how we utilize our people is a big factor in whether we do aviation security poorly or well.



Ray Bernard is Board Certified as a Physical Security Professional (PSP) by ASIS International, and is the principal consultant for [Ray Bernard Consulting Services \(RBCS\)](http://www.go-rbcs.com), a firm that provides high-security consulting services for public and private facilities. Ray is a technical consultant and writer who has provided pivotal direction and technical advice in the security and building automation industries for more than 15 years. For more information about Ray Bernard and RBCS go to www.go-rbcs.com or call 949-831-6788.
