

Note: This version of the article contains an additional four pages of material than what appeared originally in print in the October 2001 Edition of Security Technology & Design magazine, due to magazine space requirements. The article is based in part upon an airport security analysis from a July 2001 study conducted by Ray Bernard Consulting Services concerning airport security risks and the ranking of airport crimes and law enforcement effort. Although the analysis was performed prior to September 11th and the formation of the Transportation Security Administration; the threats and conditions identified are still valid although heightened airports security has eliminated the organized crime activity at checkpoints. Mark Denari, at San Francisco International Airport at the time this article was written, is now (2006) Manager of Aviation Security and Public Safety for the San Diego Regional Airport Authority.

Security vs. Freedom: Helping Civil Aviation Strike the Balance

By Ray Bernard

“These events have redefined Civilian Aviation Security forever,” said Mark Denari, Manager of Aviation Security and Special Systems at San Francisco International Airport (SFIA), regarding the recent terrorist attacks on the World Trade Center and other U.S. targets. But should a *civilian* aviation system be expected to withstand *acts of war*?

Not many days ago this would have been a purely academic question. These are questions that we ask not only as protection professionals and engineers but also as a society, a society whose very purpose is individual liberty, and a society that holds no value higher than the value of human life. These are no longer academic questions.

Helping to protect human life, and to protect important physical assets, is what the security industry has been about since before its official inception. The growth of the security industry is a reflection in part of the growth of the threats to our lives and liberty.

The recent tragic events did not stem from a failure of technology. As security professionals already know, it takes a combination of people, programs and technology to adequately implement security, based upon a realistic idea of the security needs. A failure or shortfall in any one of these elements can mean a failure of the entire system.

In testimony before Congress on September 21, 2001, Kenneth M. Mead, Inspector General for the U.S. Department of Transportation, described the “vulnerability of the of the current security system.”¹ See the sidebar “Inspector General’s Address”.

[Sidebar]

Inspector General’s Address

The following are excerpts from Inspector General Mead’s testimony before the House Transportation and Infrastructure Aviation Subcommittee.

We have been reporting on aviation security for at least a decade and have made numerous recommendations for strengthening the system covering a broad range of issues within the security system: advanced security technologies, passenger and baggage screening, airport access control, and cargo security. In the last several years alone, we have issued reports showing vulnerabilities with screening of passengers; checked and carry-on baggage and cargo; access to secure areas of the airport; and issuing and controlling airport identification badges.

¹ “Statement of The Honorable Kenneth M. Mead, Inspector General, U.S. Department of Transportation”, Report Number CC-2001-306, Page 1, http://www.oig.dot.gov/item_details.php?item=575.

We also have conducted numerous criminal investigations resulting in prosecutions involving the falsification of airport identification, security screener training records, and background checks. Most recently, a private security company was placed on 36 months probation and ordered to pay over \$1 million in fines and restitution for failing to conduct background checks and falsifying training records on employees staffing security checkpoints at a major U.S. airport.

The horror and tragedy of the September 11, 2001 terrorist attacks, with the loss of thousands of lives and the resultant economic damage, illustrates the vulnerability of the current security system. It also shows that our transportation systems, in this case aviation, can be used as a weapon against us. The aviation security system, as a vital national security interest, is a critical line of defense, but it is not foolproof, particularly against terrorists who are willing to die in their criminal schemes. This is why the effort to stop terrorist attacks along with the strengthening of transportation security is so important.

Given the scope and complexity of the security challenge as we now know it, coupled with a longstanding history of problems with the aviation security program, we believe the time has come to consider the option of vesting governance of the program and responsibility for the provision of security in one Federal organization or not-for-profit Federal corporation. This entity would have security as its primary and central focus, profession, and mission. Under the current system, those charged with aviation security oversight and regulation (FAA) and those charged with providing the security (the airlines and airports) are themselves facing other priorities, missions, and, in some cases, competing economic pressures.

A centralized, consolidated approach by an organization with a security mission would require passenger and baggage screeners to have uniform, more rigorous training, and performance standards applicable nationwide. The employees of this entity would not necessarily need to be Federal employees, but would be required to meet established performance standards, and would be subject to termination if they do not perform. This should result in more consistent security at our Nation's airports.

A Federal organization or Federal corporation would be responsible for screening passengers, employees (anyone with access to the aircraft or secure areas of the airport), carry-on baggage, checked baggage, and cargo. It would also issue, control and account for identification media at airports nationwide; search aircraft and airport facilities with canine units; and manage airport access control systems.

The organization could also include the current Federal Air Marshals; and could take over responsibility for developing, purchasing and deploying advanced security equipment, such as explosives detection equipment. The organization, not the airlines, FAA, or airports, would determine when the security equipment should be used to screen baggage and be responsible for the maintenance and upgrading of this equipment.

This entity would also be able to maintain close ties to the intelligence community, revise requirements or procedures without going through a lengthy rulemaking process, require employees to be U.S. citizens and have background and credit checks, and provide screening personnel better salaries and a career path.

Any change in the governance and organization of this system will require careful analysis, cannot be done overnight, and will require a transition period. In the interim, we must sustain the current system and improve security measures now in place.

[End of Sidebar]

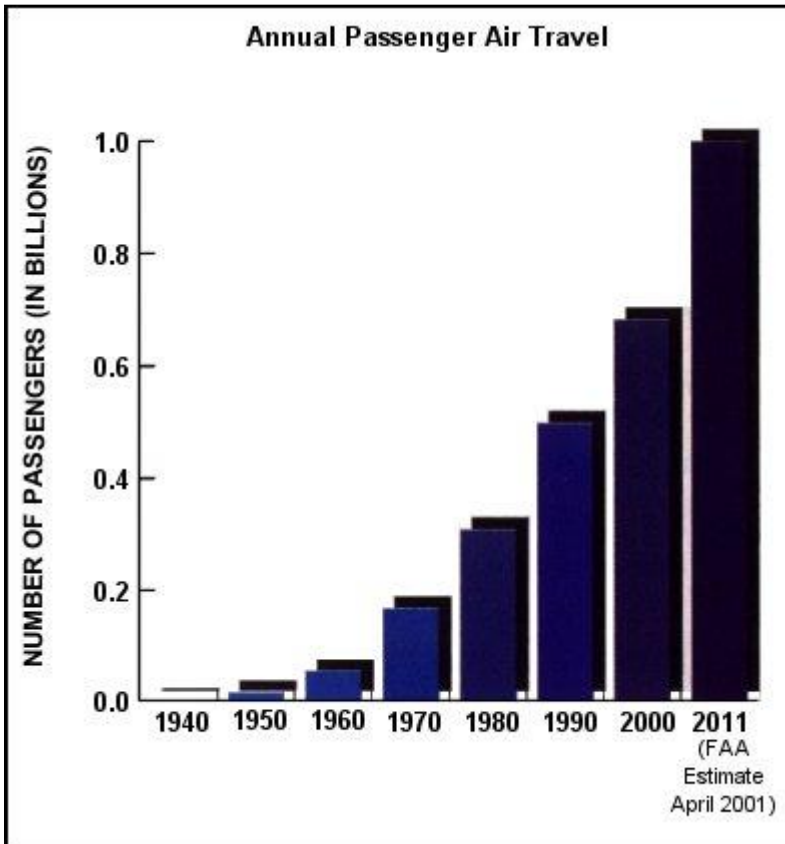
Airport Security Summit

In response to growing awareness that aviation security needed strengthening, the first annual 3-day Airport Security Summit conference was held in San Francisco this summer, produced by World Research Group of New York City, and chaired by SFIA’s Mark Denari. The title of the conference was, “Strengthening Your Security Efforts Through Best Practices and The Latest Technologies.”

Hijackings and terrorism were two of the key agenda topics at this conference, which began on July 30th, less than 45 days before the recent terrorist attacks took place.

In one sense the Airport Security Summit conference was born out of the tremendous success of U.S. civilian aviation, and the collection of challenges (of which security is only one) that this success presents to airports and air carriers. Figure 1 shows the annual increases in passenger travel since 1940, including the FAA’s estimate for 2011.

Figure 1



In focusing on the recent tragic events, we must not lose site of the immense achievements that have made today's levels of commercial air travel possible. Nonetheless, it is now abundantly clear that America's civil aviation system security needs strengthening both from within (airports and airlines) and without (federal government agencies).

Law Enforcement View

As would be expected, the recent events have caused a great deal of attention to be placed on the anti-terrorist aspect of aviation security. To do a proper assessment of security needs and security technology requirements requires a much more complete view of the security issues.

Figure 2 is a diagram of the categories of criminal threats that confront aviation security.² It includes the various groups and agencies that have responsibility for managing security related to each category of crime. The categories are:

- **Opportunistic Crime** – Dishonest people or small time criminals who can't resist the opportunity to profit from an easy "take".
- **Employee Crime** – Individual employee internal theft or baggage pilfering.
- **Individual Career Criminals** – Individual instances of purse theft, theft of a bag, or theft of items from an easily accessible automobile.
- **Organized Theft Rings** – This is organized theft of cash and credit cards, mostly at checkpoints. The cash or cards are taken out of the purse or bag, which is left on the conveyor or table. It takes seconds only. By a telephone call to others in the theft ring, up to \$10,000 can be charged on the cards within minutes. The cards are immediately discarded after the call is made.
- **Organized Transportation Rings** – Drugs, weapons, stolen goods, and other contraband are transported in various ways.
- **Organized Terrorism** – Explosives and weapons detection is the primary purpose for checkpoint screening.

It's ironic that one of the security measures in place for one category of crime, terrorism, has actually created the opportunity for another category of crime, theft at checkpoints. In some airports this is roughly 30% of the crime encountered at the airport.

Officer Bruce "Bruno" Choueiri of the Las Vegas Metropolitan Police Department explained that career criminals would even case out their victims at the casinos, and follow them to the checkpoints where they know they will be separated from their belongings.

² Thanks go to the Los Angeles Airport Police and the Last Vegas Metropolitan Police for providing information and discussion about the nature of airport law enforcement activity.

Figure 2. Airport Security Crime and Enforcement.



Complex Security Picture

Airports have a much more complicated security picture than shopping malls or office buildings. Due to the wide spectrum of possible crime there are many companies and agencies that are involved in airport security.

According to Captain Ronald Boyd at Los Angeles International Airport, “Organized criminal activity requires a very high level of cooperation between local law enforcement and federal agencies. This is a very key factor, and it’s not always easy.” As shown in Figure 2, five federal offices can be involved depending upon the type of crime. Airports, airlines and security screening companies also have primary security roles.

Looking at this picture it’s easy to see why the U.S. Department of Transportation has proposed creating a single Federal entity that would be responsible for all security at airports, and would take over security responsibilities from the airlines. The stated benefit would be to allow airlines to concentrate on their main purpose, passenger service. However, airlines would still have operational security requirements, and would be required to establish security training for their personnel. So in practice the airlines can’t be completely removed from the security picture.

Security Challenges

Regardless of who performs the security management, the security challenges remain the same. Composer, writer and entertainer Steve Allen is remembered most often for his comedy, even though he was a very serious student of the humanities and an active philosopher who often addressed audiences regarding important social issues of the day. Fifteen years ago Allen recorded these words from a speech he gave in 1971 concerning social change, “It is perhaps the primary task of this century to determine if the inherent contradiction between *freedom* on the one hand and *security* on the other can be reasonably balanced.”³ This is an issue that has come to the forefront periodically throughout the history of our country.

Since the FAA began publishing aviation security regulations airports and airlines have been struggling to achieve a workable balance between fast, efficient and unrestrictive service, and reasonable levels of security.

Some of the chief concerns voiced at the Airport Security Summit were:

- What can be done about the reluctance of budget-makers and budget-approvers to spend money on security related programs and technology?
- What can be done to raise the traveling public’s tolerance for security screening and other security measures?
- Since more than 90% of security failures are due to human factors, what can be done to lessen the role of human factors in airport security?

Negative impacts on security budgets were expected to come from the anticipated FAA 2001 budget cutbacks and the fact that most airlines were losing money for the first time

³ Steve Allen, *How to Make a Speech* (New York: McGraw Hill Book Company), p. 151.

in a decade. But given the recent events, it would be reasonable to expect that security budget barriers will be quickly overcome one way or another.

Even without budgetary restrictions, the challenge yet remains to accomplish the balance between important new levels of security and the levels of streamlined, efficient and unrestrictive service that today's sophisticated travelers have learned to expect.

As a result the aviation industry has the following general challenges for security technology:

- Significantly improve deterrence, prevention, and detection of criminal activity
- Make the application of security technology faster and more reliable
- Make the application of security technology less obtrusive and invasive
- Make airport security less dependent upon human factors

Security Initiatives

John Becker, Assistant Commissioner of Security & Information Systems at O'Hare International Airport, has been extremely proactive in implementing security at O'Hare. "O'Hare is the largest airport in the world," explained Becker. "In 1991 we handled more passengers than all but four of the airports will handle at their facilities in a year. That's why we were the first to implement an integrated security system that combined access control and security monitoring, ID badging, and 911 emergency response systems all into one office. While you can find off-the-shelf software that can integrate those functions today, nothing like that existed back in 1991. So our system was a \$54 million system using custom software developed for us by TRW. Today we could accomplish the same thing over again for significantly less. But we wouldn't go without those systems regardless of the cost, because we needed them." Becker intends to keep O'Hare's security strong by continually advancing it. Becker is not alone in this approach.

Los Angeles International Airport has recently launched a program to implement advanced use of CCTV technology that would allow the Airport Police to view activity in their cars and on handheld devices, according to Captain Boyd.

Al Krisch, Airport Security Administrator for McCarran International Airport in Las Vegas, explained that McCarran is expanding the use of their CCTV equipment to include broadcasting of captured video to selected checkpoints, terminal gates and Flight Information Display System boards. The FIDS board video display will include text asking, "Have you seen this person? If so call this number ..."

Most airports have CCTV initiatives of one kind or another on the drawing boards or already being executed that go beyond what is required by the FAA.

Some air carriers have also been implementing security improvements, although many carriers have a policy of not discussing their security programs. Some initiatives are too obvious to escape comment, like those involving passenger-screening points, which are obvious and in plain site.

"Continental Airlines has renovated a large part of its terminal space at Newark International Airport, increasing the number of passenger screening lanes, and adding a

brand-new CCTV system to provide full coverage of the screening areas," explained Reggie Baumgardner, Senior Regional Security Manager for Continental Airlines. "All cameras signals go to a Loronix Information Systems, Inc. digital recording system in Continental's newly built Security Command Center at the airport. This project, which establishes a higher level of security for our screening points, is the new standard for upgrades of other Continental terminals."

By increasing the capacity of the screening points Continental also improves the speed of service, something that is important to airlines, airports and passengers.

It also demonstrates an important point about the conflict between the demand for fast and unrestrictive service, and the restrictions required for security: *maintaining very high levels of service in spite of the security measures increases the cost of security.*

Proactive vs. Reactive

The recent Airport Security Summit was a forum not only to share information about the existing security improvement programs, but to brainstorm about how airports can be proactive in forwarding airport security.

Historically, advances in airport security have been reactive. The significant security initiatives have been prompted by major security incidents, usually resulting in Congressional action that ultimately directs the FAA to respond to the new assessment of aviation security requirements.

Attendees at the Airport Security Summit met in the hope of breaking out of that cycle.

Part of the problem that airport security managers face is the fact that national security issues and the threat of terrorism make it difficult to assess how far to take security initiatives. Previously it has been up to the FAA to take that lead. Furthermore, the cost of anti-terrorism technology is extremely high compared to other security technology. For example, the CTX-5000 explosives detection machines have previously cost about \$1 million each. Thus the FAA has also provided financial grant assistance for such equipment.

However, many security challenges have been identified that don't require input from the FAA in order for airports to take action. The challenges fall into these categories:

- Access Control/Personnel Identification
- Checkpoint Screening
- Baggage Inspection/Baggage Matching
- Perimeter Security
- Responding to Security Incidents

These are areas where technology has great value.

Access Control/Personnel Identification

To eliminate the problem of stolen or counterfeit badges being used for unauthorized access, some airports such as San Francisco International have already begun deployment of biometric systems, such as the Recognition Systems hand reader.

A primary weakness of door and gate access control is its typical dependency upon the human factor to prevent tailgating. Security revolving doors exist that incorporate anti-tailgating/anti-piggybacking features. Sally ports have been used successfully at airports to provide reliable automated vehicle access control. Baltimore Washington International Airport has had success using the Fastlane Door Detective, which utilizes an infrared field across a doorway to monitor the passage of every individual passing through the door and generate an alarm if more than one person attempts passage.

Smart card technology is getting national attention and is currently being suggested for use in a national ID card program, in which the multiple-use ID card would be used for passenger identification. Smart cards can incorporate biometric information, which makes them high-security as well as high-tech.

Another point of challenge is reconciling fire code requirements with security requirements, for example, with regard to controlled doors that must also serve as fire exits. Delayed egress technology is currently used to address this issue. It's also an issue with regard to checkpoint design, which must be compatible with emergency evacuation procedures.

Checkpoint Screening

A primary tool to combat checkpoint theft is CCTV. When used with a digital recording system to speed video review and searches, it has the added customer service benefit of being able to quickly resolve false incidents of missing items such as where one family member has picked up another family member's item. When a sufficient number of cameras are used that all activity in the screening area can be recorded, thefts are recorded and the video record can be used as evidence. When video displays are installed so that passengers and potential thieves are made aware of the cameras, the cameras can be a significant deterrent.

Checkpoint cameras are also a primary point to use facial recognition against a database of known terrorists, a technology in which airports now have a renewed strong interest.

Baggage Inspection/Baggage Matching

San Francisco International Airport is the first airport to implement an integrated Checked Baggage Inspection System (CBIS), which is part of the new 2.5 million square foot international terminal complex, the largest international terminal in North America. It has 24 wide-body gates, and 128 common-use ticket counters. Its baggage handling system includes 7 miles of conveyor belts. The system is able to perform 100% x-ray of all outbound international bags. If x-ray technology determines that the bag is suspect, it is further selected explosives detection screening (EDS) examination. This level of baggage scrutiny is far in excess of what is required by the FAA. The system uses Single Chip Systems/Ultra Electronics 2.45 GHz tag-reading system for bag routing. Encoders at the ticket counters write data onto the tags, which are then attached to the bags. Screening of bags that are selected for EDS examination are automatically routed to the detection equipment, which is completely out of sight of passengers. This eliminates ticket counter personnel having to confront passengers regarding selected baggage inspections. It has also reduced the contract security staffing requirement by 50%, providing a significant return on investment.

The SFO International Terminal features the highest level of security for international travelers found anywhere in the world. Furthermore, it processes 5,000 people each hour through U.S. Customs and Immigration, making SFO's federal inspection process among the most efficient in the U.S.

Technology for automated matching of bags with passengers has not yet evolved to the same level of sophistication and ease of use as automated baggage checking, but it remains an area of strong interest to airports.

Common Use Terminal Equipment

The SFO International Terminal is also the most technologically advanced terminal in the country, featuring one of the largest "common use" environments of any airport in the U.S. The common-user system allows different airlines to share ticket counters and gates, providing unparalleled customer service and efficiency. A wireless Ethernet system allows international travelers to remain connected while traveling.

What makes the SFO International Terminal baggage-screening initiative remarkable is the fact that under FAA regulations it is the airline companies, not the airports, which have responsibility for baggage screening. So why did the airport undertake this initiative? By providing common use baggage screening equipment, costs can be shared by the airlines, making a higher level of technology and security available to all airlines at a lower cost than if each airline were to independently try to establish a similar system.

An Airport Business Philosophy That Supports High Security

One reason that San Francisco International Airport has been able to step well beyond the FAA requirements is that it has a business philosophy designed to support the establishment of high standards for service and security.

The City and County of San Francisco's appointed Airport Commission operates the airport as a separate enterprise department of the city. The airport is an independent economic entity and receives direct taxpayer revenue.

The following underlying commercial philosophy continues to govern the Airport:

- *The Airport sets the standards for all Airport facilities and operations.*
This approach allows the Airport to set the highest standards for customer service, safety, security and efficient operations.
- *The Airport realizes the full economic value of its assets.*
Airport assets are defined to not only include our land and facilities, but also the right to access Airport passengers. Under this approach, the Airport has undertaken virtually all facilities constructed at the Airport since 1981. Further, facilities under long-term leases in many instances were bought out by the Airport.
- *The Airport maximizes the efficient use of its facilities.*
By owning facilities and controlling Airport standards, the Airport can maximize facilities usage and profits while limiting inefficient capital investments.

By including clearly-defined security objectives in its business planning, and by integrating security into operations in ways that facilitate high levels of service, SFO enables itself to excel in both service and security.

San Francisco International Airport Launches 100% EDS Initiative

During the week of October 15, 2001, SFO launched a \$50 million initiative to make it possible to use explosives detection screening (EDS) for ALL bags, international and domestic. They would be the first airport to do 100% EDS screening of all bags. Rather than wait for an FAA directive in this regard, the airport is establishing a task force to work out how this can best be accomplished as quickly as possible.

SFO has a distinct advantage over many other airports for two reasons. First, they already perform 100% x-ray screening and selective EDS screening of ALL outbound bags in the new International Terminal. They know the issues involved in implementing the kind of baggage handling system required. Second, the SFO business model minimizes red tape and encourages airport initiative for the airport's sake and for the sake of its airline tenants and passengers. They are able to define objectives and mobilize personnel without the hindrance of typical governmental bureaucracy.

Perimeter Security

Baltimore Washington International Airport utilizes a perimeter intrusion detection system that includes underground coaxial cable and microwave technology to provide a one-way alarm barrier for vehicle traffic. It allows vehicles to exit, but not enter the secured area. This type of technology is very helpful for managing cargo areas.

Responding to Security Incidents

Time is of the essence in real-time security response, but it must be *informed* response for security personnel to be maximally effective. The ability to transmit a video image of a suspect to security personnel can make or break the ability to recognize and apprehend the suspect. The ability to publicly display a suspect's image can speed the location of the suspect and can also act as a deterrent.

After the fact, documentation of the incident is of high importance. If the suspect is apprehended, the video record of the crime is essential for prosecution, and in almost all cases results in a plea bargain, reducing court appearances and their attendant expense.

Deploying Security Technology

The importance of thorough assessment, evaluation and planning cannot be overstated.

SFO's Mark Denari is a strong proponent of rigorous assessment and evaluation as part of security development. "In the past security has often been a fix or an add-on superimposed upon existing operations", said Denari. "This can result in strain on the people involved and can also detract from the normal levels of service. When deploying technology, the people and programs parts of the picture must be considered in order to achieve maximum success and maximum return on investment."

Evaluations Must Be Thorough To Avoid Creating New Problems

Security assessment and evaluation can often omit a critical step: a re-evaluation to take into account the new risks and problems that may be introduced by the proposed security measures. This is a process that may have to be performed in several iterations.

One example is the institution of passenger screening points. The separation of passengers from their belongings creates an opportunity for crime that didn't exist previously. That calls for additional security measures due to the created risk, both preventive (such as attentive security personnel and/or police, and public displays of video camera signals) and remedial measures (recorded video that can be used as evidence).

Due to recent events, biometric systems are getting high attention and rightly so. However, it would be a mistake to think that the solution is as simple as putting biometric access control at critical doors, without thinking through the consequences. Biometrics alone won't prevent a piggybacked entrance.

Right now it may be possible to steal an ID card, say from off a worker's winter jacket during lunchtime, and have a half-hour or so of time in which to use the card to access the airfield before the theft may be noticed. The use of biometric access control would prevent that scenario, but could it possibly introduce a worse one?

That's what happened with auto theft, which was reduced by the use of many types of anti-theft devices. Serious car thieves were left with only one option – steal a car out from under the driver. Thus there has been an increase in car-jacking in the U.S. and in some other countries as well.

It is not very likely that a drug smuggler would risk exposing his activities by forcing an authorized person to open a biometrically secured door at gunpoint. The chances of successful escape would be minimal. However, a terrorist could easily resort to such a tactic. We must ask, what other additional security precautions must also be put into place?

Some airports use a combination of access control, intercom, duress devices, motion-activated CCTV recording and alarm-based zone lockdown to provide a more complete door security solution. Such advanced technology solutions require thoughtful integration into security programs, including appropriate training and security drills for personnel.

Another technology that opens the door to additional risks is smart card technology. Quite apart from the civil liberty issues involved in a national ID card program are the risks of information misuse. Smart cards can store large amounts of identification and other information, and so should not be implemented without giving sufficient consideration to safeguards appropriate for the intended use of the technology.

Low-Tech Solutions Have a Place

In the rush to apply technology, sometimes low-tech solutions are overlooked. Supermarkets prevent confusion about whose goods are on the checkout conveyor belts by using flexible rubber markers to separate one shopper's goods from another's. Would a similar approach at passenger screening points, perhaps using color-coded separators, make it easier for passengers to locate their belongings and facilitate supervision of the

process by security personnel? Are there other simple ways to improve that aspect of the passenger screening process?

Another advantage of low-tech solutions is that they are often low-cost, and can help counterbalance the use of other more expensive technology.

Advanced Systems Can Provide Operational Benefits

One category of advanced technology is that which performs “smart real-time processing” of data, such as video technology that can detect when a walking person has fallen down or has changed direction. This type of capability is increasing the value of CCTV systems by allowing them to perform more than the typical visual monitoring and recording function. Motion-triggered video alarms can be used for economy in video recording, so that doors or escalators areas are only recorded when there is actual activity in the area. This can speed video review time as well as reduce video storage requirements.

Soon video systems with software-based monitoring stations will be able to perform advanced functions on a workstation-by workstation basis. For example, a manager who wants to track snow removal progress will be able to mark an area of a camera image and be notified when the area turns from white to gray. If that change doesn’t happen within the user-specified time frame, an alarm would be generated. The same feature could be used to monitor critical no-parking zones, or even plane arrivals and departures at the gates.

Thus when assessing potential return on investment from advanced security technology, its operational benefits should also be taken into account. This is not a new concept; for example, many access control systems have been used for time and attendance tracking. However, given the general advances across the boards in security technology, exploring technology operational benefits ~~technology~~ should be a standard part of any security evaluation.

Database Utilization: Improving Security and Service

One aspect of security technology that will be getting more attention at airports is the use of external databases or shared databases to improve security. It can be seen from Figure 2 that database links to Federal systems (ATF, DEA, FBI, INS and Customs) and local law enforcement systems (City, County and State) would cover the full spectrum of known criminals that the airports have to contend with. Different databases would be appropriate depending upon the type of usage. Human resources may need to access records of all known felons to support its hiring practices. Airport screening checkpoints would perhaps use only the set of known (or known and suspected) terrorists.

The use of personal information databases raises the “freedom vs. security” issue, an issue that Americans don’t take lightly. In peacetime we generally prefer more freedom and less security. Now that our peacetime living has been attacked by terrorism, we may tend to favor increased security. If that happens, how long will that preference last?

The utilization of personal information databases means that special attention must be given to their use. That applies not only to external databases, but also to data that is accumulated within the airports.

For example, expect to see limits on how long recorded video information can be kept. Except for video records of criminal activity, video storage limits will probably range between 48 hours to 30 days, depending upon the type of activity being recorded. The exact nature of video monitoring, along with the disclosure of storage practices, may well become a standard public disclosure item for airports and airlines.

One possible outcome of the “freedom vs. security” issue may be the institution of two levels of service. It may be that faster security screening will be provided to persons who participate in traveler ID programs, whether or not they utilize a national ID card. This would put the decision to participate in such a system in the lap of the customer, making it a “freedom vs. service” issue for the customer rather than a “freedom vs. security” issue for airports.

However a computerized ID system is only one part of the three-part “people, programs and technology” triangle. As already mentioned, for technology implementation to achieve a successful result all three parts must be addressed. For critical systems, a way of routinely testing the system and verifying its operation must be included in its implementation, and the review of such test results must become part of the responsible agency’s audit procedures.

The two terrorists who flew American Airlines Flight 77 into the Pentagon escaped existing detection systems (CAPS, IBIS and NAILS, see below), due to holes in the “people, programs and technology” aspect of their implementations. For example, CAPS is only utilized for passengers who have checked luggage, and the terrorists didn’t check any luggage.

Traveler ID Systems

A number of traveler ID systems are already in use:

- **APIS** - *Advanced Passenger Information System*. The INS obtains biographical passenger information in advance of passengers arriving at select U.S. Ports of Entry. This allows the INS to expedite passenger processing and enhance overall enforcement. Over 66 percent of all passengers have been inspected using APIS in 2000, and at least 67 carriers are now signatory to the APIS Memorandum of Understanding.
- **CANPASS** - *Canadian Passenger Accelerated Service System*. This is the Canadian equivalent of the U.S. INSPASS system, See below.
- **CAPS** - *Computer Assisted Passenger Screening*. This program is used to select baggage for explosives detection examination or expanded bag matching. CAPS uses information from the reservation system to screen out passengers for whom additional security procedures are unnecessary. If not enough is known about a passenger to make a judgment, then additional security measures in the form of explosives detection device screening or bag matching is applied. CAPS also selects some passengers at random for these additional security measures. This is the computer system that has been discussed recently on various news programs.
- **ETAS** - *Electronic Travel Authority System* is Australia’s advanced and streamlined travel authorization system. The ETA is an electronically stored

authority for travel to Australia for a short-term tourist or business entry. It replaces the visa label or stamp in a passport and removes the need for application forms. ETAs are issued within seconds of being requested through computer links between Australia's Department of Immigration and Multicultural Affairs (DIMA), travel agents, airlines and specialist service providers around the world. Recently ETAs were enhanced to include the capability for a traveler to apply for an ETA over the Internet.

- **FAST** - *Future Automated Screening for Travelers*. FAST is the Future Automated Screening for Travelers program, currently involving the participating countries in the Visa Waiver Pilot Program (VWPP – see below), which will allow travelers to use automated passport inspection stations.
- **IBIS** - *Interagency Border Inspection System*. This system consolidates lookout databases from more than 20 Federal agencies. It is used to identify and process individuals who may be inadmissible or removable from the U.S. or subject to other enforcement actions by another agency. Last year over 150,000 intercepts were performed based upon IBIS data.
- **IDENT** – Initially created by the U.S. Navy in order to help process the Haitian refugees in 1992, the IDENT system is currently being used as part of a federal effort to decrease the number of illegal aliens entering the United States. IDENT allows the Border Patrol to take a digital print from the index finger of each hand and a digital photograph of each illegal entrant over age 14 who is apprehended by the Patrol or INS agents. By using IDENT, Patrol agents began identifying illegal aliens who were new entrants, recidivist entrants, convicted felons, and smugglers known as "coyotes" who run operations along the borders.
- **INSPASS** - *Immigration and Naturalization Service Passenger Accelerated Service System*. INSPASS is an automated system that can significantly reduce immigration inspection processing time for authorized travelers. INSPASS combines automation with a hand geometry biometric image, to validate the claimed identity of an individual. INSPASS is currently installed in 6 U.S. and 2 Canadian airports, and INS has plans to add 11 more U.S. and 2 Canadian airports. Enrollment in INSPASS is available to citizens and permanent residents of the U.S., Canada and Bermuda, plus citizens of 29 countries that participate in the Visa Waiver Pilot Program. More than 20,000 INPASS inspections are conducted each month on average, about 72 percent for U.S. citizens. There are more than 45,000 active enrollees, and each traveler uses INSPASS an average of about four times annually. The INS does not exchange enrollment data with other nations; travelers need to provide separate enrollment information to each country.
- **NAILS** - National Automated Immigration Lookout System. NAILS is run by the Immigration and Naturalization Service and contains the immigration agency's list of deportees and other undesirables, as well as the State Department's classified tip-off list and leads from other agencies. NAILS is used by INS, U.S. Customs and the U.S. State Department.

- **SENTRI** - *Secure Electronic Network for Travelers' Rapid Inspection*. SENTRI is an Immigration and Naturalization Service (INS) system used for speedy pre-clearance of travelers crossing land borders. SENTRI is the world's first automated dedicated commuter lane, using advanced Automatic Vehicle Identification (AVI) technology modified to meet the stringent law enforcement needs at the border, while at the same time reducing congestion. INS and U.S. Customs use SENTRI to accelerate the inspections of certain low risk, pre-enrolled crossers at ports of entry. SENTRI is currently implemented in California, Michigan and New York.
- **VWPP** - *Visa Waiver Pilot Program*. VWPP enables citizens of participating countries to travel to the U.S. for tourism or business for 90 days or less without obtaining a U.S. visa. The Visa Waiver Pilot Program is administered by the Attorney General in consultation with the Secretary of State. There are 29 participating countries in the VWPP, including: Andorra, Argentina, Austria, Australia, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, The Netherlands, New Zealand, Norway, San Marino, Slovenia, Spain, Sweden, Switzerland, and United Kingdom.

As of this writing Canada has suspended use of the CANPASS system until further notice to heighten security in the wake of the Sept. 11 events. Other systems may also be suspended or may be augmented by additional security procedures.

Close examinations of the usage and results of the existing traveler ID systems should provide valuable information for use in evaluating future utilization of automated ID systems.

The Future of Airport Security Technology

Currently airport security is very complex picture in need of simplification. Much of the task of simplifying it lies outside the realm of the security industry.

Certainly security technology can be intelligently deployed to help reduce or eliminate various types of crime at airports. Airports, air carriers and travelers would all be happy to have would-be thieves driven out of airports. Hopefully wherever they would be driven to, law enforcement will be ready and waiting.

The eradication of organized criminal activities requires actions from outside the perimeters of airports, as well as from within them. Advanced technologies can be used to help eliminate opportunities for criminal activity, by prevention and detection, so that airports are no longer attractive targets for drug smuggling or terrorist actions.

If large commercial airports are successfully fortified will organized criminals and terrorists simply move to smaller, less-protected airports? Questions like this point out the importance of thoroughly evaluating security consequences not just within individual airports but also across the entire civil aviation system.

One very direct way to help contribute to the future of aviation security is to participate in the FAA's Third International *Aviation Security Technology Symposium* in Atlantic City, New Jersey, November 27 – 30, 2001. More information is available online at www.safeskiesinternational.org.

While long-term solutions are being evaluated, and short-term solutions are immediately being put into place, here are ways that we can help:

- Refrain from presenting advanced security technology as “silver bullet” solutions, no matter how impressive their capabilities.
- Continue working to simplify the deployment of technology.
- Consider the context in which security technology will be used, designing to help speed customer service in that context wherever possible.
- Continue to develop products and systems that support fast and informed response by security personnel.
- Include audit trails and system verification features in computerized systems, to help users confirm that their systems remain secure and are not being misutilized.
- Anticipate that systems which record information, including CCTV systems, will be subject to information storage and handling rules and policies; build in ways to set up appropriate rules and policies, along with means to verify that they remain in place.
- Provide products and systems that help eliminate security dependencies on human factors issues, or that mitigate the impact of human failures.
- Explore the opportunities for open system protocols and for expanding product compatibilities; this makes investment in security technology safer and makes integration across customer system boundaries a possibility.

As security professionals, now more than ever before our knowledge and skill will be called upon. Our diligence in applying ourselves to our tasks, in doing a thorough and complete job, and in taking into account the full context in which security technology is to be deployed will result in sound airport security applications that help safeguard lives and protect valuable assets.



Ray Bernard is board-certified as a Physical Security Professional (PSP) by ASIS International. Ray is the principal consultant for Ray Bernard Consulting Services (RBCS), 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.
