

Technically Speaking

airport security

The Rules Have Changed Since September 11

A SPECIAL REPORT FROM CARTER & BURGESSES

THE GATEWAYS TO air travel, our airports, became outdated on September 11, 2001. That day brought painful issues to the forefront that the aviation community must deal with:

- Terrorism is unrelenting
- The terrorist threat evolves
- The societal costs from security failures are staggering and unacceptable

As the aviation community works to increase security, all aspects of air travel are funda-

mentally changing. Entire airport functions and resulting configurations are being modified. New terminal designs will be dramatically different because of operational changes dictated by increased security measures.

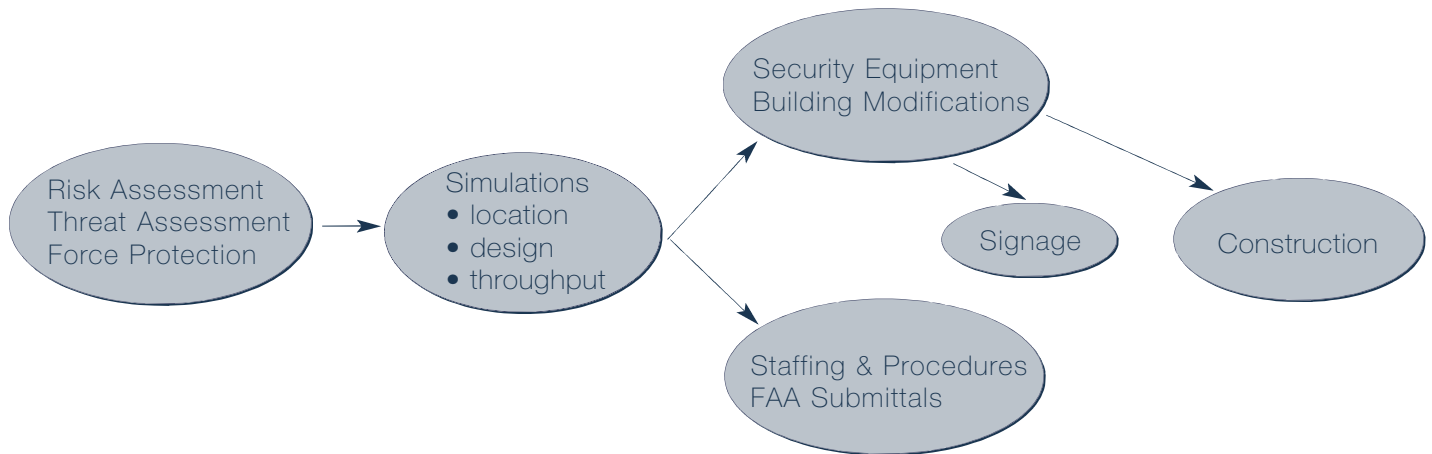
The question facing airport officials, however, is what those changes will be. The Aviation and Transportation Security Act specified important modifications to airport security processes. New passenger and baggage screening requirements include:

- matching all checked baggage to passengers on that flight (bag-matching does not initially extend to connecting flights)
- more trace detection and manual searches of carry-on items, including shoes, for explosives

No part of airport security has been scrutinized more in recent years than baggage screening and processing, and now in the wake of the September 11 attacks, baggage handling has become a key issue in commercial aviation security.



Carter & Burgess *Package Delivery of Integrated Security Solutions*



- increased wand searches and patdowns of passengers passing through security checkpoints
- additional verification of passenger identity at boarding gates
- additional passenger screening and searches of carry-ons at boarding gates
- transfer of all passenger screening to federal employees by November 19, 2002
- examining every piece of checked baggage for explosives, using EDS equipment or manual search, by the end of 2002

Combined with evolving guidelines for protecting terminals themselves against bomb attacks, these mandates have put severe time and financial pressures on airport authorities to respond within the deadlines for implementation. The speed of new rule making has left airports with undefined requirements and guidance.

In addition to new rules, airport officials must deal with a sea of other uncertainties:

- Anxious travelers
- Weakened air carriers
- Softened revenue streams for parking and concessions
- Nervous creditors and rating agencies
- A flood of new security technology with limited testing

These uncertainties tempt airport officials to wait “until things become clearer,” especially since millions of dollars are involved in the decisions.

Understandably, officials don't want to spend money in one direction if a regulatory or technology change could soon render that investment worthless. On the other hand, not providing automated bag screening and going to slower manual searches at the end of this year would significantly reduce departure rates at an airport. The revenue consequences of not being able to process baggage searches to support aircraft operations are far greater than the costs of making the facility upgrades.

Though the security challenges and uncertainties that face airport officials are daunting, they are not insurmountable. Proven security principles can be applied to all aspects of an airport's organizational processes, facility designs and operational procedures. This can create an enhanced security posture without making airports into fortresses, discouraging air travelers or breaking the bank in the process.

Successful security depends on the integration of operational processes, organizational structure and staffing, and facility systems to meet threats. Fundamentally, these measures must be oriented to specific threats and the tactics of those threats. This presents a significant challenge because, as noted earlier, threats mutate in response to security measures. This fact has several critical implications for the airport community.

First, superior intelligence is essential, and is gained only through continual, close communications with federal and local law enforcement



agencies. Airport security officials – the link to other law enforcement agencies – have a vital role in the design process, and successful designs will reflect close coordination with those officials.

Second, the design of airport facilities must be flexible to allow for additional changes as new measures are required in the future. This change, which particularly impacts the design and construction of airport facilities, conflicts with the highly optimized terminal designs that until recently sped travelers from rental car turn-in to the airplane seat. New security measures have made the process longer in duration and in distance: more screenings mean more time passing through security, and enforced parking rules extend walking distances. These, of course, can inhibit travelers and make other modes of travel relatively more attractive. Now and in the future, security will be at the heart of every airport process, so the challenge for terminal design is to understand not only how travelers and their baggage move through an airport but also how security measures must be applied at each stage. Successful designs will anticipate and accommodate modifications to those security processes.

Lastly, information technologies will be key to integrating an airport's intricate and complex security systems and processes. Never before has aviation had such an extreme requirement for

quality controls in every aspect of its operation. Equipment and procedures for screening must be operated with a zero tolerance for “down time.” Any incidents undermine passenger confidence and economic performance of the airport. Performing at this level requires computerized simulations of these operations, computerized tracking of checklists and incidents, and real-time, multiuser tracking of implementation of upgrades to these facilities and operations. Successful designs will be those that understand and anticipate that information technology will continue to gain prominence in the overall airport security posture.

adapting existing airports

WHILE TERMINALS OF the future will be able to incorporate security considerations as the driving force in design, existing terminals, built on the old model of speeding travelers to their airplane seats, must be reconfigured now to meet these still-evolving threats. Making the right modifications requires careful preparation.

The process for re-evaluating airport security involves ongoing threat identification, identifying the alternatives to address these threats, evaluation of alternatives, development of systems that support the process, establishing operational procedures including training, and finally, modifying the buildings and infrastructure to support these new systems.



The process begins with risk assessment and threat planning, then moves to the simulation phase where each of the alternatives is tested and refined. From there, the process splits with equal focus on the actual facility modifications, and on the systems and people who will make the process work. Only when all of those issues are clearly established does the actual redesign work of terminals begin.

Once the objectives of airport terminal redesign are identified and a general plan begins to take shape, there are three areas of opportunity where security upgrades will be aggressively developed in the coming months and year:

- Information technology tools – sharing data and upgrading telecommunications infrastructure to support a higher level of real-time communication and coordination
- Screening tools – more intensive screening of more passengers at security checkpoints, and the important and daunting challenge of screening all baggage for explosives
- Facility upgrades – structures that support the systems and must themselves be threat-resistant. Blast protection must be provided both at the face of the building and in areas designated for checking suspect bags. The infusion of technology requires extensive upgrades to a facility's power grid and data infrastructure, which in turn involves design of new enclosures and reconfiguration of existing ones.

information technology tools

HIGH ON THE LIST of all future airport security initiatives will be the gathering and sifting of information about passengers, private vehicles on airport property, service vendors' employees and even the planes themselves, both on the ground and in the air. In essence, an entirely new information-based management structure is being created.

"It's dazzling to see how quickly the private sector is coming up with new solutions," said James Coyne, president of the National Air Transportation Association, at the Federal Aviation Administration's third International Aviation Security Technology Symposium.

The event, planned before the September 11 attacks, drew more than twice as many people as it did five years ago – a testament to concern about the security practices that allowed terrorists to hijack and crash four jetliners, and underscoring how those attacks had changed an industry conference into a matter of national security.

FAA Administrator Jane Garvey told conference participants that technology's role depends on its universality and its effectiveness in the field.

"There is no one answer that holds the key," she said. "We must look at the technology to build layers of security." Garvey likened the current need to build public/private partnerships to the call on industry made by President Roosevelt at the onset of World War II.

Improving security will require re-examining each step in the process, analyzing the sequence and adding steps that have never been there before. There will be unprecedented sharing of data between the airlines, law enforcement officials, airports and the FAA. For example, law enforcement has lists of people to watch. The airlines don't have these lists and, in fact, will no longer be screening passengers.

Among the new security technologies that are already being put to use:

- Columbus (Ohio) Airport recently selected Cross Match Technology's ID 1000 Live Scan Fingerprint System as an additional security measure. The airport is one of the first Category One airports to purchase this type of system to satisfy new FAA security guidelines.
- Salt Lake City International Airport recently completed installation of an ExitSentry system in the Terminal 1 checkpoint. The video surveillance system detects and immediately alerts security guards to the "wrong way" motion of people attempting to enter the concourse through the exit lane. Similar systems have been installed at 16 other North American airports, including Lambert-St. Louis International, Orlando International, Dallas Love Field, Cleveland Hopkins International, Houston Hobby Airport and Calgary (Alberta) International.
- Dallas/Fort Worth International Airport announced plans to begin a "face matching" database pilot program using video cameras in terminals to compare people viewed with a database of known suspected terrorists. This process was successfully used by security personnel at the January 2001 Super Bowl in Tampa, Fla.

Another security tool is an ASP Web-based Airport Integrated Mapping System that provides real-time multiuser access to a wide range of database information and maps of airport facilities. This is a great example of Garvey's public/private initiatives, because these systems were first developed to support private companies with accelerated national rollout programs. These and customized Geographic Information System applications can be used by airports, airlines and the FAA to monitor a multitude of critical issues, including status of terminal upgrade projects,



operations status, passenger demographics, gate and space utilization, and security system status.

Applications such as these will also help eliminate “stovepiping,” when a department or group of people has information or a database that isn’t shared with other groups. This can create duplication of effort because data is collected and formatted multiple times rather than done once in an agreed format, offering universal access. A single database allows tracking of anomalies as compared to what is normal, and generating of ongoing updates.

Many technology-based security aids can be incorporated now, but there is always a question of information overload. As more information is added to the evaluation procedures, it will be even more difficult to separate “signal from noise.” These new protocols illustrate why a network that speedily transmits data from many remote sources into these information repositories is paramount. Unfortunately, high-speed communication backbones don’t exist in many airports, but new methods of deploying fiber optic cables, such as Maryland-based CityNet’s in-sewer technique, is making the process fairly easy in busy settings that cannot handle a lot of surface disruption from trenching and construction.

screening tools

NO PART OF AIRPORT security has been scrutinized more in recent years than baggage screening and processing, and now in the wake of the terrorist attacks, baggage handling has become a key issue in the effort to maintain commercial aviation safety.

The recently passed Aviation and Transportation Security Act requires that all checked bags must be screened using explosive detection systems (EDS) by the end of 2002. This is a profound acceleration of the 12-year timeframe for 100 percent EDS screening that the FAA had been proposing. This goal requires the addition of 1,800 to 5,000 more EDS machines at airports throughout the country. As of December 2001, fewer than 200 such machines were deployed at airports nationwide.

The FAA has been developing a program called Argus, a smaller, less-expensive version of EDS. Once certified, Argus will be suitable for use at small airports because it requires less physical space. The FAA has fully funded the research and development for three vendors in the Argus program, and all three are expected to complete the certification process in time to be deployed by the screening deadline.

The 100 percent security screening of baggage also poses unprecedented challenges to facility designers. When trying to reconcile baggage flow peaks and acceptable passenger service levels with the relatively low throughput capability of tomographic type devices, the airport designer is faced with allocating large amounts of floor space to this crucial activity.

Adding to the challenge is the diagonal baggage dimension limits intrinsic to tomographic devices. This constraint generates an entirely new class of oversized baggage that must be specially handled and cleared in addition to the more traditional

Currently, the government, by providing technology and oversight and the recent assumption of baggage screening, is footing a large portion of the security upgrade bill, but not all of it. Airports will certainly have to dig deeper to pay for some of the tools, technology and modifications of their terminals, although some of that cost will be reimbursable.



oversized items. Other security technologies must be used with this type of baggage, adding to the space allocation problem for equipment, security personnel and the traveling public.

The first airport likely to come into compliance with the new requirements is San Francisco International Airport. Because the new airport terminal was designed with security in mind, they were able to quickly implement a plan. The first new CTX machines ordered by the Transportation Security Agency will go into SFO, because they were ready. Shortly behind them is the Dallas/Fort Worth International Airport, which quickly mobilized a tiger team to study alternative locations for these large, heavy devices. In late February, DFW authorized two large design contracts to modify their terminals to accept this equipment. Carter & Burgess will design modifications to terminals A and C, and the design will be organized to prepare for bid packages to allow construction to start as early as possible. All modifications will be constructed by September 30, 2002. Contracts for design modifications to terminals are being executed in many cities including, Denver, Washington, Houston, Los Angeles and Boston.

With so many issues to resolve and a short timeframe in which to do so, there are no models or experiences that won't be studied and evaluated. Passenger safety and the financial viability of air-

lines and airports are at stake, and it will take the input of all parties involved to create a new system that works for commercial aviation.

facility upgrades

WHEN IT COMES to redesigning terminals themselves, the unthinkable must be anticipated. Risk assessment, systems protection and greater explosive blast protection are essential. For example, many airports have large amounts of non-blast-proof glass which could shatter into thousands of lethal shards in the event of an explosion. Understanding these risks and designing ways to protect people and systems is a high priority.

Modifying physical layouts and enhancing the structural integrity of terminal facilities to manage new security mandates and new security infrastructures will, like upgrading technology, be a never-ending process. This will demand long-term construction management principles that incorporate constant review and adjustment as part of the process.

Space allocation in terminals also must change radically. True meeter/greeter halls are a necessity when only ticketed passengers are allowed beyond security; the focus on retail amenities only in secured areas will have to change; and upgraded electrical service and telecommunications cabling

counting the cost of secure airports

Security costs money – lots of money. Though the exact costs are still unknown, increased airport security will run into the tens of billions, if not more, at a time when airline and airport revenues and the federal budget are already stretched thin. Who should pay and when funds will be available have concerned lawmakers, airport managers, airline officials and passengers.

The federal government is footing a large portion of that bill, though the exact sum is yet to be finalized. In addition to grants and guaranteed loans to the airlines, the Air Transportation Safety and System Stabilization Act of September 21, 2001 ensured funds for airport security and authorized \$120 million for the Essential Air Service program to aid air service in small markets. The Aviation and Transportation Security Act of November 2001 authorized \$1.5 billion for security cost reimbursement, but as of this writing the appropriation is not yet implemented. An additional \$175 million for Airport Improvement Program (AIP) in the pending Department of Defense budget designates funds “to compensate airports for a portion of direct costs associated with new, additional or revised security requirements imposed on airport operators,” and the Airport Improvement Program of the FAA also expects \$3.3 billion for fiscal year 2002. For 2003, the president has requested \$4.8 billion to implement the Aviation and Transportation Security Act, and \$8 billion in overall Department of Transportation funds for improving transportation safety in all areas. The FAA is also

requesting \$3.4 billion for airport improvement appropriations in 2003. As of this writing, however, Congress is still grappling with the total cost for technology and oversight, and for the equipment and personnel to conduct baggage and passenger screening in 2002.

As of February 1, 2002, U.S. passengers began contributing to the cost of air safety with a passenger security fee of \$2.50 per U.S. flight segment (up to \$10 per ticket), but this covers only a small part of the overall cost for aviation security. The increased presence of local police at airport terminals and parking garages has posed a financial strain for city budgets.

Airports large and small will certainly have to dig deeper to pay for some of the tools, technology, and modifications of their terminals, although some of their costs are reimbursable from federal funds. Major airports need to acquire sufficient bomb detection equipment to keep baggage operations flowing smoothly in peak times, while smaller regional airports, which so far have had no bomb detection equipment, need to acquire machines or work out acceptable – usually labor-intensive – alternatives such as manual searches of all luggage. While some airports are able to cover these costs up front and await reimbursement from federal appropriations, some midsize and smaller airports have no choice but to wait for federal funds.

are needed to support the increased number of cameras and electronic screening devices. Power and data systems themselves will need higher levels of security. And space must be made for command centers that oversee security, operations, and data flow.

Before any structural changes are made, simulations must be performed to assess each threat and ways to defend against it. How, for example, would a terminal structure handle a bomb detonated in a parking garage, or in the passenger dropoff lane? Are some areas of the terminal particularly vulnerable to instantaneous or progressive collapse? Such questions mean changes not only for terminals but for parking and vehicle traffic and passenger movement through the entire airport.

In addition to “what if?” questions, simulations can resolve known problems, such as the revised flow of passengers and baggage through the various screening processes. Increased passenger screening requirements have rendered the current space allocations and traffic flow patterns for security pavilions inadequate. Improved passenger screening involves more lanes of metal detectors and screening equipment for carry-on items, as well as more tables and waiting space for removing laptop computers and coats, hand-search of carry-ons, and for screened items to accumulate while passengers themselves are being wand searched and patted down. Passengers need stools for removing shoes for examination, and as threats mutate and government employees assume more security functions, even more changes are likely such as “trusted traveler” cards that prescreen some individuals. Time and motion studies would help to determine where the passenger screening process slows down, where it needs even tighter controls, and where greater space and personnel allocations would improve flow.

Simulations are also crucial to ensure that all checked baggage is properly screened. Much of the EDS equipment currently in airports is not optimally located, and the flow of passenger check-in bottlenecks as passengers move or accompany their checked baggage from ticketing counters to distant screening machines to baggage conveyor belts or back to the ticket counter. Even before additional EDS equipment is delivered, simulations are needed to determine the best placement of each machine for passenger and baggage flow and to assess whether the structure can support the enormous weight of the machines. Modeling of baggage and passenger flow through the new system may reveal additional problems, all of which must be addressed before actual design work begins.



When it comes to redesigning terminals themselves, the unthinkable must be anticipated. Developing protective models to reflect greater explosive blast protection, risk assessment and systems protection is essential.

carter & burgess provides airport security solutions

AS A PRODUCT OF more than 60 years of experience designing and developing airports, Carter & Burgess has assembled a carefully selected team of employees and strategic vendors that provides comprehensive safety and security analysis, facility design and project implementation services based on up-to-date FAA requirements and knowledge of other industries, including military, government and commercial. Our experience providing threat assessments, force protection, and systems protection for Department of Defense facilities around the world is being offered to our commercial aviation clients.

The Carter & Burgess facility evaluation process focuses on all aspects of airport security review and re-execution. Carter & Burgess combines multidisciplinary aviation design and construction expertise with expert capabilities.

Comprehensive services include:

- Threat assessment and risk planning
- ASP web-based airport integrated mapping system
- Facilities design, including structural, MEP, and telecommunications
- Information technology consulting
- Adaptive reuse of military facilities
- Construction management and program management
- Airfield design

Consistently listed at the top of a variety of industry rankings of Engineering/Architectural/Construction Management firms, Carter & Burgess is a full-service firm offering consulting services to the communication, transportation, land development, public works, retail and building industries. The firm has been in continuous professional practice for more than 60 years. Over the last 10 years the firm has experienced rapid, sustained growth, and has expanded geographically to office locations in every region of the country.



Presorted
Standard
U.S. Postage
PAID
Ft. Worth, TX
Permit No. 2265

www.c-b.com

Arlington, TX817.860.8887	Las Vegas, NV702.938.5400
Atlanta, GA770.951.0020	Little Rock, AR501.223.0515
Austin, TX512.314.3100	Los Angeles, CA	
Baltimore, MD410.727.6773	Commerce323.890.9380
Boston, MA617.225.0200	Encino818.784.7585
Chicago, IL		New Haven, CT203.771.6883
Downtown312.578.9252	New York, NY212.354.3675
Warrenville630.393.7790	Oakland, CA	
Cleveland, OH216.803.1813	Broadway Street510.465.8400
Columbus, OH614.221.7300	Frank H. Ogawa Pl.	510.457.0027
Dallas, TX		Oklahoma City, OK405.810.8254
Elmbrook Drive214.638.0145	Orange County, CA714.327.1600
Mockingbird Lane214.920.8100	Orlando, FL407.514.1400
Denver, CO303.820.5240	Phoenix, AZ602.263.5309
Detroit, MI248.633.1440	Portland, OR503.535.8036
Fort Lauderdale, FL954.958.0300	Raleigh, NC919.783.5988
Fort Worth, TX		Sacramento, CA916.929.3323
Main Street817.735.6000	Salt Lake City, UT801.355.1112
Meacham Blvd.817.222.8500	San Antonio, TX210.494.0088
Greenville, SC864.329.8500	San Jose, CA408.428.2010
Honolulu, HI808.523.9696	Seattle, WA425.822.7096
Houston, TX713.869.7900	Tallahassee, FL850.877.8711
Indianapolis, IN317.945.1810	Washington, D.C.202.776.7718

Carter & Burgess Architects/Engineers, Inc., Carter & Burgess Consultants, Inc., C&B Architects/Engineers, Inc., C&B Architects/Engineers, P.C., C&B Nevada, Inc., and Nixon & Laird Architects/Engineers, P.C., are entities related to Carter & Burgess, Inc.