



THE 9/10/11 PROJECT



AVIATION
SECURITY

Are We Ready for the Day Before Tomorrow?

Imagine it is September 10, 2011 – 9/10/11 – a full decade since the devastating terrorist attacks of September 11, 2001. Is our nation equipped for whatever catastrophe may happen tomorrow? How have our prevention, preparedness, response and resiliency structures changed, matured and become operational?

The Homeland Security & Defense Business Council's 9/10/11 Project looks at how far the country has come since the day before 9/11/2001. Through fresh interviews with industry leaders the Council is seeking to vividly illustrate the strides our government at all levels, working with the private sector, has made to secure the country and to stay at least one step ahead of events and disasters that could destroy our way of life.

On the 10th of each month between now and through September 2011, the Council will provide a historical context for how far we have come and where we are now, as well as an assessment of the future of the most pressing homeland security issues. Each monograph will include a running timeline (interactive on our website) illustrating the events, incidents, and critical government responses pertinent to that month's topic. This month's monograph focuses on where it all began: The events leading up to, and culminating in, 9/11's effect on Aviation Security.

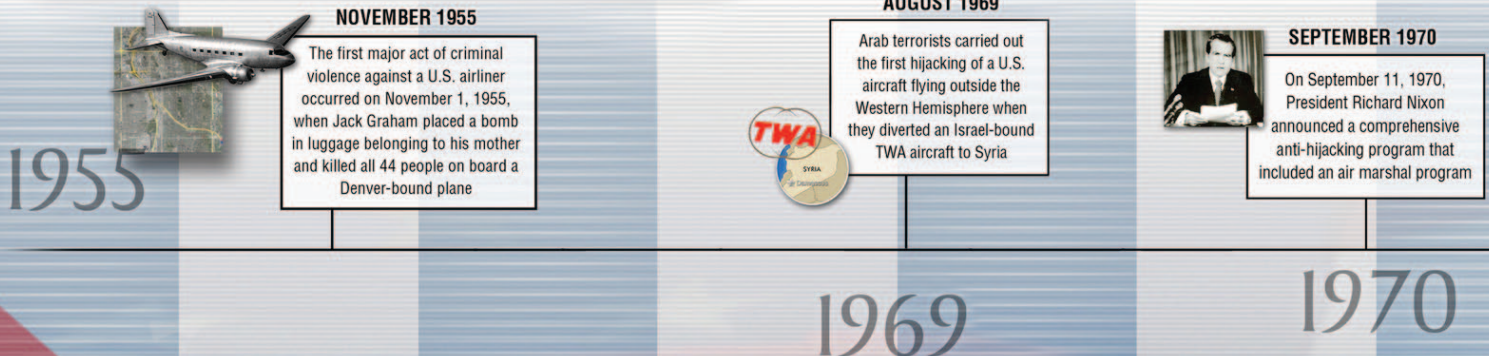
Where We Were

On September 10, 2001, the Jones family decided to take a spontaneous cross-country trip to Disneyland. It wasn't particularly hard to purchase the tickets, and though a new school year had recently started, the parents felt that their children were young enough to miss a couple of days without much of an adverse effect, and besides—the rates were cheaper. So, with their 7-year-old son and 3-year-old daughter in tow, John and Mary Jones went up to the ticket counter, bought four tickets, told the airline clerk that they had, indeed, packed their own bags, and then those same bags were checked to California. The family gathered their personal belongings and trooped through the obligatory metal detector (as did friends, who had taken them to the airport and were seeing them off at the gate).

The metal detector they encountered was the only evident security around. The machines were a remnant of, primarily, a series of politically-oriented hijackings that took place from the late 1960s through the late 1980s. It was no big deal to go through them, and in fact, some didn't even work. The airlines controlled the detectors, but usually hired out the screening work, so contract workers waved the family through without much scrutiny.

On that bright September 10th, though, the family had nothing but fun on their minds. Before too long, hugs were exchanged and the family was finally onboard their Boeing 767 enjoying a smooth, carefree flight all the way to California. Jimmy, the 7-year-old, got to visit the cockpit, and his sister, Suzy, received some wings from an airline attendant. The captain strolled through the cabin greeting customers. The sky was clear.

The next day dawned beautifully, too, with the East Coast crystal clear and bathed in sunshine. But on that Tuesday, four commer-





One Anomaly Among the Chaos

An airport is in constant motion. It was just one person among thousands going through airport security that day. Except that a person dropped a small bag before going back through the line and out the front door of a major international airport.

The bag was enough to catch the eye of a security guard at the gate but operators in the central control room were already on red alert: The motion of the person walking backwards through the line and the bag left on the floor had triggered alarms in the video surveillance system. Immediate action to assess and manage this relatively subtle situation ultimately put a stop to the plans of a terrorist organization.

Optelecom-NKF provides proven and customized IP and hybrid video surveillance solutions for any application. We make safety and security effective, simple, and hassle-free.



www.siqura.com/vca-47

by Optelecom-NKF

cial airliners were used in an unimagined and unprecedented way—fully fueled planes were made into bombs by Al Qaeda terrorists and flown directly into New York’s World Trade Center and the Pentagon in Washington, D.C. (with the fourth plane presumably headed at our nation’s Capitol). Thousands of innocent and unsuspecting people were killed that day – just for being on an airplane or for going to work. September 11th forever changed this country. The nation, stunned and scared, wept.

For three days no commercial flights flew in an eerily empty sky. Military jets roared high over Washington, D.C. and New York City. In D.C. an occasional military helicopter also passed over. But on the ground, silence and fear reigned.

The Jones’ weren’t able to go to Disneyland for a couple of days because it was closed hours after the attack, so Mr. Jones was almost relieved when he learned that no flights would be going anywhere for three days. At least, he thought, his frightened children would finally get to see the park and maybe have some fun, even amidst the collective grief that permeated the nation.

Initial Steps – Government and Industry’s Response

Events make history; history spurs technological innovation; and the private sector provides solutions.

On September 20, 2001, then-president George W. Bush addressed a joint session of Congress, proposing a new Office of Homeland Security. Because we had been attacked from the air, top private-sector minds from aviation and security were quickly brought together and a “go team” was set up. The events of 9/11 began to further mold aviation security. In what Marcus Collier of General Dynamics calls “the fastest retrofit of commercial aviation that was ever done,” all U.S. airliner cockpit doors were sealed and bullet-proofed by October 7, 2001—within one month of the attacks.

To further ease the public’s fears, armed National Guard troops were deployed at many airports. Thousands of contract-security workers

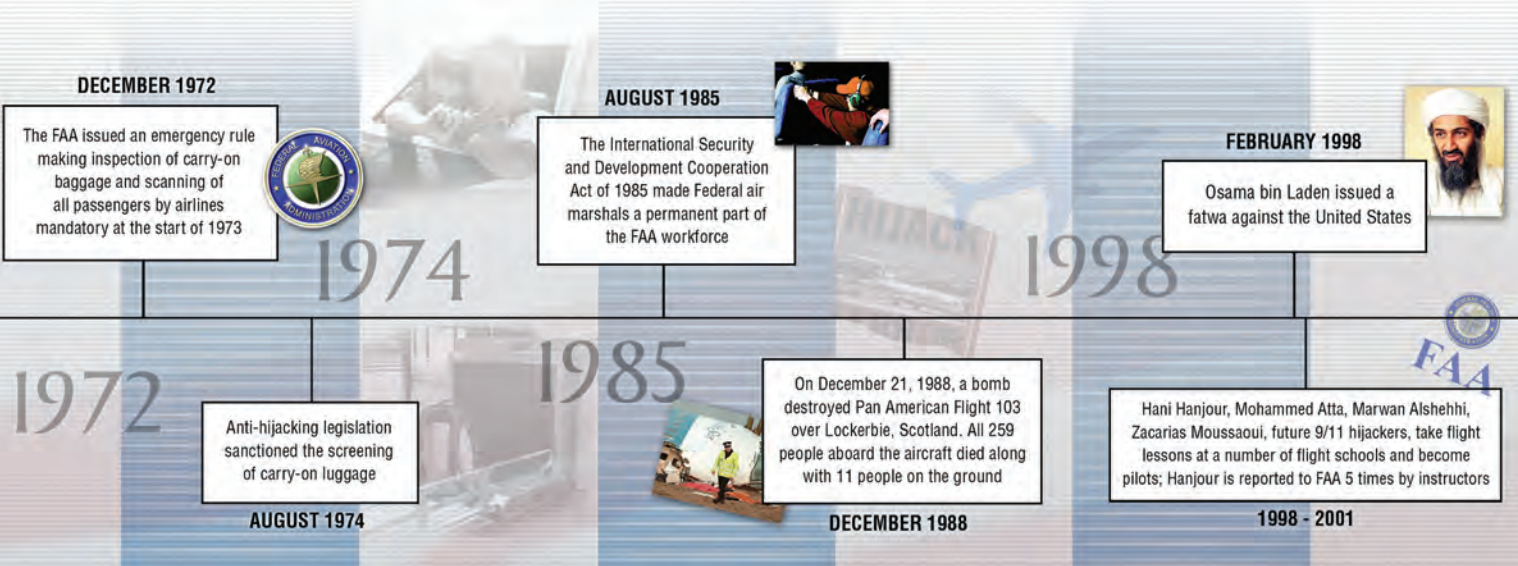
were hired and trained to be baggage screeners; private-sector technologists began the innovation process to counter these new threats, both seen and unseen.

On November 19, 2001 Bush signed the *Aviation and Transportation Security Act* creating the Transportation Security Administration (TSA), which would work under the Department of Transportation. It was stood up from scratch with the help of companies like Deloitte, Lockheed Martin Corporation and Booz Allen Hamilton, and was to employ the latest and most sophisticated technologies. Moreover, it had no entrenched bureaucratic culture to impede its mission. It has always had a very clear mission and a common culture.

Fast on the heels of the TSA’s creation came the *Airport Security Federalization Act*, which, among other things, mandated background checks for airport workers, and required airport operators to establish security programs that included a military presence at each airport—including at screening locations. The Act also required more federal air marshals to be on selected passenger flights, and allowed pilots to carry firearms in the cockpit. It mandated that a system be implemented to screen all checked bags at all U.S. airports “no later than December 31, 2003,” and required the installation of explosive detection equipment to screen checked bags and cargo “as soon as possible.” These so-called systems and all the screening equipment would, of course, come from the private sector.

In another example of how events shape our post 9/11 world, Richard Reid’s failed attempt to detonate a bomb mid-flight by lighting his shoes on fire in December 2001 resulted in a new TSA requirement – removing shoes for screening. It would, however, take until 2004 before all butane and common lighters were outlawed, making the U.S. the only nation in the world to keep passengers from carrying lighters onboard – a rule that remained in place until 2007. Because Reid, the so-called shoe bomber, had tried to use explosive materials, their detection was deemed a major priority and the private-sector ramped up its work on explosive-detection equipment.

When a liquid-explosive bomb plot originating in the U.K. was uncovered in August of 2006, thankfully before the terrorists got on a plane,



most of the international community embraced the TSA's "3-1-1" policy, which reduced the volume of liquids, gels and aerosols passengers could bring in their carry-ons to three ounces or less. The rule mandated that all such bottles be put in a quart-sized, clear zip-bag, and each passenger is, to this day, allowed only one. Passengers additionally lost their ability to carry water bottles from home, including those purchased in front of the scanners, onto their flight. Mothers with newborns weren't even allowed to bring their bottled breast milk onboard.

Despite these changes, terrorists still connive to use commercial aircraft to kill. Christmas Day 2009 came very close to being the date of another horrific episode when the "underwear bomber," Umar Farouk Abdulmutallab, tried to ignite explosives hidden under his clothes. Luckily, he spent too much time in the plane's bathroom and his plot to blow up the plane over Detroit was discovered and thwarted.

Flying the friendly skies was no longer what it used to be in any way, shape or form.

Today's Aviation Security

Although passengers may carry lighters once again, most of the early rules stemming from the 9/11 attacks remain intact.

The flying public is now quite used to hearing repeated announcements encouraging vigilance, urging them to safeguard access to their luggage, to remove their shoes and belts and make clear plastic bags ready for screeners, to unload their laptops and cell phones, and to arrive at least two hours before a flight, especially at larger airports. They are prepared to be selectively taken out of line to be searched—either at the security checkpoint or even just before boarding their flight. Today, all flyers are more perceptive and aware; they are on the lookout for things we never thought of before, and they are ready to take action if necessary.

But events and attempts at terrorism, as on Christmas Day, remain a constant danger (please see timeline, below), and TSA's and the private sector's responses are forced to keep evolving in an attempt to stay one step ahead of the terrorists. Now, there are "watch" and "no fly" lists, with information gathered at "fusion centers" in order to work

on "behavioral pattern recognition." The Science and Technology Directorate, which is the primary research and development arm of the Department of Homeland Security (DHS), along with the private-sector companies are creating all sorts of solutions – innovating in gaming technology, artificial intelligence, information sharing and quicker, more effective sensors that are able to "see" right into baggage to detect exactly what materials are inside.

Those old metal detectors are still around, but today industry has evolved them into "puffer" machines that can also sniff trace amounts of explosives. All carry-on baggage is x-rayed right at the screening areas, and now it is done by a trained professional staff of some 50,000 TSA personnel, not by private security forces. If something piques a screener's interest, passengers will likely have their bags hand searched and their bodies scanned with a wand.

There are cameras everywhere, and hand-held sensors at check-in areas designed to scan and detect the gamut of chemical, biological, radiation, nuclear and explosive materials within seconds. Controversial full-body, millimeter wave scanners, which privacy groups are protesting as nothing more than a "digital strip search," are being deployed in many locations, again because of the Christmas 2009 incident. The legacy scanner couldn't see under the would-be terrorist's clothes, but a full-body scanner would have identified the explosives instantly. Recently the TSA introduced a new methodical, and some say equally invasive, pat-down for secondary searches or for those who decline screening by whole body imaging devices. TSA, now under the DHS umbrella but with its own professional staff, has—with the private sector—done much to make air travel safer. Many of these initiatives correlate to events in the timeline below and some examples of this partnership are listed here:

- Lockheed Martin Corporation partnered with TSA to train more than 54,000 passenger and baggage screeners, and provides full-service Passenger Screener Training systems and assistance to support the TSA. Lockheed also trains federal air marshals, federal flight deck officers, and state and local law enforcement officers on transportation security.

JULY 2001

FBI Agent Ken Williams writes the "Phoenix Memo" recommending collection of information on all civil aeronautics schools while investigating students with possible terrorist links

NOVEMBER 2001

President Bush signs the Aviation and Transportation Security Act, creating the TSA November 19th
President Bush signs the Airport Security Federalization Act

MARCH 2002

Egyptian co-pilot blamed for aircraft crash

MAY 2002

FBI Agent Coleen Rowley writes to FBI Director Robert S. Mueller, III about the Minneapolis investigation of Zacarias Moussaoui, his flight lessons and detention in August, 2001

2001



SEPTEMBER 11th ATTACKS

Richard Reid attempts to detonate a bomb in his shoe on American Airlines Flight 63 December 22nd

DECEMBER 2001

2002

An Egyptian man, Hesham Mohamed Hadayet, shoots and kills three people at LAX

JULY 2002

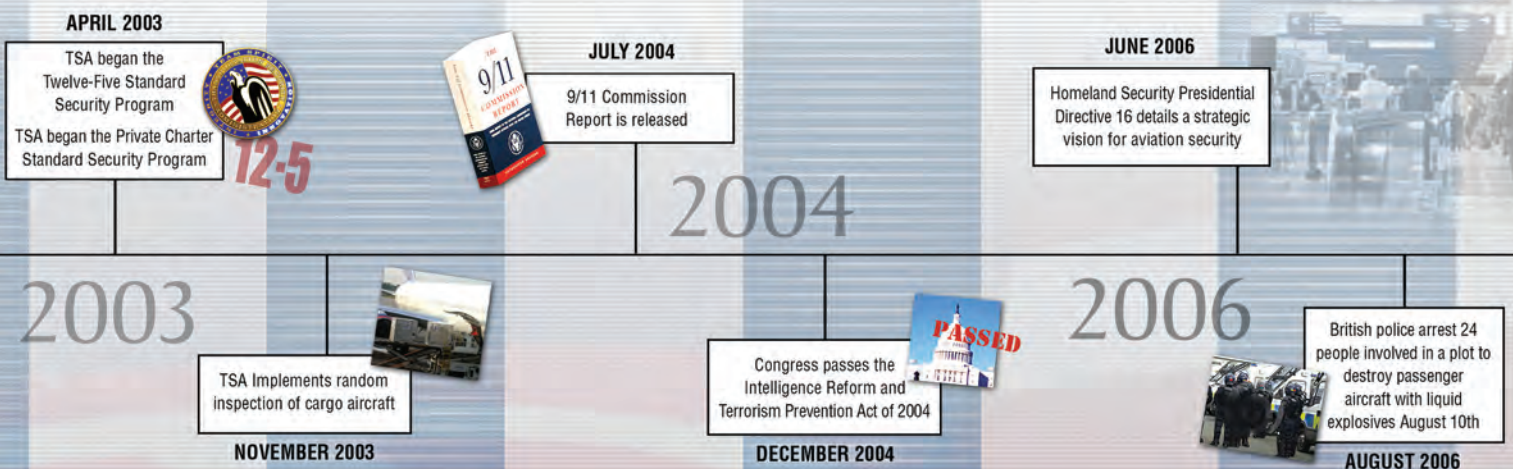


- DHS achieved 100% screening of passengers, both foreign and domestic, on U.S. airlines in June 2010, an achievement that accomplishes an important commission recommendation, which became law in 2007 (PL 110-53). (*Progress in Implementing 9/11 Commission Recommendations: July 2010 Update, page 2.*)
- IBM was a main developer of DHS' Secure Flight program, now fully operational, which shifts pre-departure watch-list-matching responsibilities from individual airlines to the TSA. Secure Flight requires that airlines get a flyer's full name (first, middle name or initial, and last, as it appears on the valid, government-issued photo ID that is presented at the airport); date of birth; gender; and redress number if applicable.
- As of May 2010, DHS was screening 75% of cargo on passenger aircraft departing from the United States, although it wasn't able to meet the August 2010 deadline for screening all cargo on domestic passenger aircraft. (This amounts to roughly 1 billion checked bags a year.) Raytheon has contracts with TSA that include cargo and baggage screening as well as perimeter security.
- In addition to installing whole-body imaging machines, explosive-material detectors and bottled-liquid scanners at U.S. airports, the TSA is investing in new explosive-detection systems and other technologies to streamline checked baggage screening at U.S. airports. DHS is also working with the Department of Energy's national laboratories to develop further technological innovations for aviation security. As an additional layer of security, 730 canine-detection teams patrol the nation's airports.
- Battelle works with the Department and conducts research and product development for canine detection teams, explosives detection, and x-ray screening, among many other tasks. Booz Allen Hamilton provides intelligence, operations, and transportation security consulting services.
- SAIC produces the *Palette VACIS*® gamma ray imaging system, through which trained personnel can spot weapons, contraband and other items of interest. It also has other aviation services such as

providing "smart cards," and biometrics as well as weapon, explosive, drug, and cargo detection systems.

- ABS Consulting provides air traffic management, security risk management and threat modeling, threat and security vulnerability assessments and security risk assessments for airports and airlines, among other work. ABS has provided services related to Homeland Security Presidential Directive 16 (Strategic Vision for Aviation Security, June 2006).
- Avaya Government Solutions has been actively engaged in supporting a number of important homeland security initiatives, including applications development, systems integration and engineering, as well as biometric systems.
- BAE Systems created a commercial airliner infrared missile protection system called JETEYE™, which protects aircraft from infrared ("heat-seeking") missiles by using an integrated suite of sensors and laser. The sensors detect any missile that is launched at the aircraft, and the laser is then fired at the missile to disrupt its trajectory, causing it to fly harmlessly away from the aircraft.
- Since the attempted bombing of Northwest Airlines Flight 253 on Christmas Day 2009, Homeland Security Secretary Janet Napolitano has been working with the U.N.'s International Civil Aviation Organization (ICAO) to improve international aviation security. The department expects ICAO members to affirm new standards and other security measures at the organization's triennial meeting in September.

These combined efforts have reaped enormous dividends. DHS's analysis of passenger data, for example, played a critical role in several high-profile terrorism cases including those of Najibullah Zazi, who pleaded guilty in February 2009 to plotting to bomb New York City subways; David Headley, who pleaded guilty for his role in the 2008 Mumbai terrorist attacks; and Faisal Shahzad, who pleaded guilty in July 2010 to charges in the attempted car-bombing of Times Square on May 1, 2010.



Are We Ready for Tomorrow?

The American people expect to fly safely and to maintain a solid economy, so the future is a balancing act between commerce, customers and safety. To succeed, we will continue to need a vibrant, responsive system that is both flexible and nimble enough to respond to new and expected threats as they occur. Innovative technologies must continue to be developed, and true security is only possible with a strong and continued partnership between government and industry.

Although there is no clear consensus as to what the ideal in aviation security will eventually be, security and aviation experts know that "Threats will always emerge, as those who seek to do harm continually look for vulnerabilities. Aviation security must be approached as a 'system of systems' with each part considered as an interdependent element of the whole. TSA addresses this through its layered approach, but it also requires each of us as travelers to remain diligent. Complacency has no place in today's national security mission," as David Patterson, president and CEO of Optelecom-NKF puts it. Smaller airports, for example, may not have the budget for advanced technological solutions, and terrorists know this.

Darryl Moody, a consultant on homeland security with Accenture who was part of the TSA's original private-sector "go team," likens airport security to dollops of peanut butter. "One of the scariest things I've heard was that I don't really need screening in Topeka; I need it in Lagos, Nigeria," he recalls. "Some argue that you put the biggest dollops 'where security is needed,' but that is everywhere. So, do I spread it out to try and cover everything, leaving less across the board? It's a very difficult problem."

It may help to revise our perspective on airports. James F. X. Payne, head of Telcordia Technologies' national security/cyber security efforts, says it's critical to "see airports and their infrastructures as a city.... We need to think more holistically." Airports are usually owned by airport authorities, municipalities, and public/private organizations while national security is run by state and federal agencies. Payne sees a strong need for more dialogue between, and technology showcases for these

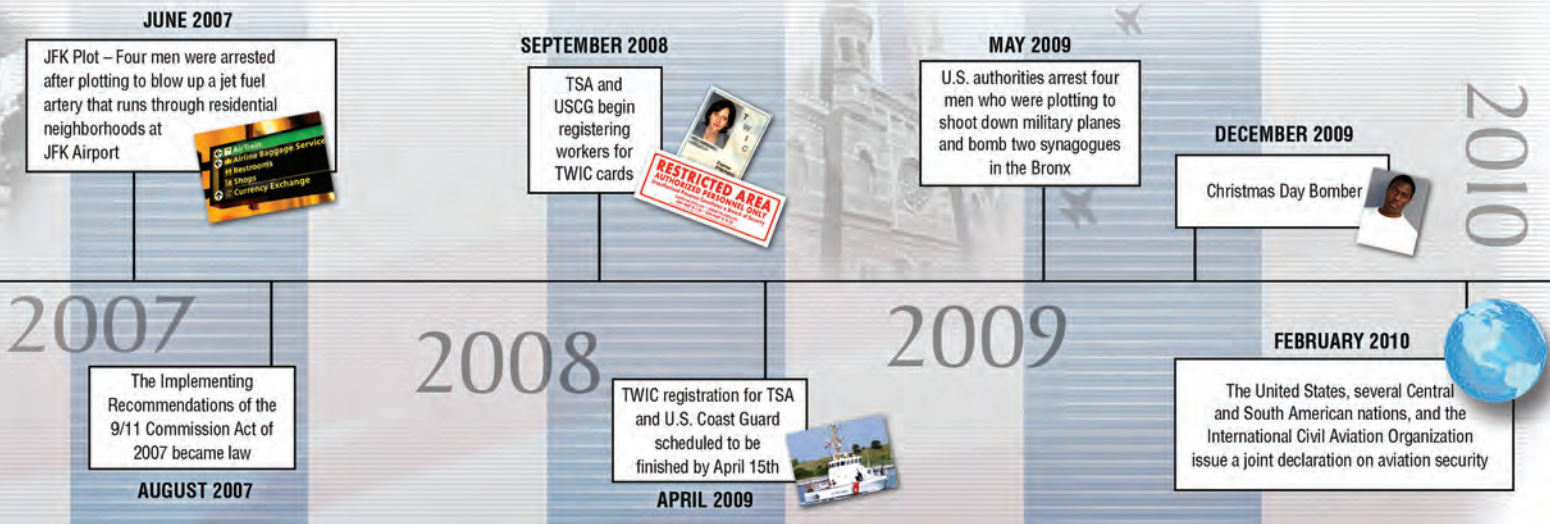
local, state and government officials tasked with securing the nation, similar to a recent HSDBC Aviation Security Technology Demonstration that took place on Capitol Hill. "It is a matter of everyone seeing what is there, seeing the realm of the possible," he notes.

That realm now includes artificial intelligence and Jeffery Freeman, vice president of Homeland Security Programs for DRS Technologies, is a strong advocate for technology wising up. "We need sophisticated imaging technologies using advanced algorithms that make sensors and cameras 'smart,' and we need to get away from a TSA operator staring at a screen," he says. "The human mind can't comprehend all that data or detect a high enough percentage of what could be dangerous items." (Many experts concur; however, in some unique cases humans [and canine teams] remain our best defenses).

Artificial intelligence is also being looked at, as is predictive analytical software, to address human behavioral patterns because historically the terrorists have always done dry runs. Michael Kelly, director, Battelle Office of Homeland Security, says that the Office of Science & Technology is experimenting with FAST, or the Future Attributes Screening Technology Lab, which, with Battelle, also involves Draper Labs. The group is looking to see if there are any indicators, such as a high pulse rate, rapid eye movement or excessive sweating, which can cause a "smart" system to say "we want to look at this person." This will require the human element, he says, because "humans make decisions; machines screen."

The airport's perimeter is equally or perhaps even more important in aviation security. Many industry experts interviewed for this article pointed out that the weakest part of an airport's security system is before passengers reach the secured area, which is past the screening zone. At most airports, the local police department is responsible for all the space up to the secure area, and TSA is responsible for all that occurs after it. Several companies are now combining machine learning, computer vision and artificial intelligence in new and viable ways to push out the checkpoints from the terminal to the curb.

Battelle's Kelly concurs that the challenge is "...the assault from the



outside, but also the ability to smoothly process passengers in an economic matter so you're not disrupting," and the airlines wouldn't disagree. Throughput is critically important for continued, unabated commerce as well. "It's going to take a while to make sensors efficient in both detection and time," says General Dynamics' Collier, "Is 10 seconds good? Maybe not, but 5 seconds is."

Collier also firmly believes that, for example, people with security clearances need not clog up the security lines, and that a biometric product like Clear™ or an identity-management card such as Eid Passport's RAPIDgate™ will speed up security lines tremendously while still insuring passenger safety. IBM's Secure Flight is a positive step in that direction.

Jack Mayer, executive vice president at Booz Allen Hamilton and leader of its work with DHS and the Department of Defense, is ultimately pleased with airport security's progress. "Having a professional workforce responsible for security at airports is a good thing," he says, "and they have become more professional over time." But, he adds that "although the probability of hijacking in the air is exceptionally small, bringing a plane down with a bomb is still a real threat." The idea, Mayer iterates, is "to layer the security and always make it more complex and uncertain for the person trying to do something bad. DHS and the world get an 'A' for doing that with air transportation security."

That said, the TSA is still a young agency with lots of growing to do. Procedures for discussions with private industry, as well as internal processes, need to be refined so that it can eventually become a mature and well-oiled machine. "Vision planning that looks five years out is critical, or we become simply reactive." DRS' Freeman says. "We need insightful forecasting, so we don't just throw money at this event or that tragedy," he adds.

The need for such vision planning was also echoed in a survey done by the Council in early 2010. Members overwhelmingly supported long-term planning that would allow industry to align its resources to achieve long-term missions. Battelle's Kelly says "It is critical to understand the entire system and what the priorities for the system are so we can look at the current state of technology and ascertain where we expect it to be in the future."

Having people in charge with experience in managing large and complex organizations, as well as in developing a strategic vision is also critical. Greg Pellegrino, Deloitte's Global Industry Leader for the Public Sector, points out that government cannot separate itself from private industry, nor be comprised of individual fiefdoms. "They must be interdependent," he says. "The more they isolate themselves from each other and from industry, the worse it's going to be when everything they are trying to do is dependent upon the private sector

and what it does." Considering that private parties own and protect roughly 90% of the U.S.' critical infrastructure, including airports, the point is powerful.

"One of the most valuable components of the public/private partnership is the priceless open flow of ideas and perspectives, and collaboration between industry and government assures that the best thoughts and concepts are applied to aviation security," says Marc Pearl, president and CEO of the Homeland Security & Defense Business Council. "Without a deep understanding between government and industry on the others' processes and interests, the nation's security is seriously at risk."

In addition, aviation security is not, obviously, just an American problem; terrorists have been actively attacking U.S. and foreign entities abroad, and today the international community is more actively contributing viable ideas and solutions, as well as acknowledging the need for similar security and screening procedures at their own airports. As Telcordia's Payne says, "It is somewhat myopic to think that all technologies are coming from the U.S. We are looking for that global vision, to get the best of the best."

Today, aviation security is but one part of an overall picture of homeland security, which also includes railways, buses and a number of other critical infrastructure areas. But, as stated earlier, events drive action. Thus, the United States began fighting the war on terror where it was hit – going after the weakness in aviation security that allowed 19 terrorists to board four planes with metal box cutters, to enter their cockpits, kill or wound their crews and turn airplanes into weapons.

Since that horrific September day in 2001, the newly created TSA, the airports, the airlines, different governmental groups, industry solution providers, and the public have had to figure out how to work together for a common goal—the safety and security of the country's airline industry and its customers. Aviation security's measure of success is seen every time an airplane lands safely and without incident—and by that measure, TSA and its partners deserve praise. A lot of people are out there working to eliminate aviation security's vulnerabilities, but we remain committed to achieving a system resilient to future threats and robust enough to withstand any attack.

The Homeland Security & Defense Business Council (HSDBC) works to ensure that the perspective, innovation, expertise and capabilities of the private sector are recognized, respected and integrated with the public sector. The 9/10/11 Project has called upon critical thought leaders and subject matter experts, including our chief writer, Vicki Contavespi. For more information on the Council's 9/10/11 Project visit: www.homelandcouncil.org/91011-Project.html

For more information on the Homeland Security & Defense Business Council visit: www.homelandcouncil.org

Homeland Security & Defense Business Council • 1140 Connecticut Avenue Suite 1008 • Washington, D.C. 20036 • (202) 470-6440

Marc A. Pearl, *President/CEO* • Kristina Tanasichuk, *Vice President & Project Director*

Using intelligent technology to counter crime



Traditionally, CCTV installations have been used to monitor sensitive areas in airports and other facilities to ensure safety and security. Operators would watch computer screens and look for unusual situations. Yet the vast amount of information collected by even a single camera makes the operator's job very difficult, requiring constant vigilance throughout a shift.

By integrating video content analysis (VCA) into existing CCTV installations, a single operator is able to oversee numerous cameras in various positions or places. These systems use intelligent algorithms to continually analyze camera images for unusual occurrences and to alert operators within seconds of the type of incident and its location.

From a centralized control center, the notified operator can visually verify and assess the situation, and react appropriately. This may entail anything from alerting mobile security personnel in the area to remotely closing off specified locations through centralized access controls, as well as informing authorities, such as the police, fire department, or emergency medical services.

This results in a powerful tool through which operators can instantly evaluate the severity of an incident and respond quickly and confidently.

Opportunity in tough times

The current economic crisis has been a wake-up call. While some companies have battled with prices, others have benefited from the opportunity to revamp their way of doing business. One such company is Optelecom-NKF, manufacturer of advanced Siqura® surveillance solutions.

Optelecom-NKF has focused its company strategy on offering its customers and the industry precisely what they need.

The simplicity of this approach has proven its success.

With over 35 years of experience, Optelecom-NKF provides global surveillance solutions to three markets: Transportation, Government, and Critical Infrastructure. Optelecom-NKF focuses its research and development entirely on producing specialized networks using mature technology that can adapt and grow with the user's needs from the very first day of deployment. By working with systems integrators and end users from the design stages through to operation, Optelecom-NKF ensures the best return on investment, leveraging legacy systems while simultaneously implementing state-of-the-art surveillance systems.



by Optelecom-NKF