A PRIMER ON AIRPORT SECURITY

Darryl Jenkins

The purpose of this paper is to discuss changes that have been mandated at airports because of the events of September 11, 2001. These changes will be compared to best practices used by Israel, Germany, and other European countries. This paper will proceed in the following manner: first, I will discuss the changes mandated by the Transportation Security Act of 2001 and signed into law by President Bush on November 11, 2001. I will then describe the airports' current security system and how it will change in the next couple of years. Finally, I will conclude with a discussion of best practices and compare them to those mandated by the law.

It is concluded that while the recent changes will have marginal benefits to the security system, it is still based on a flawed foundation: that of baggage screening rather than person screening. The biggest problem with baggage screening is that it is boring and repetitive, and therefore prone to error. As the law mandates better-educated screeners, we may actually see worse security, as the work is too mundane to hold their attention.

Another significant problem with the security procedures is that they do not take into account how terrorism has changed in the last decade. The most significant improvements in security may have come through pilots becoming non-passive and passengers becoming aggressive towards terrorism. The necessary element for airport security – that of intelligence gathering at the federal level – has not yet been addressed.

THE AVIATION AND TRANSPORTATION SECURITY ACT

On November 19, 2001, President George W. Bush signed the Aviation and Transportation Security Act (the Act, Pub.L. 107-71) into law. This comprehensive statute established the Transportation Security Administration (TSA), as well as the position of under secretary of transportation for security, and required the federal government to overhaul its approach to securing all modes of transportation.

The TSA will assume responsibility for security beginning this year. The bulk of the new agency's authority is centered on the air transportation system, particularly protecting against terrorist threats, sabotage, and other acts of violence. A core element of this aviation security regime is the screening of passengers and property at all airports that provide commercial air service.

To execute this complex function, TSA will hire and deploy security screeners and supervisors at 429 airports over the next 10 months. Based on the dual requirements of protecting the system and moving passengers who present no threat through security checkpoints efficiently, the screener workforce is likely to exceed 30,000 people. In addition, TSA will employ thousands of Federal Law Enforcement Officers (LEOs), as well as intelligence and support personnel.

Given its size, the number of passengers with whom it will come in direct contact, and the importance of its role in ongoing operations, the screener workforce represents the core of the agency. To ensure the protection and smooth operation of the aviation system, and the long-term success of TSA, screeners must receive premium-quality, intense, and measurable training on the range of responsibilities and scenarios they are likely to face. At the time of the writing of this article, the following items under the law have been carried out, and the following remain to be completed.

IN PLACE

- Increased use of a computer program that identifies potentially suspicious travelers for bag searches or interviews
- As of January 18, 2002, all checked luggage must be screened by either explosive detection machines, matching the bag to the passenger, hand searches, or the use of bomb-sniffing dogs.

- Increased use of random searches of carry-on bags
- Limits on carry-on items
- Government-issued ID necessary for boarding
- Parking and curbside access will be limited.
- Armed National Guardsmen stationed at security checkpoints
- Stricter procedures at checkpoints, including frequent hand-wand checks and pat-downs at many large airports
- FAA agents will shut down concourses and hold flights if they observe flaws in security procedures.
- Cockpit doors remain shut; flight crews inflexible about in-flight rules
- Increased presence of Federal Armed Marshals on some flights
- The FAA requires criminal background checks of all employees with access to secure areas at airports.
- Bags and passengers screened at small airports are not required to be rechecked before boarding connecting flights.

REMAINS UNDONE

- No additional training has been provided for checkpoint screeners.
- Checkpoint screeners still have no health benefits.

CURRENT SECURITY PRACTICES IN DOMESTIC AIRPORTS

Millions of people fly every day. The vast majority of them are law-abiding folks who have no intention of harming anyone. But there is always the possibility that a terrorist or a criminal is hidden among the masses. Also, many people with no intent to cause harm may accidentally carry hazardous material onto the plane. To avoid these problems, airport security is an important part of any airport. The fact that the plurality of people who pass through checkpoints will bring no danger to the

system brings us to the most important problem in maintaining security: human factors. The likelihood of any one screener ever catching a terrorist is remote in the extreme. So while terrorism causes the push for increased security, screeners will have to deal with more routine daily operational problems. Knowing this, they will lack the necessary tension to fully conduct their duties. To overcome this, audits, etc., are conducted. The problem with the previous system was high turnover; screeners never had any motivation to do their jobs well, as the job was only a stepping stone to another low-paying job. However, tension is necessary to perform these types of tasks well. It is assumed that this will always be a problem, but hopefully, it will be less of a problem in the new regime.

Since this paper is concerned mostly with terrorism, I will ignore the other security aspects like air rage, disgruntled employees, etc., and concentrate solely on preventing terrorist acts and the current and proposed procedures to do this.

If we try to imagine a terrorist attempting to blow up or hijack a plane, we need to consider all of the different techniques the terrorist might use to get a bomb into position, and whether the new procedures could stop him or her. A terrorist could:

- Plant a bomb in an unsuspecting passenger's luggage
- Smuggle a bomb in his luggage
- Strap a bomb or gun onto his body
- Walk onto the tarmac by hopping a fence and approach a plane from the ground
- Like the terrorists on September 11, 2001, work through the system as it exists and know all of its weak points

The first line of security at an airport is confirming identity. For domestic flights, this is done by checking a photo ID, such as a driver's license. When people travel internationally, they need to present a passport. Confirming a person's identity is difficult; it could be one of the greatest tasks in the new security regime. Even fingerprints cannot confirm a person's identity, but they can reveal whether or not a person was in jail. The identity portion of security is important, as it gives us leads about certain people's backgrounds. Because identity is uncertain, profiling takes on increased importance.

During the check-in process, the attendant asks security questions:

- Has your luggage been in your possession at all times?
- Has anyone given you anything or asked you to carry on or check any items for them?

While we often ridicule these questions when going through check-in, they are very important, as a tactic terrorists occasionally use is to hide a bomb inside an unsuspecting person's luggage. Another tactic is to give something, perhaps a toy or stuffed animal, to someone who is about to board a plane. That object, although it seems innocent, may actually be a bomb or other harmful device.

The Civil Aviation Security (CAS), a division of the Federal Aviation Administration, establishes guidelines and requirements for airport security. CAS has three main objectives for airport security:

- To prevent attacks on airports or aircraft
- To prevent accidents and fatalities due to transport of hazardous materials
- To ensure safety and security of passengers

FAA agents working under CAS are located at every major airport for immediate response to possible threats. Most major airports also have an entire police force monitoring all facets of the facility, and require background checks on all airport personnel, from baggage handlers to security-team members, before they can be employed. All airport personnel have photo-ID cards with their name, position, and access privileges clearly labeled. One of the biggest problems with the new security workforce is the time required to do background checks – as the law has mandated 10-year instead of five-year background checks, they will take as long as 10 months per individual.

A fence generally secures the entire perimeter of an airport. It restricts access to the runways, cargo-handling facilities, and terminal gates. However, fences are easily breached and are seldom patrolled. The purpose of the perimeter is to channel all public access through the terminal, where every person must walk through a metal detector and all carry-on items must go through an X-ray machine. Currently, checked baggage is screened only on a random basis, with the law mandating 100 percent screening within one year. This will be difficult, as the com-

panies that are now certificated to build these machines do not have the production capability to do this.

Almost all airport metal detectors are based on pulse induction (PI). Typical PI systems use a coil of wire on one side of the arch as the transmitter and receiver. This technology sends powerful, short bursts (pulses) of current through the coil of wire. Each pulse generates a brief magnetic field. When the pulse ends, the magnetic field reverses polarity and collapses very suddenly, resulting in a sharp electrical spike. This spike lasts a few microseconds (millionths of a second) and causes another current to run through the coil. This subsequent current is called the reflected pulse and lasts only about 30 microseconds. Another pulse is then sent and the process repeats. A typical PI-based metal detector sends about 100 pulses per second, but the number can vary greatly based on the manufacturer and model, ranging from about 25 pulses per second to over 1,000.

If a metal object passes through the metal detector, the pulse creates an opposite magnetic field in the object. When the pulse's magnetic field collapses, causing the reflected pulse, the magnetic field of the object makes it take longer for the reflected pulse to completely disappear. This process works something like echoes: if you yell in a room with only a few hard surfaces, you probably hear only a very brief echo, or you may not hear one at all. But if you yell into a room with a lot of hard surfaces, the echo lasts longer. In a PI metal detector, the magnetic fields from target objects add their "echo" to the reflected pulse, making it last a fraction longer than it would without them.

A sampling circuit in the metal detector is set to monitor the length of the reflected pulse. By comparing it to the expected length, the circuit can determine if another magnetic field has caused the reflected pulse to take longer to decay. If the decay of the reflected pulse takes more than a few microseconds longer than normal, there is probably a metal object interfering with it.

The sampling circuit sends the tiny, weak signals that it monitors to a device call an integrator. The integrator reads the signals from the sampling circuit, amplifying and converting them to direct current (DC). The DC's voltage is connected to an audio circuit, where it is changed into a tone that the metal detector uses to indicate that a target object has been found. If an item is found, passengers are asked to remove any metal objects from their person and step through again. If the metal

detector continues to indicate the presence of metal, the attendant uses a handheld detector, based on the same PI technology, to isolate the cause.

Many of the newer metal detectors on the market are multi-zone. This means that they have multiple transmit and receive coils, each one at a different height. Basically, it is like having several metal detectors in a single unit.

While a person steps through the metal detector, his carry-on items are going through the X-ray system. A conveyor belt carries each item past an X-ray machine. X-rays are like light in that they are electromagnetic waves, but they are more energetic, so they can penetrate many materials. The machines used in airports are usually based on a dual-energy X-ray system. This system has a single X-ray source sending out X-rays typically in the range of 140 to 160 kilovolt peak (KVP). KVP refers to the amount of penetration an X-ray makes. The higher the KVP, the further the X-ray penetrates.

After the X-rays pass through the item, they are picked up by a detector. This detector then passes the X-rays on to a filter, which blocks out the lower-energy X-rays. The remaining high-energy X-rays hit a second detector. A computer circuit compares the pick-ups of the two detectors to better represent low-energy objects, such as most organic materials.

Since different materials absorb X-rays at different levels, the image on the monitor lets the machine operator see distinct items inside bags. Items are typically colored on the display monitor, based on the range of energy that passes through the object, to represent one of three main categories:

- Organic
- Inorganic
- Metal

While the colors used to signify “inorganic” and “metal” may vary between manufacturers, all X-ray systems use shades of orange to represent “organic.” This is because most explosives are organic. Machine operators are trained to look for suspicious items – and not just obviously suspicious items like guns or knives, but also anything that could

be a component of an improvised explosive device (IED). Since there is no such thing as a commercially available bomb, most terrorists and hijackers use IEDs to gain control. An IED can be made in an astounding variety of ways, from basic pipe bombs to sophisticated, electronically controlled component bombs.

A common misconception is that the X-ray machine used to check carry-on items damages film and electronic media. In actuality, all modern carry-on X-ray systems are considered film-safe. This means that the amount of X-ray radiation is not high enough to damage photographic film. Since electronic media can withstand much more radiation than film can, it is also safe from damage. However, the CT scanner and many of the high-energy X-ray systems used to examine checked baggage can damage film (electronic media is still safe), so it should be carried on the plane.

Electronic items, such as laptop computers, have so many different items packed into a relatively small area that it can be difficult to determine if a bomb is hidden within the device. That is why screeners sometimes ask passengers to turn on their laptops. But even this is not sufficient evidence, since a skilled criminal could hide a bomb within a working electronic device. For that reason, many airports also have a chemical sniffer. This is essentially an automated chemistry lab in a box. At random intervals, or if there is reason to suspect an electronic device someone is carrying, the security attendant quickly swipes a cloth over the device and places the cloth on the sniffer. The sniffer analyzes the cloth for any trace residue of the types of chemicals used to make bombs. If there is any residue, the sniffer warns the security attendant of a potential bomb.

In addition to passenger baggage, most planes carry enormous amounts of cargo. All of this cargo has to be checked before it is loaded.

Most airports use one of three systems to do this:

- Medium X-ray systems – These are fixed systems that can scan an entire pallet of cargo for suspicious items.
- Mobile X-ray systems – A large truck carries a complete X-ray scanning system. The truck drives very slowly beside a parked truck to scan the entire contents of that truck for suspicious items.

- Fixed-site systems – This is an entire building that is basically one huge X-ray scanner. A tractor-trailer is pulled into the building and the entire truck is scanned at one time.

One old-fashioned method of bomb detection still works as well or better than most high-tech systems – the use of trained dogs. These special dogs, called K-9 units, have been trained to sniff out the specific odors emitted by chemicals that are used to make bombs, as well the odors of other items such as drugs. Incredibly fast and accurate, a K-9 barks at a suspicious bag or package, alerting the human companion that this item needs to be investigated. One of the problems we have discovered with using dogs is that they find this work as boring as humans do and are generally only good for one hour a day.

In addition to an X-ray system, many airports also use larger scanners. The first security inspection checked bags pass through depends on the airport. In the United States, most major airports have a computer tomography (CT) scanner. A CT scanner is a hollow tube that surrounds the bag. An X-ray mechanism revolves slowly around it, bombarding it with X-rays and recording the resulting data. The CT scanner uses all of this data to create a very detailed tomogram (slice) of the bag. The scanner is able to calculate the mass and density of individual objects in the bag based on this tomogram. If an object's mass/density falls within the range of a dangerous material, the CT scanner warns the operator of a potential hazardous object.

CT scanners are slow compared to other types of baggage-scanning systems, so they are not used to check every bag. Instead, only bags that the computer flags as "suspicious" are checked. These flags are triggered by any anomaly that shows up in the reservation or check-in process. For example, if a person buys a one-way ticket and pays cash, this is considered atypical and could cause the computer to flag that person. When this happens, that person's checked bags are immediately sent through the CT scanner, which is usually located somewhere near the ticketing counter.

In most other countries, particularly in Europe, all baggage is run through a scanning system. These systems are basically larger versions of the X-ray system used for carry-on items. The main differences are that they are high-speed, automated machines integrated into the normal baggage-handling system and the KVP range of the X-rays is higher.

While most of the things that cannot be taken on board an airplane are fairly obvious (guns, knives, explosives), there are others that most people would not think of – who would have thought a smoke detector could be considered hazardous? A person could be fined up to $27,500 for transporting a hazardous material on a passenger plane without declaring it. In a plane, a can of shaving cream is more dangerous than a bomb without a detonator attached. If a plane has structural problems and goes into decompression, any aerosol can inside it would explode.

As another safety precaution, aviation workers, from flight attendants to security personnel, are trained to react to certain words, such as "bomb," "hijack" or "gun." A person could be immediately removed from the plane and quite possibly arrested for saying these words, even in jest.

FAA AIR TRAVELER ADVISORY OF OCTOBER 8, 2001

On October 8, 2001, the FAA issued the following tips to help air travelers meet and assist the heightened security measures implemented since the September 11 attacks:

Carry-On Baggage

- Air travelers are limited to one carry-on bag and one personal item (such as a purse or briefcase) on all flights.

Allow Extra Time

- Heightened security measures require more time to properly screen travelers. Travelers should contact their airline to find out how early they should arrive at the airport.
- Take public transportation to the airport if possible. Parking and curbside access is likely to be controlled and limited.
- Curbside check-in is available on an airline-by-airline basis. Travelers should contact their airline to see if it is in place at their airport.

Check-in

- A government-issued ID (federal, state, or local) is required. Travelers may be asked to show this ID at subsequent points, such as at the gate, along with their boarding passes.
- Automated check-in kiosks are available for airlines that have appropriate security measures in place. Travelers interested in this option should check with their airline.
- E-ticket travelers should check with their airline to make sure they have proper documentation. Written confirmation, such as a letter from the airline acknowledging the reservation, may be required.

Screener Checkpoints

- Only ticketed passengers are allowed beyond the screener checkpoints, except for those with specific medical or parental needs.
- All electronic items, such as laptops and cell phones, may be subjected to additional screening. Passengers should be prepared to remove laptops from their travel cases so that both can be X-rayed separately.
- Passengers should limit the amount of jewelry or other metal objects they wear.
- Travelers should remove all metal objects prior to passing through the metal detectors in order to facilitate the screening process.

AIRPORT SECURITY IN OTHER COUNTRIES: BEST PRACTICES

This section will compare some of the security procedures in Europe and Israel. The public literature for this section is taken from General Accounting Office reports (GAO), and most of the information comes from *Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance RCED-00-75 June 28, 2000*. Little else is available on this subject, but the following information can be used to compare other countries to the United States:

1. The two most important reasons for screeners' poor performance are the rapid turnover among them and human factor problems. Turnover exceeds 100 percent per year at most airports, leaving few screeners with much experience at the largest hubs.

2. The main reasons for the high turnover rate are low wages and the human factor issues – those of repetitive, boring, stressful work requiring constant vigilance.

3. Belgium, Canada, France, the Netherlands, and the United Kingdom conduct their screening differently, performing regular "pat downs" of passengers.

4. These countries also pay their screeners more and provide benefits.

5. All of these countries have better screener performance (they are twice as good as Americans in detecting hazardous material), but still have a large number of dangerous materials going through their checkpoints.

6. In addition, the five European countries only allow ticketed passengers beyond checkpoints. This practice was started in the United States only after 9-11.

7. The European countries also require five times more training than their American counterparts, which is still by many measures insignificant, as it only requires a couple of weeks to begin work.

8. The Israeli system is one of passenger screening rather than baggage screening.

There is also the problem of governance. Under the new legislation, the United States is moving away from airport-controlled security towards government-controlled security. Yet we know few details about how the United States will run its new operations, as little information is available at this time, and outside contractors will be required for many years to make the transition. By comparison, these countries use the following governance:

Throughout all of the **United Kingdom**, the primary responsibility for airport security measures falls to the airport authority – the entity that operates the airport. The airport authority – not the airlines – hires private security contractors to staff security checkpoints. In addition, there is a significant police presence in the screening areas to support the private security workforce.

Three government ministries control security at all airports in **Amsterdam**. Working together, these ministries hire private contractors to provide airport security services. The contractors work in unison with a local police force to handle all airport security checkpoints.

As in the UK, the airport authorities in **Ireland** have the responsibility of providing security at all the country's airports. The security workers are direct employees of the airport authority. This security force works together with the airport police force and private security contractors at all security checkpoints.

The Ministry of the Interior in **Germany** has the charge of providing airport security nationwide. The Interior Ministry hires private contractors to provide security services at the major German airports. The private security contractors are supervised at the checkpoints by a local police force.

Some of the highest levels of airport security are provided in **Israel**. Like in Europe, the airport authority is responsible for security measures. The Israel Airports Authority also has help from the country's internal security service. In addition, these two entities have extra security support from private security contractors hired by El Al Airlines.

DISCUSSION

There is little, if anything, about the way the United States domestic airline industry has conducted airport security that is worthy of emulation. At the same time, most of the changes that are being implemented under the new legislation would not have deterred the hijackers on September 11, 2001. There are a number of problems that the new legislation does not address:

1. The changing face of terrorism
2. The human factor problems
3. Who is going to pay for all of this?
4. The role of the federal government in gathering intelligence

The terrorists who acted on September 11 were different from those the United States had ever seen before. They were well paid and had strategies that worked. They spent years in training, and the U.S. government had no indications of their plan. Their ability to formulate these plans and keep them secret for so long shows a governance capacity among terrorists that is quite impressive. Also, there was not a rush to admit guilt as there has been in the past. During the early 1990s, terrorists around the world readily admitted to their actions after the attacks had taken place. This has signaled a changeover in terrorists' strategies, the difference being that religiously motivated terrorists gain approval from divinity, which always knows what is going on, so they do not need CNN to announce their triumphs to the world. This makes terrorists deadlier enemies for the future.

The failure to detect terrorist plans stems from direct policies implemented by the Congress to cut security and intelligence gathering, most likely because the country became complacent to threats during the late 1990s. The economy was booming, lower taxes became the mantra, and national security became a very low priority. However, the real reason that the events of 9-11 did not happen earlier is simply that we have been lucky. The luck of the draw does not imply security on our part.

Another problem in the new security world is that of human factors. It is important to recognize in any airport security discussion that gazing into a computer screen at three-dimensional objects presented in two dimensions is problematic. The first problem is the absolute boredom of the task, and the second problem is one of interpretation.

The first part of the problem is best handled by using screeners who are mentally challenged, as they are better able to attend to repetitive tasks. At the same time, this makes it easier for the majority of travelers with no regard for the system, terrorists, and others to circumvent the system. Yet more intelligent screeners, most likely, do not perform the job as well due to the monotony. We need to find ways to motivate screeners and rotate them through a variety of tasks in order to keep them fresh. The human factor problems show how wise the Israelis are. Their system is based on screening people, rather than baggage. This does not mean they do not screen baggage; they do, but they spend most of their resources doing interviews. While it is unlikely that the United States will or can adopt the Israeli system, it can implement a derivative. Interviews seem to deter terrorists the most – the fear of being caught, by a human, in a situation wherein they have no resources for escape.

At the same time, the more intelligent screener is better capable of doing pat downs and conducting intelligence gathering (interviewing passengers) to access threats. The predicament is an interesting one, as the qualifications for the best security personnel (intelligence, conversation, etc.) are the opposite of those required by a system grounded in checking baggage.

The third problem – that of paying for all the needed changes to secure airports – is daunting. Discussing the changes made at Heathrow airport in London some years ago can put this into perspective. Heathrow's changes cost over $300 million. Adding to this the new security equipment needed at 420 airports results in a staggering amount of money. Senators, who agreed 100-0 on the new measures, will fall apart during the next year figuring out how to pay for their laws.

The last issue – that of integrating the new airport security people with federal intelligence gathering – is also daunting, as the history of agency conflicts and turf is one of stove piping, and little cooperation could be one of the biggest problems to overcome.

Meanwhile, things have changed since 9-11 that may be more important than anything the federal government has done or can do. These are:

1. The aggressive attitudes of commercial airline pilots

2. The aggressive attitudes of passengers and flight attendants

Pilots' attitudes are important, as in the past they were taught to be passive during hijackings. The reasoning was that if they cooperated with the hijacker, there was greater likelihood they and their passengers would escape without any harm. The events of 9-11 changed this. Pilots, when alerted to hijackings, can put a plane in extremely unnatural attitudes that make it impossible for anybody to move the plane around. We have also seen a marked change in flight attendants' and passengers' attitudes. This was seen in the case of the American Airlines flight from Paris, when the flight attendant acted heroically and the passengers came to her aid.

We will never know for sure what happened to the United Airlines plane that crashed in Pennsylvania, but the passengers' actions – whatever they were – changed passengers' actions in hijacking situations forever.