AVIATION AND AIRPORT SECURITY

Terrorism and Safety Concerns

Second Edition

Kathleen M. Sweet

CRC Press
Taylor & Francis Group

AVIATION AND AIRPORT SECURITY

Terrorism and Safety Concerns

Second Edition

AVIATION AND AIRPORT SECURITY

Terrorism and Safety Concerns

Second Edition

Kathleen M. Sweet


CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20131121

International Standard Book Number-13: 978-1-4398-9473-6 (eBook - PDF)

This book is dedicated to my ever supportive husband, Tim,
and all my friends in the
Department of Criminal Justice
at St. Cloud University.

Contents

Chapter 6

Chapter 7

Foreword

As I first sat down to write the introductory words to the first edition of this book in the peace of the English countryside in spring, the war against Saddam Hussein was probably hours away from its opening. Many of my friends and former colleagues in the British and American armed forces were eventually involved. I would have to sit this one out and experience it only vicariously. The overall operational commander of the British forces was a former student of mine—the first one I ever launched on his first solo flight, 35 years before Gulf War II, when I was an instructor pilot.

I have had this strange feeling of closeness yet remoteness during many previous conflicts: I was just completing training as a conscript back in 1956 when the Suez conflict ran its short course; I was on exchange duty at the United States Air Force (USAF) Air War College when my British colleagues fought to regain the Falkland Islands in 1982. But at least I knew what the airmen, sailors, and ground troops were engaged upon, and what their equipment could deliver. For the vast majority of the population of Britain and the United States, that kind of knowledge has for a long time been out of reach. The all-volunteer force and reducing numbers of men and women in uniform combined to make the business of war a very specialized subject. Until 11 September 2001.

From that day on, the terrorist threat has brought bloodshed into the workplace and transferred violence and death off the in-flight entertainment screen right into your face—permanently and finally. We are all at risk. There is no sure hiding place.

Kathleen Sweet provides the template for dealing with this acute challenge to our normal freedoms. She is ideally qualified to do so. She is certainly motivated to do so. I first met her when yet another conflict was claiming lives as I stood on the sidelines. We were both in Moscow in the mid-1990s, working as attachés in our respective embassies. Kathy was a mold-breaker: the Russians were not entirely at ease with the idea of a female attaché, let alone one who seemed to know her way round aircraft. So they gave her more freedom than any of us poor mere men could ever hope for, and as a result she was let loose inside a Sukhoi 4th generation jet fighter while the rest of us wondered if we could even get a photo of it! She demonstrated resilience and resourcefulness throughout a long tour of duty in Moscow, deploying all her manifold skills and talents: as intelligence gatherer and analyst, as linguist, as jurist, but above all as a lady of considerable energy and determination.

Thus, it came as no surprise to me to find her writing the definitive handbook on the terrorist threat to commercial airline and airport security. It was a unique privilege to be asked to provide a short foreword to that volume. Her previously published review of the topic was thorough and—of its day—timely. But not even she is immune to fate. As the first book went to print, the events of 11 September 2001 struck their grievous blows against the international community. The original volume took the reader, amateur or concerned professional, through the history of air terrorism and the ways in which countermeasures are developing. It revealed the dynamism with which international and national agencies are responding to the challenges of terrorism. It became required reading for any air service operator and invaluable to the traveling member of the public as well as the responsible legislator; in short, a key contribution to the current campaign against the terrorist. It is only too obvious that normal commercial operation of transport across land, sea, and air routes now faces increasingly sophisticated terrorist threats. It is equally obvious that the transport industry's response to these threats has added—and will continue to add—cost and complexity to the movement of goods and people. And the other sobering bottom line is that death and destruction await if the response is inadequate.

This present volume reflects the depth and intensity of the author's research and of her active involvement in the business of security. Over the last six or so years, she has traveled the world and surveyed the whole gamut of challenges to transportation security. She has trained security

personnel in the discharge of their management and operational responsibilities. She has provided customized advice to international government agencies and major commercial enterprises. She has addressed top-flight conference and symposium audiences. And, I must note, has moved house a few times and acquired larger dogs than most people would take on.

That is the key to Kathleen. As mentioned, I first met her in Moscow some 13 years ago when we both worked as Armed Forces attachés in our respective embassies. She managed to pack more into her daily routine than most of our colleagues would consider sensible. When she stepped outside the routine work areas she often struck gold. This latest book of hers will confirm these talents—it is a thorough review of the main subject, leaving no avenue unexplored. And it has those gems of insight that will confirm it as a "must have" volume on security and transport professionals' shelves.

I am therefore again both privileged and delighted to have the chance to contribute a few opening words to this new product from Kathleen. She has the knack of being ahead of the field, and I have no doubt this latest set of insights and recommendations for action will be as influential as those that have gone before.

Phil Wilkinson

Air Commodore, Royal Air Force (retired)

Hampshire, England

About the Author

Kathleen M. Sweet, Lt. Col., Ret., USAF, JD, is currently on the adjunct faculty at the University of Maryland, University Campus, where she teaches courses in strategic intelligence, security, and terrorism.

Dr. Sweet was retired from the US Air Force in 1999. While in the military, she was an instructor at the Air War College at Maxwell AFB, Alabama, and an assistant air attaché to the Russian Federation, an intelligence officer, and a member of the Judge Advocate General's Department.

Additionally, she was assigned as a military/political affairs officer to the 353rd Special Operations Wing located at Clark AFB, Republic of the Philippines. She is presently a consultant with International Risk Control Ltd, London, England and president and CEO of Risk Management Security Group and RMSG Ireland Ltd., a transportation security consulting firm doing business in the United States and Europe.

Introduction

NEWS

11 September 2001: Four aircraft are hijacked in the United States. Two fly into and destroy the World Trade Center in New York City, one slams into the Pentagon, and a third crashes in Pennsylvania, apparently disrupting the terrorists' hopes of also smashing into the White House.

11 March 2004: An Al'Qaeda-sponsored attack in Madrid, Spain, consisted of a series of ten explosions that occurred at the height of rush hour aboard four commuter trains (Cercanías in Spain). Thirteen improvised explosive devices were reported to have been used, all but three of which detonated. The attacks were the deadliest assault by a terrorist organization against civilians in Europe since the Lockerbie bombing in 1988 and the worst terrorist assault in modern Spanish history.

1 September 2004: Armed Muslim terrorists took hundreds of school children and adults hostage at School Number One in the Russian town of Beslan in North Ossetia. On the third day of the standoff, shooting broke out between the hostage-takers and Russian security forces. During the crisis, 344 civilians were killed, at least 172 of them children, and hundreds more were wounded. The attack was the responsibility of Chechen terrorist Shamil Basayev and his principal Ingushetia-based deputy Magomet Yevloyev.

7 July 2005: A series of four bomb attacks struck London's public transport system during the morning rush hour. At 8:50 a.m., three bombs exploded within 50 seconds of each other on three London Underground trains. A fourth bomb exploded on a bus at 9:47 a.m. in Tavistock Square. Fifty-six people were killed in the al'Qaeda-sponsored attacks, including the four suspected bombers, with 700 injured. The incident was the deadliest bombing in London since the World War II.

21 July 2005: Four attempted bomb attacks disrupted part of London's public transport system two weeks after the previous bombings. The explosions occurred at Shepherd's Bush, Warren Street, and Oval stations on the London Underground, and on a bus in Bethnal Green. A fifth bomber dumped his device without attempting to set it off. Metropolitan Police later said the intention was to cause large-scale loss of life, but only the detonators exploded.

INTRODUCTION TO AVIATION AND TERRORISM

As I sit in my solarium with the rain pounding on the glass, I have come to realize that the "War on Terrorism" cannot be won, at least not in conventional warfare terms. It would be a wonderful concept to think that the rain could wash the problem away, but it will take decades to stop, let alone reverse, the trends that have developed the vast scourge that has come to encompass the term. The concept has spread to include every disenfranchised group of people on the planet. They have made the decision to make the unqualified jump from rhetoric to violence and to publicize their personal viewpoint on topics from nationalism to religious fanaticism. Historically, the term was coined to describe the terror inflicted on the aristocracy and the public during the French Revolution. It has broadened quite a bit since that time. Scholars have attempted to both define it and classify it. But in reality, its unconventional warfare nature stems from a lack of ability to fight a "war" between

combatants. It chooses to strike fear into noncombatants. Terrorists do this to sensationalize a personal perspective and threaten the democratic ideals of powerful and sometimes wealthier nations bound by antiquated systems of criminal justice. Unable to control the proliferation of the threat, the battle rages on in terms of both ideology and carnage.

Many people, both in and out of government, have experienced firsthand the complicated effort it takes to defeat a terrorist campaign. Battleworn from the exploits of the Irish Republican Army (IRA), the British are fully aware of the differences between, and the benefits and drawbacks, of a strictly law-enforcement approach versus a military response. The tactics are distinct, and both can be appropriate or totally inappropriate depending on the unique circumstances of a specific risk. The lessons of what did not work in Northern Ireland can be more useful than what did. The British authorities are currently utilizing the lessons learned from the Northern Ireland "time of troubles" to the Muslim fundamentalist movement, but with some significant differences. The IRA, whatever your political viewpoint, was a nationalist movement. The Al'Qaeda syndrome seeks to bring down democratic traditions and create a theocratic form of government based on a radical interpretation of the Islamic tradition.

Terrorism, in its immediate aftermath, often typically prompts democratic societies to set aside critical civil liberties in the name of more security. Britain, after the deadly July 7, 2005 subway and bus bombings, in conjunction with the additional but botched attempts soon thereafter in London, has been no exception. It is a very thin line between throwing out the bathwater and throwing out the baby with the bathwater. The United States, by incarcerating loyal Japanese-Americans in the immediate aftermath of Pearl Harbor, knows this scenario all too well. Problems can proliferate when security efforts consign whole communities or portions of ethnic communities to the status of second-class citizens. The whole community is broadly brushed with a negative connotation that results in community leaders failing to cooperate with the overall antiterrorist plan, when they themselves fall within the "criminal" or "terrorist" profile.

For example, since July 2005, former Prime Minister Tony Blair has planned to criminalize not just direct incitement to terrorism in Britain, but anything the government may categorize as "condoning," "glorifying," or "justifying" terrorism anywhere in the world. Words like that are very vague and open to abuse. Of similar concern is the British government's plan to expand its list of deportable offenses to include the expression of "what the government considers to be extreme views." Last, the idea of making naturalized, but not native-born, British citizens deportable for "extremism" might create some unwanted results. It is clearly understandable that the British citizenry are offended by the fact that the bombers were "homegrown." In fact, the latter thrived due in large part to the democratic ideals inherent in British society.

Another factor to consider is the heartfelt faith of many innocent Muslims. Arab and Muslim devotees are deeply entrenched in religion, a religion which at its basic roots is at odds with many of the concepts of secularism. It is precisely this agenda of attempting to disengage Arabs and Muslims from their basic religious doctrines that so offends the moderate and feeds the sentiment of anti-Western hostility. It should be remembered that U.S. State Department analysts warned the Clinton administration as early as July 1996 that Usama bin Laden's move to Afghanistan would give him an even more dangerous haven as he sought to expand radical Islam "well beyond the Middle East." Bin Laden has indeed spread his radical interpretations and hatred worldwide. In what would prove a frightening warning, the analysts said in a top-secret assessment in 1996 that bin Laden's "prolonged stay in Afghanistan could prove more dangerous to U.S. interests in the long run than his three-year liaison with Khartoum" in Sudan.

The intelligence community prior to 1996 considered bin Laden more as a financier of terrorism: the bank so to speak. This was at a time before he publicly urged Muslims to attack the United States, even though officials suspected he was taking a more active role; including his part in the bombings in June 1996 that killed 19 U.S. soldiers at the Khobar Towers in Dhahran, Saudi Arabia. Soon thereafter he participated in the planning and execution of two major operations which struck two U.S. embassies in East Africa, leading to failed military efforts by the Clinton administration to

capture or kill him in Afghanistan. Three years later, on Sept. 11, 2001, Al'Qaeda struck the World Trade Center and the Pentagon in an operation supervised from the base in Afghanistan.

To be successful, all agencies involved in the counterterrorism effort need to understand the history of terrorism and the nuances of the current threat as it exists today. This book represents such an effort, drafted from a law enforcement and military professional perspective. The book is geared toward providing the necessary facts for anyone to understand the world of terrorism and its dark past and ongoing future. The key to combating terrorism rests on many levels. One of them is awareness. This book contains the necessary information with which to devise a strategy that college students, military personnel, and police counterterrorist unit alike can use to educate themselves. Without education, the war is already lost.

1 The Aviation Industry
A National Security Asset

NEWS

2000: By the year 2010, aviation's impact on the world economy could exceed 1800 billion U.S. dollars with more than 31 million jobs provided and passenger traffic topping 2.3 billion per year.

2003: Air Transportation's percentage of gross domestic product continues to grow post 11 September 2001: 1998 (106.9), 1999 (111.7), 2000 (121.9), 2001 (106.0), 2002 (101.1), and 2003 (116.9) per the Bureau of Economic Analysis, U.S. Department of Commerce.

August 2005: United Parcel Service (UPS) orders eight Boeing 747-400 freighter planes to boost cargo capacity on its top international routes. UPS does not disclose the terms of the deal, but it would be worth 1.68 billion U.S. dollars at list prices. UPS says it chose General Electric to supply the engines for the planes, which can handle more cargo than UPS's current mainstay, the Boeing MD-11.

2005: The U.S. Justice Department has urged against giving antitrust immunity to five members of the SkyTeam airline alliance. They indicate there is "a significant risk" of reduced competition if the airlines are allowed wide latitude to share information and coordinate their operations. Members include Continental, Northwest, and KLM, which merged with Air France, Korean Air, Alitalia, Delta, CSA Czech Airlines, and AeroMexico.

2004–2007: In 2000, Congress passed and President Clinton signed the Wendell H. Ford Aviation Investment and Reform Act for the 21st Century (FAIR-21). This multiyear FAA reauthorization bill includes authorizations of 9.9 billion U.S. dollars for the Airport Improvement Program (AIP) for fiscal years 2001 to 2003. The bill also increases the Passenger Facility Charge to $4.50 per boarding passenger. Congress, in 2003, reauthorizes the AIP for 2004 to 2007 at 14.2 billion U.S. dollars for four years.

IMPORTANCE OF AIR TRANSPORTATION

The entire age of air transportation is not yet older than the life span of an ordinary human being. On 17 December 1903, the Wright Brothers launched an airplane with controllable powered engines at Kitty Hawk, North Carolina, and changed the world forever, even though evidence has now revealed that several New Zealanders had actually flown first. The historic "controllable-powered" flight covered only 120 feet, which is a shorter distance than an average flight attendant traverses in walking from the front end of a large commercial airliner to the other end. The invention of the airplane enabled man for the first time in history to rapidly and easily travel over land-dominated obstacles like mountains, deserts, and ice caps. It has since also provided speed not even imagined a generation ago. The greatest tribute to air transportation, however, may be the simple fact that it is taken so much for granted. Any passenger can walk into any scheduled airline service and purchase a ticket to virtually anywhere on the planet because of the airlines' intercarrier cooperative programs. The

same service is available for freight shipments. The world depends on it. Unfortunately, there are signs that its infrastructure and security have been somewhat neglected and taken for granted.

Clearly, the hopes and dreams of future generations are dependent on air travel and eventually the vastness and potential of space transportation. British and Japanese engineers are already reengineering the space shuttle for private commercial passenger flights to space and hope to offer commercial service within the decade. Consequently, the air transport industry constitutes one of the most vital and fastest paced economic forces in the global economy. In addition, commercial aviation will only increase in importance in the future and will continue to do so throughout the 21st Century. As technology improves, concurrently so does air transportation and the ability to travel and reposition cargo over longer distances in shorter periods of time.

Air transportation also symbolizes a sterling example of applied technology. As technology improves, so must air transportation and the facilities and equipment that support it. The ability to provide safe air travel and freight carriage to the industry's patrons represents a continuous challenge. These advances in technology must also enable authorities to secure the airport environment from those that would potentially disrupt it. At the same time, care needs to be taken that security measures do not delay air cargo to the point where it is noncompetitive with goods shipped via other means of transportation. The global economy depends on continued and uninterrupted service. Terrorists and other criminal activities threaten that safe environment.

AIRWAYS

Remarkably, air transport as a means of moving passengers and freight has gained an important place in the U.S. civilian economy in only the past quarter century. Ferdinand Graf von Zeppelin created the world's first commercial airline in 1912 in Europe using dirigibles to transport more than 34,000 passengers before the start of World War I. After the war, European governments heavily subsidized such now well-known airlines as British Airways, Air France, and the Royal Dutch Airlines, KLM.

In the United States, the development of commercial airlines progressed more slowly. It was as recently as 1958 that U.S. airlines finally carried more passengers, as measured by passenger miles, than the railroads. Admittedly, in comparison with rail and truck transport, the airlines still carry an insignificant proportion of the total volume of freight around the world. However, air cargo service still remains vitally important because of its capabilities for rapid delivery over lengthy distances without the requirement of frequent transfer. The volume of air freight traffic has, in fact, been growing rapidly. This is particularly true in light of the development of standardized containers, which greatly facilitate loading and unloading. As regards passenger carriage, no piece of equipment ever invented, other than the airplane, has impacted transportation on such a global scale so rapidly.

The interconnectivity of the airline industry has framed the perception that the planet seems smaller. It can be argued that the intermixture of cultures and peoples has changed the diversity of the world. Travelers can literally see the Pyramids at Giza, the Taj Mahal, the Golden Gate Bridge, and Westminster Abbey all within a few days if they are up to the trip. Air transportation, enhanced by advances in communications, has expanded the world's economy exponentially.

DEVELOPMENT OF THE AVIATION INDUSTRY

Flight as a practical means of transportation was highlighted with Charles A. Lindbergh's transatlantic flight in 1927. Improvements continued to be made in the design of commercial aircraft, but it was not until World War I that aviation came into its own as an industry. Out of necessity during the war, the United States had built almost 17,000 aircraft, and over 10,000 people had been trained to fly. After the war, surplus aircraft were converted to civilian commercial use. The idea of commercial flight started to proliferate, and regular mail service began in 1918 between Washington,

D.C., Philadelphia, and New York. The U.S. Post Office subsequently and greatly contributed to the creation of a nationwide system of airports, making transcontinental service soon available.

In 1925, the Air Mail Act authorized the U.S. Post Office to award airmail routes to private contractors. The practice continues today and raises unique problems pertaining to the needs of airport security personnel in inspecting sealed bags of mail. The U.S. commercial air industry really began to expand when the U.S. Army transferred some of the rail routes to commercial carriers. After that, the Air Commerce Act of 1926 gave further encouragement to the development of the airline industry. The law provided for the certification of aircraft and airmen, the drafting and implementation of air traffic rules, and the creation of civil airways. The government had stopped operation of airmail routes in 1927, transferring the business to the exploding aviation industry. Except for a short period in 1934, civilian air carriers have consistently been reimbursed for carriage of the mail, often making them quite a profit. Interestingly enough, to reduce the cost of this carriage, the government required the air carriers to provide space for passengers. Hence, significant development of the airline passenger industry was begun. The expansion of air travel on regularly scheduled airlines grew speedily and has obviously resulted in tremendous convenience for the world traveler.

The Civil Aeronautics Act of 1938 further promoted the development of today's airline industry. The Act provided for the establishment of a Civilian Aeronautic Board (CAB) to establish routes, fares, and safety standards. Congress specifically intended to express a policy of encouraging the development of air transportation and to foster regulations to promote aviation. They sought to provide the public with air transportation at reasonable rates as safely as possible. World War II also gave a tremendous boost to aviation as military improvements in aircraft eventually leaked into commercial aviation. Some of these improvements and advancements had immediate civilian applications. Eventually, trunk lines were expanded, local lines multiplied, and scheduled air carriers instituted freight service. Soon thereafter, airlines carrying only cargo also appeared.

Aviation-related advancements are always in development. Increases in speed, range, capacities of aircraft, and navigation are constantly improving. Giant strides are additionally made in the area of air traffic control. The control tower is one of the nerve centers of any airport. Air traffic controllers, who are constantly under pressure attempting to juggle aircraft, can arguably be over-tasked during peak hours. The controllers use radar, radio, signal lights, and innovations in communications and navigation to direct air traffic near the airport as well as on the ground. All these systems are susceptible to interference, and the consequences would be potentially catastrophic. Enhancements were needed when the commercial jet era began in 1958 and have broadened to the evolution of the supersonic transport (SST), which reached speeds of 1400 miles per hour. Even faster aircraft are currently under development by the National Aeronautic and Space Administration. Communication, navigation, and infrastructure capabilities must all match these advancements.

The industry got an additional boost during the late 1970s. The U.S. government hoped to further enhance the rapid growth of aviation with the decision to deregulate the airlines in 1978. The Airline Deregulation Act of 1978 permitted air carriers to set individual routes. In 1982, they were allowed to set exclusive fares as well. Eventually, the CAB was abolished and the Federal Aviation Administration (FAA) was tasked with regulating safety. Financial difficulties in the 1980s generated the consolidation of many of the larger air carriers, and smaller carriers subsequently created regional niche markets. The industry continued to grow, and in 1998, the ten largest carriers transported 551 million passengers controlling 96 percent of the market (Columbia Encyclopedia, 2001). By 2005, U.S. airlines carried 4.1 percent more domestic passengers on almost the same number of domestic flights as they operated in 2004. The Bureau of Transportation Statistics (BTS), a part of the Research and Innovative Technology Administration (RITA) of the U.S. Department of Transportation (DOT), more recently reported that the airlines carried 678 million domestic passengers during 2007, up from the 657 million carried in 2006 (Bureau of Transportation Statistics, Internet: http://www.transtats.bts.gov/homepage.asp). In addition, U.S. scheduled passenger airlines employed 3.7 percent more workers in November 2007 than in November 2006, the tenth consecutive increase in full-time equivalent employee (FTE) levels for the scheduled passenger carriers

from the same month of the previous year (Bureau of Transportation Statistics, Internet: http://www.bts.gov/ press_releases/2008/bts004_08/html/bts004_08.html).

However, deregulation also generated increased burdens on the FAA to provide safe yet efficient airports and aircraft standards without a corresponding increase in staff and budget. Two significant crashes, one over San Diego in 1978 and one at Chicago O'Hare in 1979, in conjunction with an increase in hijackings, intensified public demand for more strict and expanded safety measures. At the same time, the FAA became embroiled in controversy over how to handle the multi-task mandate of regulating a rapidly growing industry, facilitating that growth and the briskly proliferating terrorist threat. Initially, they were tasked with handling all three, becoming, according to some scholars, a captured agency.

Airlines

Americans have come to rely heavily on the expediency of air travel. Passenger traffic grew from 172 million passengers in 1970 to nearly 642 million in a little over 30 years. Unfortunately, the events of 11 September 2001 combined with an economic recession and increasing oil prices have resulted in not only slower growth, but also a reduction in travel to levels a decade ago. The major airlines routinely transport people and cargo over regularly scheduled routes or on routes, called "charters," specifically designed for a group of travelers or a particular cargo. Several genre of airlines function throughout the world. However in the United States, there are currently 15 major airlines, 12 passenger and 3 all-cargo, which the U.S. DOT defines as having operating revenues of more than 1 billion U.S. dollars. The Big Six, or legacy airlines, generally have a "hub" and also fly internationally. The hubs are established at a centrally located or designated airport to accommodate a majority of their own flights from numerous locations and provide a point at which passengers can transfer to flights that the airline also serves within its own and other networks. In this way, the greatest number of passengers, from as many locations as possible, can be served in the most efficient way with a given set of resources.

In the last decade, the legacy airlines now must also compete with low-cost, low-fare carriers. These carriers either provide a specific unique service, i.e., TV's located at each seat, or offer flights to a limited number of destinations very reasonably priced. They focus, in general, on regional and relatively short routes and on no-frills flights. Historically, they have been popular with vacationing passengers and passengers traveling with children. However, these airlines are now expanding both the customer base and traditional routes. The number of commuter and regional carriers has grown to include over 75 airlines. Some of the largest regional carriers are subsidiaries of the major airlines, but most are independently owned, often contracting services to the major airlines. A regional airlines' fleet consists primarily of smaller 19- to 68-seat turboprop and 40- to 70-seat jet aircraft. The regional airlines are the fastest growing segment of commercial aviation, with 1 of every 7 domestic airline passengers flying on a regional airline during at least part of a trip (U.S. Department of Labor, Internet: http://www.bls.gov/oco/cg/cgs016.htm).

Facilities

Cities, counties, states, or public corporations own and operate most of the larger airports in the United States; however many smaller airports are still privately maintained. The FAA acts as the primary responsible governing agency and regulates design and operational standards. The FAA also regulates safety and security in conjunction with the Transportation Security Administration (TSA). Civilian airports are classified as either air carrier airports or general aviation airports. Military facilities fall into another category. Each has its own respective security requirements. Arguably, no segment of aviation has been under more specific scrutiny than general aviation (GA). After grounding all GA in September 2001, the federal government incrementally restored flight operations after a careful security review. The White House Office of Homeland Security (predecessor of

Table 1.1 Median annual earnings of the largest occupations in air transportation, May 2004

Occupation	Air transportation	All industries
Airline pilots, copilots, and flight engineers	$137,160	$129,250
Aircraft mechanics and service technicians	54,890	45,290
First-line supervisors/managers of office and administrative support workers	47,450	41,030
Flight attendants	43,470	43,440
Baggage porters and bellhops	38,600	17,760
Transportation workers, all other	37,790	32,170
Cargo and freight agents	36,700	34,250
Reservation and transportation ticket agents and travel clerks	31,450	27,750
Customer service representatives	28,420	27,020
Laborers and freight, stock, and material movers, hand	21,570	20,120

U.S. Department of Labor, 2004.

the current cabinet-level Homeland Security Department), the TSA, the Department of Defense, the National Security Council, the Secret Service, the FBI, the DOT, the FAA, and other agencies have specifically examined general aviation flight operations in all parts of the nation and have sanctioned continued GA flights. In November 2003, the Aviation Security Advisory Committee (ASAC) accepted a report on General Aviation Airport Security. The report recommended several guidelines (Aviation Security Advisory Committee, Pamphlet A-100) for voluntary "best practices" designed to establish nonregulatory standards for general aviation airports. Commercial airports, except for those that have utilized the "opt out" screening program, remain under the control of the TSA for specific security requirements and utilizing TSA screeners.

Airway Routes

The routes of the airway system consist of designated air space through which the movement of aircraft is controlled. In the interest of safety, a highly technical system of navigational aids enables highly trained controllers to guide aircraft and to control movement of those aircraft. Adequate aircraft landing facilities, airports, and auxiliary services are critical. Two serious consequences of the rapid expansion of general aviation have been the heavy saturation of air space and overloading the capacity of many airports. According to some experts, this overcrowding has reached critical proportions. The situation has received much media attention, especially after tragic accidents, and the release of government reports criticizing the FAA and the financial profit-making motives of the airline industry.

The airport facilities' crisis has several facets. The increase in air traffic consisting of general aviation aircraft, large commercial airlines, commuter airlines, and freight traffic is progressively overburdening airports built decades ago. An air carrier airport may service commuter, regional, national, freight only, international passenger, and cargo airlines all at the same time. The 1978 deregulation of the industry generated an increase in the number of commercial airlines using major airports as well as an increase in the flight schedules of all airlines using such airports without corresponding upgrades in facilities. The cycle of industry growth without infrastructure growth has been perpetuating itself for more than 20 years. On top of this, less crowded reliever airports have not adequately absorbed increases in general aviation traffic. Furthermore, the absence of adequate ground navigational facilities at these airports forces many light and medium sized air-

craft to use the larger airports especially during bad weather, complicating the safe management of these airports.

Because air transport is one of the fastest growing sectors of the world economy, any blip in the carefully orchestrated daily movement of airborne aircraft has a ripple effect. When airports close or are restricted in anyway, the entire worldwide system feels the effects in some manner. By the year 2010, aviation's impact could exceed 1800 billion U.S. dollars, with over 31 million jobs provided to the world's workforce (Internet: http://www.atag.org/ECO, 4/22/01 pg. 3). Consequently, the financial effects can be significant when even a small disruption occurs. In addition, approximately one third of the world's manufactured exports (by value) are now transported by air. The effects of the aviation industry on the global economy are significant. It is an indisputable fact that the shut down of U.S. aviation after 11 September 2001 clearly negatively affected the global economy. Interruptions in service have major repercussions not only to the aviation industry, but also to almost all facets of the world's economic productivity, so much so that governing political figures have frequently intervened to prevent strikes, bankruptcies, and mergers. Governments also interject demands on security requirements when the terrorist or criminal threat receives media attention and requires a public response.

The demand and the need for adequate and well-protected airports will only continue to increase (see Figure 1.1). In the United States, a 1999 study indicated that strains on the airport infrastructure likely cost the airlines and the public more than 4.5 billion U.S. dollars that year (Air Transportation Association Study, 1999). The Air Transportation Association of America has attempted to place most of the blame on air traffic control delays, but such delays represent only part of the problem. Governments must soon recognize that future global economic growth is substantially threatened unless concrete investment in airport infrastructure comes about soon. Additionally, airports face a new challenge in the anticipated growth of corporate jets that seat four to six passengers; a shift of two percent of today's commercial passengers to corporate jets would result in triple the number of flights. At the other extreme, larger planes carrying 800 or more passengers also would represent a significant challenge for the current infrastructure of airports.

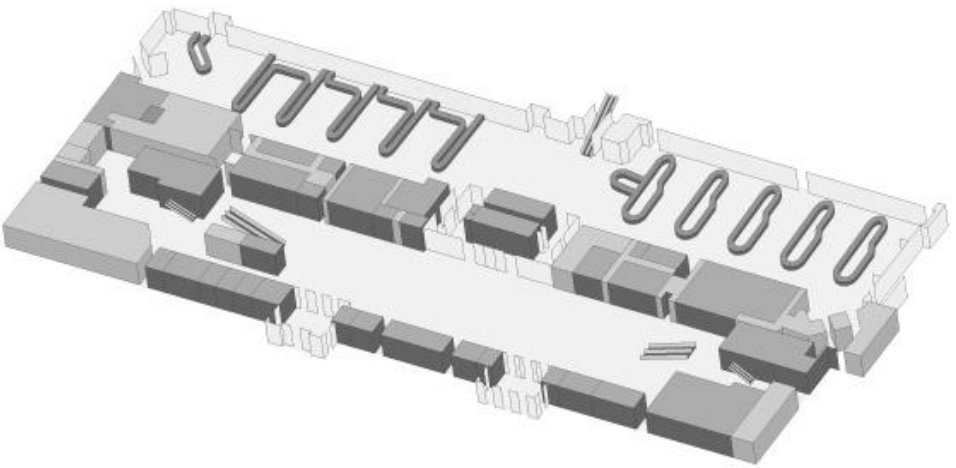

FIGURE 1.1 Layout of the arrivals level at Dublin International Airport, Dublin, Ireland. Proper airport design can be a crucial factor in thwarting terrorist activity especially in light of the historic terminal attacks on the Rome and Tel Aviv airports as well as the more recent attack at the El Al counter in Los Angeles. Not only is Dublin Airport Ireland's busiest airport, it is also one of the 10 busiest airports in Europe. Dublin Airport manages an average of 60,000 passengers per day, rising to 80,000 during the peak season, and more than 600 aircraft movements every day.

The nation's air traffic control system remains a looming issue of concern. In the mid-1980s, the FAA estimated that it would take 10 years and $12 billion to modernize the nation's air traffic control systems. Twenty years and $35 billion later, the task remains incomplete, and the FAA expects that it will take at least 3 additional years and an additional $16 billion. Meanwhile, the number of aircraft handled by air traffic control is expected to increase from 45.1 million in 2004 to 58.4 million by 2015 (Federal Aviation Administration, December, 2004). Problems also persist pertaining to the number of qualified and experienced controllers available to do the job. Since September 3, 2006, nearly 800 experienced controllers have retired. According to FAA figures, there are just 11,467 experienced controllers left in the country. That's an 11-year low, and more than 1100 fewer than were working on 11 September 2001, despite rising traffic volume that has left Americans completely frustrated and angered by a record number of flight delays (Internet: http://www.natca.net/mediacenter/press-release-detail.aspx?id=455).

In 1998, the world's airlines carried more than 1600 million passengers and over 29 million metric tons of freight. The world's fleet of aircraft consists of about 18,000 aircraft operating over 15 million kilometers and serving nearly 10,000 airports. "Passenger and freight traffic are expected to increase an average annual rate of around 4 to 5% between 1998 and 2010, significantly greater than the growth of the global gross domestic product" (Air Transportation Action Group, 2000). With air cargo statistics for the first half of 2007 posting 5 percent volume gains over 2006 totals, the slow but stable growth indicates the industry will maintain at an even rate of growth throughout 2008. Admittedly, 2007 figures evidenced a less than a banner year in comparison to the 6.2 percent annual average growth rate recorded by the International Air Transport Association between 2002 and 2006. A sluggish U.S. economy, coupled with strong price competition from other modes of transport and record high oil prices, likely slowed growth in the domestic market. These figures will only grow in the future and are indicative of the size and dimensions of the piece of the pie that the air transportation industry encompasses. Such an important segment of the economy needs constant attention by the FAA, the TSA, the airlines, freight forwarders, and security professionals.

DEREGULATION

As mentioned, few federal statutes pertaining to the economic regulation of the air transportation industry existed between 1926 and 1938. The Air Mail Act of 1934 launched the appointment of a Federal Aviation Commission tasked with making recommendations to Congress on national aviation issues. The Civil Aeronautics Act of 1938 implemented many of the commission's recommendations and laid out the outline of economic regulation that existed until 1978, when Congress literally deregulated the entire industry.

The Civil Aeronautics Act of 1938 contained many controls that mirrored the economic regulations placed on railroads and trucking industries. Many experts have argued for the return of these kinds of regulation. First, air carriers were required to obtain certificates of public convenience and were required to provide necessary and adequate facilities on routes for which they had authorization. Routes could not be abandoned without the prior approval of the government. Second, carriers were obligated to charge just and reasonable rates and provide safe and adequate service and facilities. Rates and fares had to be published for public inspection and had to be filed with the appropriate government regulatory agency. The rates were published, and changes required a 30-day notice period. In 1972, the CAB was even authorized to regulate rates to and from foreign countries. Today, a passenger can be sitting in a seat for which they paid $300, whereas the passenger seated directly next to them paid $800 or more. Another passenger may have purchased an Internet discount rate at $69 one way. The Civil Aeronautics Act also gave the corresponding regulatory agency the power to investigate alleged unfair and deceptive practices or unfair methods of competition and to issue "cease and desist" orders to air carriers (52 Statute. 973, Civil Aeronautics Act Annotated). The CAB also controlled consolidations and mergers of airline companies and acquisitions of control and leases of air carriers. Therefore, it previously played an important role in preventing monopolies.

Nonetheless, on 24 October 1978, the Airline Deregulation Act of 1978 was signed into law. The basic purpose of the airline deregulation legislation was to encourage an air transportation system that placed primary reliance on competitive market forces as the basic determinant of commercial airline operations. The timetable called for a seven-year phase out. The Act allowed wide discretion in the setting of passenger fares. The confusing fares of today are a direct result of this decision and have created a situation many passengers resent. It also dismantled the governing board, the CAB, and distributed its responsibilities among the DOT, the Department of Justice, and the U.S. Postal Service (Mini-Brief, Library of Congress, 1980). The laissez-faire argument of competitive market prices benefiting the consumer has arguably not occurred in the minds of the traveling public. In fact, some passengers would claim the airlines actually engage in price-fixing and predatory pricing practices to drive competitors out of business. Both are detrimental to the consumer.

Many airline mergers have indeed reduced costs and expanded market shares. However, whether the savings are actually passed onto the consumer presents a different debate. Price-fixing, forcing smaller airlines out of business, increasing the number of seats per aircraft, and reducing competition in a particular market is not uncommon, as evidenced by the dismantlement of some regional airlines by larger ones. Furthermore, generally monopolistic acts and predatory pricing are also not unusual features of gigantic corporations, including the airlines, as evidenced by price-fixing on passenger and cargo flights by British Airways and Korean Air Lines, for which they pled guilty and for which a fine of 300 million U.S. dollars was imposed. Last but not least, accusations of senior management receiving exorbitant salaries, golden parachutes, and other perks have plagued the industry legacy airlines.

CONSEQUENCES OF 11 SEPTEMBER TO THE INDUSTRY

After the tragedy of 11 September 2001, the stock value of the major airlines provided a clear indication of the consequences of a single terrorist act that involved two major airlines and four aircraft. Two hijacked airliners destroyed the twin towers of New York's World Trade Center, another slammed into the Pentagon in Washington, D.C. A fourth airliner, believed destined for the White House, crashed in Pennsylvania when several passengers overtook the hijackers in a last ditch and heroic effort to save American lives. All normal commercial and general aviation was suspended following the attacks.

Hence, the nation's commercial airlines and general aviation aircraft were grounded. For three full days the skies above America were virtually silent except for military aircraft. Slowly, the airports were reopened, and commercial flight was resumed. Note: The only permitted flights picked up and removed the relatives of Usama bin Laden from the territory of the United States for their own safety at the request and funding of the Saudi Arabian government. On 20 December 2001, the DOT lifted flying restrictions on Class B airspace. This essentially restored visual flight rules, (VFR) to pre- September 11 conditions in major metropolitan areas. However, it was not until April 2002 that Ronald Reagan Washington Airport had the remaining restrictions on the operation of commercial aviation removed (see Figure 1.2).

Between 31 December 2000 and 31 December 2001, the percentage negative change in stock value of the two carriers directly involved was substantial. American Airlines stock was down 43.1 percent, and United Airlines stock dropped 65.3 percent. The other airlines were significantly affected as well. Northwest stock plummeted 47.9 percent, Delta dropped 41.7 percent, and a third fell a whopping 84.4 percent (Plane Business, Internet: http://www.plane business. com/stock performance/2001.html, 28 May 2002). The airline industry began to scream for assistance. Airports suffered as well. Flight restrictions imposed around the nation's capital after 11 September 2001, crippled College Park Airport, Potomac Airfield, and nearby Washington Executive Hyde Field. It was not until 2005 that regulations were relaxed further. The three Maryland airports previously hosted hundreds of planes, and to stay in business, the Washington Executive Hyde Field in Clinton,

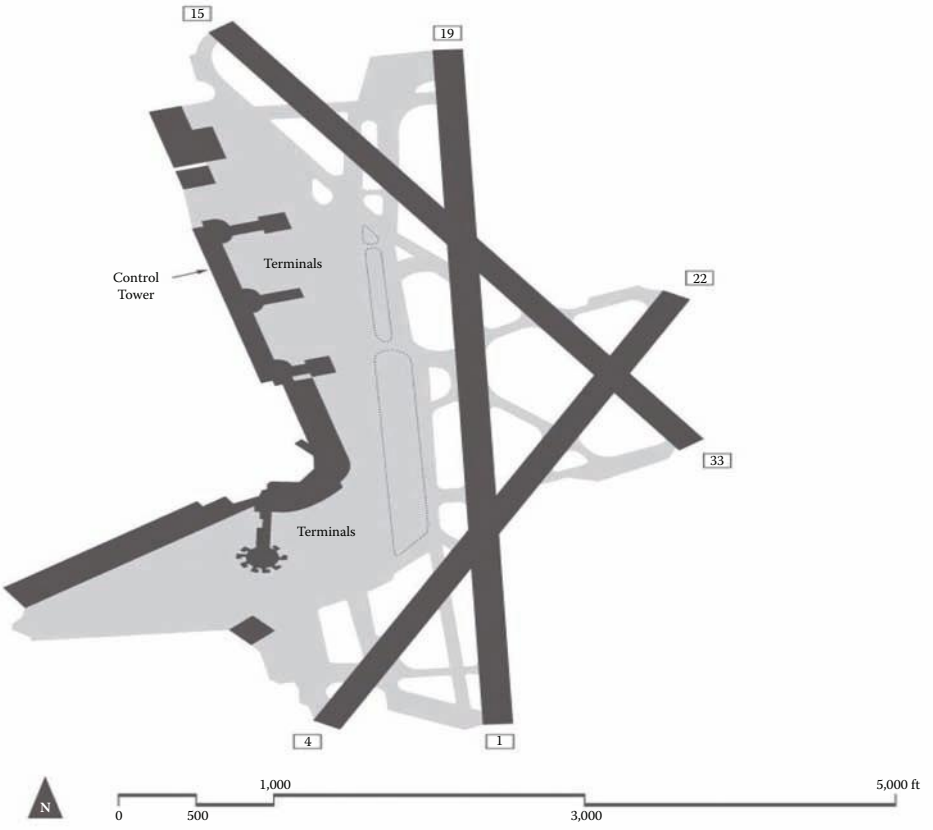

FIGURE 1.2 Restrictions were imposed at Washington's Ronald Reagan Airport post September II, 200I. Many special security restrictions remain in force at the airport because of its proximity to Washington's government buildings and monuments. (Source: Federal Aviation Administration. www.faa.gov)

MD. resorted to having part of its property mined for sand and gravel after business dropped to 20% from what it had been.

EMERGENCY FUNDING

In an effort to bail out the airlines, Congress passed the Air Transportation Safety and System Stabilization Act (ATSSA), which authorized $15 billion in expenditures. President Bush, seeking to gain rapid approval of the bill, announced that safe, viable, and effective commercial air traffic is important to the U.S. way of life. In response, the House of Representatives quickly passed the bill 356 to 54 votes, and the Senate followed suit with a vote of 96 to 1 in probably the largest showing of bipartisanship since the World War II. Specifically, the legislation gave the airlines 5 billion U.S. dollars in immediate cash assistance and 10 billion U.S. dollars in loan guarantees. Many Congressmen expressed concerns over bailing out an already financially insecure industry, but the pressure to do something quickly was too much for politically motivated leaders in Congress. At the time, it seemed unpatriotic to oppose the bill, even though one lone Congressman did just that.

To address one apprehension, the bill contains a provision, which limits the salaries of airline executives. Any airline that accepted the bailout money was prohibited from raising the salaries of its executives that make over 300,000 U.S. dollars per year for a specific period of time. It was thought this provision would prevent the bailout money from ending up in the pockets of top executives

instead of serving its intended purpose. Admittedly, the traveling public virtually stopped flying for a period of time immediately after the attack. It remains to be seen whether the significant losses the airlines allegedly incurred are an accounting fiction.

Airlines squealed that they were significantly struggling after the attack, complaining of empty planes and lost profits. They quickly laid off 80,000 workers and grounded 20 percent of the flights (Adams, 2001). However, in December of 2001, approximately two months later, the financially desperate months seemed to be fading away. For example, American Airlines announced it intended to recall many reservations agents and decided to cancel the scheduled layoffs of numerous mechanics. The other airlines followed suit and by mid-2002 it once again became difficult to find a seat on an aircraft. Once again aircraft were full, and the airlines began rescheduling previously canceled flights. The short-lived days of cheaper and more competitive airfares to regenerate passenger travel had already dissipated. For example, in the summer of 2002, it became almost impossible to find a really discounted fare to Europe, especially on short notice.

The airline industry is recovering from 11 September. However, statistics indicate that many passengers are flying at small regional airports rather than larger international ones. Some of the larger airports continue to have long security lines, especially during peak traveling times and dates. Northwest Airlines, the world's fourth largest airline, lost $264 million in the first half of 2002, which is actually less than most of the other major carriers. The year 2002 witnessed, U S Airways filing for bankruptcy, United Airlines lobbying for government support, and most airlines making major job cuts. According to the Air Transport Association, revenue declined for all major airlines during the first half of 2002. United Airlines income dropped 22 percent, U S Airways 24 percent, and American Airlines 16 percent. Holding on were Alaskan Airlines at 2.2 percent, Southwest at 8.5 percent, and Delta at 13.7 percent (Air Transport Association, 2002). In comparison, airline industry operating revenues in 2005 reached 151,255 millions of dollars and 163,824 in 2006 (Air Transport Association of America, Summary: 1995 to 2006).

PROTECTING PUBLIC AIR TRANSPORTATION

It is clear that airlines are a primary means of public transportation in large cities. Thousands of people may jam a terminal on any given day. Larger airports resemble small cities and definitely present a particularly enticing target for terrorists for several logistical reasons. First of all, they typically are crowded with people every day. Second, airlines move on a scheduled basis in predictable geographic locations. Most importantly, they are public facilities providing a public service and are extremely difficult to harden as targets. Consequently, public transportation is an attractive target in terms of difficulty in providing adequate physical, personnel, and operational security. The challenge is substantial and should not be neglected.

The threat can emanate from a terminal assault, a hijacking, and the use of an aircraft as a weapon and even the exposure of commercial aircraft to surface-to-air missiles. Congress seems to have reached the conclusion that lethal force must be met with lethal force. The Senate joined the House of Representatives in September 2002 in voting overwhelmingly to permit pilots to carry guns in the cockpit. The wisdom of this publicity motivated vote remains to be fully evaluated. The government has engaged in many false starts over the years in protecting the public air transportation system. This is likely one of them. In another rush to "defend the public," the government lowered the standards for airport screeners in an attempt to meet Congressional mandated but arbitrary compliance dates for federal airport screening. The fact that 29 people were arrested in the fall of 2002 on federal charges of lying or offering false papers to get jobs at three Florida airports makes the point. The following chapters will review the history behind the threats to airports, aircraft, and the airline industry in general. The book will also analyze local, national, and international efforts to protect the public and the air transportation industry.

FIGURE 1.3 General and corporate aviation was literally grounded after 9/11, but has prospered and expanded in spite of the now familiar TSA "hassle factor."

CONCLUSION

The horrific events of 11 September have exemplified the potential results of terrorist attacks on not only the aviation industry, but also the financial heartbeat of the nation and the global economy in general. The attack on the World Trade Center and the Pentagon will clearly be the most expensive aviation disaster in U.S. history. The lingering costs, according to the airlines, came close to completely devastating the economic well-being of the industry, let alone the national economy as a whole. From an equipment perspective alone, each of the four airplanes was insured for 2 billion U.S. dollars; 50 billion U.S. dollars for the airframe, and the remaining amount for damage and liability. These figures omit, of course, the incalculable loss of life. Regardless of any particular viewpoint on the exact extent of the damage, the concept of the airline industry as a strategic national asset was affirmed. Essentially the attacks threw an incredible wrench into the national and world economic machinery, reaching almost everyone in some manner, whether personal or economic (see Figure 1.3).

The U.S. stock exchange was closed for several days after the attack but eventually reopened on Monday, 18 September. As perspective, it is significant to point out that the U.S. stock markets had not been closed for three consecutive days since the Great Depression. When the markets reopened, the economic effects of the tragedy became self-evident. As already noted, airline stocks in particular plummeted. Other related industries were similarly affected. Warnings of additional threats continue to disrupt confidence in the markets, complementing previous unrelated economic woes. Consequently, investor faith in a quick economic recovery lingers behind previous expectations.

The previous Friday, the House and the Senate of the U.S. Congress overwhelmingly approved a $15 billion bill aimed at rescuing the aviation industry from the immediate effects of the terrorist hijackings. The bill also contained a provision of an additional $3 billion in support of enhanced security upgrades. The costs related to upgraded security will also remain a hot topic of debate. Who should pay and exactly how much should be spent will affect both security and the gross national product for years to come in many ways.

Again, according to the airlines, the attacks allegedly financially overwhelmed airlines worldwide. In response, in Minnesota, Northwest Airlines announced the company would lay off 10,000 employees. In Atlanta, Delta announced the furloughing of 13,000 employees. Industry executives invoked wartime powers to override no-layoff protections in employee contracts. The CEO of Northwest, Richard Anderson, summed up the situation when he said, "The fact that our industry

was essentially turned into a weapon of terrorism on September 11 causes us to take immediate action to be certain we preserve the long-time future of the airline." (Kennedy and Phelps, 2001).

Whatever your perspective, it is no longer reasonable to argue that the airline industry is not a national and global asset. The aviation industry is clearly an asset that directly affects the employment of millions of aviation industry employees and indirectly affects many millions more. Security officials must also be cognizant of the threat to cargo and avoid focusing totally on screening passengers and luggage. The real question is how the world came to be immersed in the quagmire of globalized terrorism and what can realistically be done about it on an international global scale.

REFERENCES

Adams, Marilyn, *USA Today*, 26 December 2001.

Air Transport Association, Percent Change in operating revenues first six months of 2002, *Star Tribune*, 8 September 2002, pg. D8.

Air Transport Association of America, Washington, D.C., *Air Transport Annual Report*, Table 1038. U. S. Scheduled Airline Industry—Summary: 1995 to 2006.

Air Transportation Action Group, The Economic Benefits of Air Transport, 2000 edition, pg. 4.

Air Transportation Association Study, 1999.

Aviation Security Advisory Committee, Report on General Aviation Airport Security, Pamphlet A-100, November 2003.

Bureau of Transportation Statistics, http://www.bts.gov/press_releases/2008/bts004_08/html/bts004_08.html.

Bureau of Economic Analysis, U.S. Department of Commerce.

Bureau of Transportation Statistics, T-100 Domestic Market; http://www.transtats.bts.gov/homepage.asp.

Civil Aeronautics Act Annotated, 52 Statute, 973.

Columbia Encyclopedia, 6th ed., Columbia University Press, 2001.

http://www.atag.org/ECO, 4/22/01 pg. 3.

http://www.natca.net/mediacenter/press-release-detail.aspx?id=455.

Kennedy, Tom, and David Phelps, NWA will lay off 10,000; $15 billion airline aid OK'd, *Star Tribune*, 22 September 2001, pg. 1.

Mini-Brief, "Airline Deregulation: An Early Appraisal," Congressional Research Services, Library of Congress, 25 June 1980, No. MB 79247, pg.1.

Plane Business, 2001 Stock Performance, http://www.plane business. com/stock performance/2001.html, 28 May 2002.

U.S. Department of Labor, Bureau of Labor Statistics, http://www.bls.gov/oco/cg/cgs016.htm.

2 The Historical Hijacking Threat and Government Response
A Persistent Problem

NEWS

September 1970: Palestinian terrorists hijack several airliners forcing them to fly to the Jordanian desert. With the media present and cameras filming, the aircraft are destroyed in fiery explosions costing the airlines millions.

1985: During the height of the Christmas season, fanatic Japanese terrorists, in support of the Palestinian cause, open fire on helpless airline passengers at both the Vienna and Rome airports. In addition, Shi'ite gunmen hijack TWA Flight 847 from Athens. The hijackers kill one of the passengers and disperse the rest of them throughout Beirut, making significant demands for their release.

1988: Libyan intelligence officers plant a bomb in the belly of Pan American Flight 103, which explodes over Lockerbie, Scotland killing hundreds.

2001: President Bush calls on U.S. governors to mobilize the National Guard to help boost security at the nation's airports until tighter security can be put into place.

4 July 2002: A former Egyptian citizen living in California opens fire on passengers waiting in line at the El Al check-in counter. A security guard fatally shoots the attacker.

August 2006: Dutch F-16s escorted a Northwest Airlines flight bound for India back to Schiphol airport in Amsterdam after the pilot radios for help. Police arrest 12 passengers who had aroused suspicions.

HIJACKING

Hijacking has been characterized as the forcible seizure of any vehicle in transit to commit robbery, extort money, kidnap passengers, or carry out other crimes. Historically, the term was used to indicate the illegal taking of property from someone traveling on a public road. In the United States, the term first came to mean the theft of goods in transit by truck. Eventually, the term hijacking grew to encompass the seizure of ships, usually for theft and extortion. The concept of hijacking was eventually extended to include the unlawful taking of airplanes.

More accurately, under the reign of Queen Elizabeth I of England, the Elizabethan Sea Dogs, privateer ships sailing under the protection of the English flag, committed repeated violent acts of piracy against the Spanish fleet. Under similar circumstances, American pirates significantly contributed to the American Revolution and the War of 1812. Both countries had strict laws against such conduct, even though they unofficially resorted to analogous conduct themselves.

Sea piracy continues today, especially in the South China Sea where it has received international attention because of its frequency and operational proficiency. Westerners are, nonetheless, more familiar with the hijacking of the Achille Lauro. The Palestinian Liberation Organization

hijacked the Italian cruise ship off the Mediterranean coast of Egypt on 7 October 1985. Egyptian President at the time, Hosni Mubarak, induced the hijackers to surrender after promising air passage to Tunisia. However, during the incident the hijackers had shot to death a Jewish American passenger, 69-year-old Leon Klinghoffer. Consequently, President Ronald Reagan sent U.S. Navy jets to intercept the escaping hijacked aircraft and forced the plane to land at Naval Air Station (NAS) Sigonella, Italy. Critics have alleged that U.S. troops engaged in some piracy of their own. Modern terrorism continues to take the form of piracy, but it has expanded to include attacks in the air as well as on the sea.

Currently, hijacking, skyjacking, or air piracy is defined as the forcible commandeering of an aircraft while in flight. During the 1970s, the incidences of hijacking in the United States became intolerable. Cuban exiles, fleeing felons, and extortionists topped the list of hijackers. In 1973, the Federal Aviation Administration (FAA) consistently began searching all passengers and carry-on luggage. Prior to such efforts, political terrorists had begun to consistently carry out hijackings either to gain publicity for a cause or to obtain the release of fellow terrorists from prison. U.S. government figures for the past three decades show the highest number of hijackings took place in 1970 when the total reached 74 (*Associated Press*, 1 Jan 2000).

In the mid 1980s, the problem escalated further. In 1985, a TransWorld Airlines (TWA) flight, departing from Athens, was hijacked and diverted to Lebanon where the hostages were detained for 17 days (see Figure 2.1). The TWA Boeing 727 had 153 people on board. Three Lebanese Moslem Shia demanded the release of more than 750 Lebanese and Palestinians imprisoned in Israel. In a cooperative effort, Israel released 31 prisoners, and the hostages were eventually released. As mentioned, soon thereafter, the Italian ship Achille Lauro was hijacked in the Mediterranean Sea, further highlighting the problem. In both instances, American citizens were killed. The situation demanded action, and the FAA began to improve security measures while government leaders sought to improve international cooperation to combat the use of aircraft to further terrorism.

Regardless of massive security efforts on the part of authorities at the time, hijackings continued (see Figure 2.2). In fact, 20 years later, between the years of 1992 and 1996, although indicating a reduced number, 129 aircraft were still hijacked internationally. According to FAA statistics, 40 planes were hijacked in 1990, 12 planes in 1992, 31 in 1993, 23 in 1994, 9 in 1995, and 14 more in 1996 (Federal Aviation Administration, 1996). There were no hijackings in the United States from

FIGURE 2.1 An armed terrorist holds a gun on Trans World Airline pilot John Testrake during an interview from the hijacked plane, TWA Flight 847, at the Beirut International Airport. Terrorists have become particularly adept at using the media to advertise their cause.

FIGURE 2.2 The hijacking of TWA Flight 847 in 1985. (Source: AFP Agence France Presse)

1991 through 2000 (U.S. Department of Transportation, 2002). Increased security has indeed been productive and lifesaving; although it has not stopped, nor will it likely ever stop the threat completely. Terrorists who will surely continue to exploit any lapses in security measures will always discover any reduction in such diligence. The lull between 1996 and 2000 was shattered on 11 September 2001, when terrorists hijacked four U.S. airliners and crashed three of them into buildings and one into the ground, causing the death of thousands. As is now common knowledge, this unprecedented attack resulted in an immediate and drastic heightening of air transportation security.

Furthermore, the public, especially since 11 September, has continued to demand even more innovative techniques to fight the continuing problem. Some of these innovations are arguably more intrusive than the now familiar metal detectors and x-ray machines. Therefore, much like in the past, and despite renewed demands by the public for safer airport security; some critics have pursued legal battles to stymie efforts to increase levels of security.

LEGAL RESPONSES TO EXPANDING SECURITY MEASURES

Gregory T. Nojeim, legislative consultant to the American Civil Liberties Union (ACLU), presented a statement on the civil liberties' implications of airport security measures before the White House Commission on Aviation and Security on 5 September 1996. Generally, the ACLU devotes its efforts to protecting the principles of freedom, including the prohibition against unreasonable searches and seizures set forth in the Bill of Rights. The group has supported the need for appropriate measures to ensure that air travel remains relatively safe. On the other hand, the ACLU has publicly and persistently reminded the proponents of intrusive security procedures that civil liberties should not be sacrificed to make air travel more secure. The statement made to the Commission outlines three basic premises, and they remain pertinent today:

- Passengers should not be detained, questioned, and searched as if they are potential criminals, unless there are specific facts that indicate that they may commit a criminal act.
- No passenger should be singled out on the basis of his or her perceived or actual race, religion, national origin, gender, sexual orientation, or political opinion.

- Passengers not legitimately under suspicion should not have to fear that their private effects and private lives will be held up to public scrutiny or that personal data about them will be made accessible to others without their fully informed, and genuinely noncoerced, consent (Internet: http://www.aclu.org/congress/airtest.htm, 2001).

An example of a case, which exemplifies the concerns of civil libertarians, is highlighted in the case of *Brent versus Ashley,* et al. 247 F.3d 1294, 2001. Rhonda Brent, the only black woman arriving on a flight to the United States from Nigeria, alleged in a federal lawsuit a violation of her Fourth Amendment rights during a strip search and subsequent x-ray of her person. Two U.S. Customs officers initially searched her baggage and found nothing. They decided to conduct a full body patdown and strip search. The officers, according to court records, justified the search based on the nervousness of Brent and her arrival from an alleged source country. The body patdown and strip search consisted of touching her crotch area, ordering her to pull down her clothes, removing and examining her sanitary napkin, squeezing her abdomen from the pubic to thorax and monitoring her responsive actions. An electronic document search also revealed nothing. The Customs agents decided that an x-ray and pelvic examination at a hospital was appropriate. Brent was presented with a consent form and told that if she refused to sign it she could be held for 35 days or indefinitely until a judge ordered the x-ray. Brent requested to speak to an attorney and to call home. Both requests were denied. The pelvic examination and x-ray revealed the complete absence of drugs. After a ten-hour delay in her trip, she was returned to the airport. Brent filed suit against nine Customs employees alleging the commission of common law torts and constitutional violations.

The court concluded that the decision to stop and search Brent was based on the fact that she shook her head in disapproval on seeing the way Customs officials were treating a black male copassenger. Brent argues that a simple expression of disapproval does not provide reasonable suspicion to justify a search and the court agreed. However, the law clearly provides that "routine border searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause or warrant." The court further reasoned that an invasive border search of someone's body requires a showing of reasonable suspicion (*United States versus Montoya de Hernandez,* 473 US 531, 538, 105 S Ct. 1300 [1985]). The court ultimately held that because Brent had failed to demonstrate that the initial stop did not constitute more than a routine border search, the initial stop did not violate her Fourth Amendment rights. However, a nonintrusive search of Brent's person and her luggage revealed nothing; she presented verifiable residence and employment information, and an electronic document search of her revealed nothing. The court, therefore, went on to find the strip search of Brent was unconstitutional. It is not likely many people would tolerate this kind of conduct and still want to spend money to fly. Although hopefully well intended, the conduct of these U.S. Customs agents, with hindsight, appears to be way out of proportion to the overall situation even in light of 11 September.

Other critics have focused on racial profiling, computerized passenger registries, and cameras that search under clothing. For example, the Center for National Security Studies in Washington, D.C. believed that legislation signed into law by the Clinton Administration posed serious threats to constitutional rights. This group had focused on the fact there had been only two international terrorist acts committed on U.S. soil up to that time, namely, the notorious bombing of the World Trade Center in February 1993, and the occupation of the Iranian Mission in New York City in April of 1992. The massive attack of 11 September changed the perceptions of many travelers and reinforced the idea that the overwhelming number of American air travelers appear willing to submit to more technologically superior levels of security intrusion to keep the air travel environment safe from criminals or terrorists. This does not obviate the constitutional issues. Furthermore, since 11 September, former Attorney General Donald Ashcroft had announced, in conjunction with Congressional approval, intentions to empower law enforcement with even broader powers.

Of note, is that future threats may well emanate from within the United States. Post 11 September, dissemination of anthrax via the mail represents a prime example of the possibility of such an

internal threat. Domestic terrorist groups are proliferating, and international terrorists will still seek to carry their cause to the United States. It is a clear and present danger that sufficient threat still exists. Concurrently, travelers appear to support the continuation of appropriate security measures. That support, however, continues to be dependent on the public's perception of the threat and the conduct of those administering them. Furthermore, the perceptions of the ACLU, the Center for National Security Studies, the Arab-American League, and others that constitutional guarantees are being placed in danger will persist.

INTERNATIONAL PERSPECTIVES

International efforts to combat the problems related to air hijacking have been mixed. Some countries have matched or exceeded the efforts of the Unites States, most notably those in Europe and Israel. Other countries may recognize the threat but be totally unable to finance any improvement measures. Still others totally disregard the need for adequate security measures and tend to make air travel to and from those countries potentially dangerous. Admittedly, the temptations offered by a specific airport environment to terrorists will fluctuate, and the approaches to counter the threat will vary as well.

Additionally, efforts to enforce and adequately make use of existing international treaties will also only progress when the international community is forced to recognize the need. Unfortunately, different commitment levels on the part of the signatories often limit the effectiveness of international treaties. Divergent interpretations of provisions, various attitudes toward the particular treaty, and the difficulty in appropriately enforcing them also affect the outcome of each effort to utilize the treaties. Overall, countries diverge in perception of the threat. Exposure to a particular threat also differs, and levels of international attention to fluctuating sets of circumstances often change. Consequently, although well-intentioned, the treaties have often proved to be ineffective.

THE TREND BEGINS

On November 24th, the day before Thanksgiving 1971, a passenger calling himself Dan Cooper boarded Northwest Orient Flight 305, at Portland, OR. He looked like any other businessman. Only 36 other passengers were on board that day, and the plane was, therefore, only partially filled. Just as the plane was taxiing for takeoff, Mr. Cooper handed a note to the flight attendant telling her to read it immediately. The note concisely indicated, "I have a bomb in my briefcase." Cooper announced he would blow up the plane unless he was given $200,000 and four parachutes. To bolster his demand, he let two of the flight attendants physically see what he claimed was a bomb.

In Seattle, WA, the authorities decided to comply. Mr. Cooper received the money and the parachutes, even though the chutes hastily were prepared at nearby McChord, Air Force Base. The hijacker permitted all the passengers and two of the flight attendants to deplane, but demanded the pilot fly on to Reno, NV, despite the fact he had earlier expressed a desire to proceed to Mexico. Surprising authorities, and as per Cooper's specific instructions, the plane headed for Reno at low altitude and minimum cruising speed with the flaps down and ventral stairs extended. When the crew landed at Reno, he was not on board. Miraculously, he allegedly survived after parachuting out over rough terrain. He has never been officially found, although stories abound about both his success and alternatively about his possible death on impact. Nine years after the incident, 8-year-old Brian Ingram found $5,800 of the extortion money when he was vacationing with his family. The FBI reopened the case at the very end of 2007, hoping that improvements in technology would help crack the case.

With the ensuing publicity the incident received, Cooper became a bit of a folk hero, and his legend grows somewhat each time the tale is told. Nonetheless, airport authorities did sit up and take notice of his success and began to take measures to prevent the event from recurring elsewhere. From a certain perspective, this was one of the first and only truly potentially successful hijackings.

It was a simple criminal act. Even more deadly threats were soon to be improved on and fine-tuned by international terrorists. It was to take much more serious disasters to really get the public's, the U.S. government's, and the international community's solid attention.

EARLY FEDERAL AVIATION REGULATIONS

It is generally understood that Federal Aviation Regulations (FARs) designed to ensure the security of airports serving scheduled air carriers were required to have screening programs. In other words, air carriers had the responsibility to prevent and deter carriage of weapons and explosives aboard aircraft by potential hijackers. Where applicable, air carriers issued and carried out written security programs, which accomplished 100 percent screening of all passengers and searched all carry-on items (FAR Part 121.538 and Part 108.7).* Post 11 September, this basic concept has been expanded to require all baggage be screened by explosive detection equipment before 31 December 2002 and not by agents of the airlines but by the government.

Conversely, airports serving applicable air carriers are responsible for preventing and deterring unauthorized access to the air operations area and for providing law enforcement support at passenger screening stations. Basically, FAR, Parts 107 and 108, required airport operators and airlines to issue a security program incorporating the above procedures. Overall, the FARs set the general guidelines for all security assets and procedures at U.S. airports and for U.S. and foreign airlines servicing U.S. airports.

Originally, the amount of security required to effectively deter hijacking was thought to be directly proportional to the size of the aircraft. This approach took into consideration the relationship between the amounts of publicity the hijacker could receive from the incident and the number of passengers on board; meaning the larger the aircraft the more hostages and the bigger media event. Therefore, tighter security rules were originally developed for larger passenger aircraft.

To ensure consistent application of the FAA's security rules and to achieve the necessary and appropriate level of security per aircraft, FAA Regulation Part 108 evolved. As stated, Part 108 based security requirements on aircraft complexity instead of certification and categorized commercial airplanes into three groups according to configured seating capacities:

- 0ver 60 seats
- 31 through 60 seats,
- Less than 31 seats.

Commercial aircraft with over 60 seats had the most stringent requirements. Concurrently, Part 108 required the adoption of a comprehensive security program for operations with 31 through 60 seats. The program was supposed to be comparable to that required for operations with airplanes having more than 60 seats, but normally the smaller operators were required to only have to implement those portions of the program that required the following:

- Procedures for contacting a law enforcement agency and arranging for a response to an incident when needed
- Instruction for all crewmembers and internal employees in appropriate security procedures. Each operator was required to implement its full security program on notification of specific threats by the FAA.

For operators of smaller aircraft, 1 through 30 seats, no security program was required unless passengers had uncontrolled access to a sterile area. The concept of "sterile areas" will be discussed in a later chapter. In all cases where passengers had uncontrolled access, or where passengers were

* *Note*: Current regulations are contained in 49 CFR Chapter XII, Parts 1500–1699.

discharged into a sterile area, provisions had to be made to properly screen the passengers. Carriers controlled access to the sterile area through surveillance and escort procedures or through the screening procedures of another carrier.

This has become a particularly sensitive issue, especially since 11 September. Experts agree that it can be fairly easy to circumvent security procedures at a small feeder airport and later gain access to the sterile concourse at a larger airport. Unfortunately, as recently as March 2002, one small airport in Minnesota had a brand new x-ray screening machine still visible in the terminal in its original box and still not deployed for regular use.

AIRPORT SECURITY PROGRAMS

Where security programs were required by the FARs, both the airlines and the airport were required to have security programs in writing signed by the operators and approved by the FAA. Overall, the airport security program was at a minimum to include descriptions of the following:

- The air operations area — that portion of the airport designed and used for landing, takeoff or surface maneuvering of aircraft
- Areas on or adjacent to the airport, which affect security of the air operations area
- Each exclusive area
- The procedures, facilities, and equipment used to perform the control functions by the airport operator and by each air carrier
- Notification procedures
- Alternate security procedures for use in emergencies and other unusual conditions
- The system for maintaining records of security-related incidents
- The law enforcement support system and the peace officer training program*

Furthermore, as mentioned, Part 139 did not regulate security procedures at reliever or feeder airports that flow into larger metropolitan airports. For example, Flying Cloud Airport in Eden Prairie, MN routinely left the gates to the airport open at all times. Controversy has often developed between owners of aircraft that want aircraft secured and operators of a flight school that want easy access for students. On top of proprietary concerns, these smaller airports are far too accessible to the determined terrorist for a variety of reasons. Recent threats of potential biological attacks possibly by use of crop-dusting aircraft are a perfect example. The overall security situation at these facilities still poses a major loophole in a broader aviation security context. Additionally, the status of the student pilots has become an issue.

NEW CARRIER RULES 1972

Part 121.538, the rule specifically pertaining to air carriers at the time, became effective on 31 January 1972 (Federal Register 37:2500, Docket 11432). It required each certificate holder to adopt and implement a screening system that would detect weapons and explosives in carry-on baggage or on the person of passengers. Because the public was screaming for action, the amendment to Part 121 was rapidly, some say hastily, put into effect with only three days' notice to the airlines. The Rules were also once again adjusted to require each carrier to submit its screening program

* *Note*: As opposed to the common notion of airport passenger security, the security provisions of FAR Part 139 are primarily concerned with public protection and appropriate safeguards against inadvertent entry of persons or large domestic animals into any air operations area. The provisions of FAR Part 107 Airport Security are related to the control of access to air operations areas by unauthorized persons and ground vehicles. Like Part 107, Part 108 "Airplane and Airport Operator Security" was also concerned with the prevention of unauthorized persons and vehicles. In essence, FAR 107 and FAR 108 addresses issues of criminal violence and aircraft piracy, whereas Part 139 is concerned with the segregation of the public from air operations as a function of operational safety.

to the FAA Administrator no later than 5 June 1972 (Federal Register, 37:4904, 7 March 1972). Procedures were inconsistent between airlines, and the rush was on to comply with the new rules.

Each carrier's program was to contain some minimum acceptable elements. They included:

- The ability to prevent or deter unauthorized access to its aircraft;
- The means to ensure that baggage would be checked in by a responsible agent or representative of the certificate holder; and
- The capability to prevent cargo and checked baggage from being loaded aboard its aircraft unless handled in accordance with the certificate holder's security procedures.

How each of these requirements was implemented was varied, depending on the airline. The airlines subsequently had many comments to submit, as was their right under the Administrative Procedures Act. Many useful suggestions were made based on airline experiences during this first trial and error period. Several other provisions were incorporated after receiving comments submitted as per the original notice of Proposed Rulemaking issued in September. The rules have been continually amended over the years and are once again being closely reviewed and updated by the new Transportation Security Administration (TSA) as part of 49 CFR Chapter XII. The rules had also undergone considerable review in the year 2000-2001.

Admittedly, in 1972, after President Nixon issued a presidential decree declaring a renewed emphasis on air security, rules were somewhat tumultuously put into place. Consequently, the rules were revamped again to reflect the perceived pressure to immediately implement the screening requirements. The new deadline for carrier screening programs was moved up to 8 May 1972. Further refinements took place in 1981 when Part 121.538 was re-written as Part 108. Part 107 continued to pertain strictly to the airport operator. The Report of the President's Commission on Aviation Security and Terrorism, issued on 5 May 1990, became the catalyst for recommendations to again amend the rules in the 1990s.

Due to pressure from the public and concerned government officials, the FAA originally had rushed to implement changes to the FARs. As stated, Part 121.538 was issued on 31 January 1972, and required each certificate holder to adopt and implement a screening system that would detect weapons and explosives in carry-on baggage or on the person of passengers, all with only three days' notice. The rules, although not considered by the airlines and airport operators to be totally unnecessary, presented some huge obstacles. The airlines and airport operators were deeply concerned over the ability to achieve them within the required time frame. Equipment was scarce, the costs were likely to be high, and the airlines were concerned about passenger reactions to the delays. The same situation permeated the industry in light of new rules mandating 100 percent screening by new explosive detection equipment in 2001.

The development of airport and airline security regulations actually evolved over many years and months. Aviation bombings and hijackings were rare but represented a significant threat, especially if you are a passenger on board or involved on the ground. In an attempt to reduce the vulnerability of aircraft, implementation of the 1972 rules forced air carriers to bear the primary responsibility for applying security measures to passengers, flight and maintenance crews, carry-on baggage, and cargo. Furthermore, originally Section 538 of the former Part 121 specifically required each scheduled carrier to develop and implement a security program designed to prevent or deter the carriage aboard aircraft of sabotage devices or weapons and to prevent or deter unauthorized access to aircraft. It also required passenger baggage to be checked and cleared in accordance with detailed security procedures, thereby resulting in the security checkpoints now so familiar at airports today.

Landmark revision of procedures and security measures after repeated hijacking incidents in the 1970's also gave rise to the specifics of Part 107 and Part 108. Part 107 formally gave airport operators the responsibility for providing protection against unauthorized access to air operations areas. Furthermore, airports governed by State and local authorities were held responsible for assuming

duties to maintain a secure ground environment, supported by official law enforcement personnel. Part 107 specifically applied to Airport Operators and Part 108 pertained to the airline carrier. Both parts have been amended from time to time and were first significantly amended as a result of the Report of the President's Commission on Aviation Security and Terrorism of 1972.

Part 108 rules have also gone through much iteration, but by the end of 1972 the increasing frequency of terrorist or criminal threat prompted the FAA to require at a minimum:

- Screening of all persons and carry-on baggage before entering an airport's departure area (only authorized personnel should be able to enter restricted areas)
- The availability of a sworn law enforcement officer at the screening point within a specific period of time
- Development by both scheduled airline carriers and airport managers of security programs approved by the FAA
- Development of an airport disaster plan

Use of the new procedures exposed some of the flaws. For example, an emergency order closed a glaring loophole in the law, which had originally excluded smaller aircraft from the screening procedures. After two hijackings of Pacific Southwest Airlines on 5 and 6 July 1972, respectively, the need to expand the screening requirements became self-evident. At the time, a California man received the unenviable distinction of being hijacked twice in a single trip. The emergency order was directed at high density "shuttle flights" (*Aviation Daily*, 1972). This order was to become effective 30 days after issuance, and all carry-on baggage was to be screened for this level of travel as well. Passengers themselves were simply required to show two forms of identification, and those that could not were required to be screened. At the time, the smaller airlines claimed they were being discriminated against because at the time larger airlines still had not been forced to conduct 100 percent screening of passengers and carry-on baggage. This set of circumstances, of course, would change in the very near future.

Additional revisions to FAR Parts 107, 108, and 139, effective in November 2001, filled in other loopholes in the initial rules. The rules increased the number of aircraft operators subject to the security program provisions. They now included all individuals that enplaned or deplaned into a sterile area and even pertained to certain helicopter operators. The rules also expanded the training requirements for these same aircraft operator security personnel and required them to participate in airport-sponsored contingency exercises. It should be pointed out that general aviation aircraft were not intended to be covered by Part 108, but these aircraft as well as fixed based operators (FBOs) were covered as tenants under the rules contained in Part 107 and Part 139. The changes better defined the areas of an airport in which security interests are the most critical.

NEW AIRPORT OPERATOR RULES 1972

The air carriers were not the only entities compelled to quickly provide a safe environment for aviation. The rewritten Part 107 required the airport operator to "immediately adopt and put into use facilities and procedures designed to prevent or deter persons and vehicles from unauthorized access to air operations" (Federal Register, 37:5689, 5691 18 March 1972). In another hurried but necessary move, the FAA gave airport operators only 90 days in which to prepare and submit to the FAA Administrator an entire security plan for the airport facility. Airport operators all over the nation scrambled to comply. Again the quality of the procedures varied from airport to airport. Some local authorities believed their airport was low risk and did not emphasize the need for real quality programs. Others immediately grasped the need and reacted appropriately.

Unfortunately problems persisted. From the time period December 1998 through May 1999, the inspector general of the FAA conducted approximately 173 tests at eight U.S. airports. In a somewhat shocking discovery, the investigators gained unauthorized entry to restricted areas on 117

occasions. The Inspector General gained access by following authorized employees into restricted areas, riding unguarded elevators, going through unlocked gates and doors, and walking through cargo areas. Some of the problems that plagued airport operators in the past therefore endure today. The investigators concluded that airport operators and air carriers had not implemented effective access control procedures, that they engaged in improper training of employees, and that the FAA did not coordinate appropriate oversight programs (Anderson, 2000.) History often repeats itself.

RESISTANCE FADES

The airlines abandoned the last bit of resistance to 100 percent mandatory screening ironically after two nonterrorist attempted hijackings in October 1972. In a twist of fate, the airlines were completely frustrated with the increasing numbers of fleeing felons seeking to escape by acquiring free airline transportation. In one particular case, an airline agent walked down a jetway to secure the aircraft door prior to taxiing and takeoff. Before the agent was finished securing the door, four late passengers followed him into the jetway and shot him. They also shot at a ramp serviceman, who was motioning to the flight crew and simply caught the attention of the escaping felons. He was trying to advise the flight crew that they had started the engines while the plane was still being refueled. The hijackers turned out to be a bank robber and three murder suspects. They professed no political cause, just a desire for a quick getaway, and the plane appeared to them to be a handy tool to do so.

Immediately on the heels of the first incident, three alleged rapists hijacked a Southern Airways DC-9 departing Birmingham, AL, in November 1973. They controlled the aircraft for almost 30 hours and eventually shot and wounded the copilot. A demand for 10 million U.S. dollars was deferred, and authorities turned over 2 million U.S. dollars to the hijackers, who subsequently diverted the plane to Havana, Cuba. Of particular note, was that at one point the hijackers wanted the pilot to fly the aircraft into a nuclear facility. This comment alarmed a great many people, particularly the authorities at the Tennessee Valley Authority who were alerted to the threat (Brennan, 1973). The incident did have a silver lining. Both federal authorities and airline security were unprepared for incidents of this type, and the incidents provided a wakeup call. At this point, the public, law enforcement, and airline and airport security officials were forced to collaborate on more effective ways to successfully deal with hijackers.

In another quickly implemented attempt to curb the tide of both terrorist and simple criminal attempts to commandeer aircraft, the FAA issued two emergency regulations on 5 December 1972. One gave carriers 30 days in which to institute a 100 percent search of all passengers and carry-on items, and the other gave airport operators 60 days in which to station at least one law enforcement officer at each passenger checkpoint during boarding and preboarding. The airlines and airport operators again immediately scrambled to comply. The costs were considered to be prohibitive by the airlines and those entities operating the airports: private, local, and state alike. Local law enforcement often insisted that they had neither the resources nor the desire to accept such responsibility. Many believed hijacking was a federal issue. Consequently, airline and operator response was instantaneous, vocal, and negative. This was despite the fact they knew that something had to be done. It was the burden of cost that was the critically disputed factor. What entities should actually bear these costs continues as a controversial issue.

Regardless of all opposition, the airlines and airport operators attempted to implement the procedures on 5 January 1973. Passengers proved to be more resilient and infinitely more patient than the airlines had anticipated. The fear of terrorism had softened the public's attitude toward the benefits of improved and stringent security. Confusion, the absence of sufficient screening equipment, unfamiliarity with adequate security procedures, and the fear of legal repercussions from passengers all contributed to the general chaos, regardless of everyone's good intentions. Somehow everyone survived, and in time, regular routines were established. The process became more orderly and the flow of passengers smoother.

HOW TO IMPLEMENT THE NEW RULES

Regardless of general acceptance of the threat, not everyone agreed on how to meet the challenges the threat created. For example, the Airport Operators Council International (AOCI) initially sought a restraining order to stop the implementation of the new rules. They contended that hijacking was a chronic national problem and not an emergency. In response, they sought to overturn implementation of the new rules on an administrative technicality. They reasoned that the FAA, by not allowing time for comment before issuing the orders, was acting in violation of the Federal Administrative Procedures Act. A federal judge agreed, based purely on the procedural error argument and issued a ten-day restraining order. Many people believe that the real issue was whether the required law enforcement was to be federal or local and who should pay for the increased security. At the time, the Department of Transportation (DOT) clearly advocated that law enforcement responsibility remained with local authorities. Undersecretary of DOT, Egil Krogh, even testified before a congressional hearing that "We see no rationale for distinguishing the airport from the bus depot or the train station in the provision of police protection." (*Aviation Daily*, 28 February 1973). Although his comments sound like they hold a great deal of common sense, the comparison of a train station, bus depot, and airport is not quite valid, considering the complexity of the airport environment. Airports differ significantly from other transportation hubs such as bus terminals or train depots. First, airports require considerably more land, and they are generally located quite a distance from the cities they serve.

The controversy raged on, but on 12 February 1973, the judge vacated the restraining order, which had earlier been issued purely on an administrative technicality. The court correctly decided that the safety of the traveling public was in jeopardy by failure to implement the regulations (*Aviation Daily*, 13 February 1973). Regardless, AOCI continued the fight in the U.S. Court of Appeals. At that level, the court ruled that the FAA could continue to carry out the new rules, but penalties were not to be imposed without a hearing if the airport operator cited was making a reasonable effort to comply with the requirement (*Aviation Daily,* 10 February 1973) A good faith effort was required in light of the need, and minor infractions could be overlooked for the time being. Basically, airport operators evidencing the proper efforts to comply were not to be fined.

At the time, airline carriers were not only confronted with the gigantic issues of who should pay and who exactly should be in charge of law enforcement, but with other procedural specifics as well. Topics relating to the legality of searches and seizures plagued early compliance attempts. Some airlines had even forbidden employees from performing personal searches of passengers, fearing lawsuits. Right from the beginning, the airlines perceived the dilemma of having to deny permission to board the aircraft to those passengers that could not be cleared by the available magnetometers, thereby returning their fares, losing their business, and reducing company profits. The airlines were also legitimately concerned over potential lawsuits from intrusive searches from passengers who were not just insulted by the searches, but believed they invaded their personal privacy. The airlines were correct, and over the years untold numbers of lawsuits would be filed, settled, and litigated at great cost.

Jurisdictional issues also continued to arise. Who is really in charge is a familiar cliché. Back in 1973, Civil Aeronautics Board Chairman Secor Browne had criticized the program, arguing that airport security should be the purview of federal rather than local responsibility and that the federal government should allocate funds to cover the costs (*Aviation Daily*, 14 January 1973). He did not have much support, however, and local law enforcement persevered while bearing the lion's share of the responsibility. In a cooperative effort, however, the FAA continued to station federal law enforcement agents at airports as part of a regulated FAA security program and the Sky Marshal Program.

As mentioned, consistency was another problem, and early in 1975, the Air Transportation Association sought to work out a single standard security program. Their efforts produced the Air Carrier Standard Security Program (ACSSP), which attempted to bring some pattern to the diverse

interpretations of the new rules. In 1976, all but a few of the carriers accepted the program, and today it is mandatory.

PUBLIC LAW 93–366

By 1974, it became obvious that U.S. law relating to hijacking needed strengthening. On 5 August 1974, Public Law 93–366 was signed into law. Title I, better known as the Anti-Hijacking Act of 1974, and Title II, the Air Transportation Security Act of 1974, significantly changed the Federal Aviation Act of 1958. The law literally implemented the provisions of the Hague Convention for the Suppression of Unlawful Seizure of Aircraft agreed to by the international community.

To give some teeth to the new law, the international aspects of the legislation gave the President some broad statutory authority to regulate international air operations. For example, he could "without notice or hearing and for as long as he determines necessary" suspend the right of any carrier, either U.S. or foreign, to engage in air transportation between the United States and any nation permitting its territory to be used in furtherance of air piracy. In an additional broadening provision, the President also could suspend foreign air commerce between the United States and any foreign carrier that continued air service between itself and a nation harboring terrorists. This broad regulatory power sounds good, but like many things is more complicated and more difficult to enforce than it appears on the surface.

DISSEMINATION OF THREAT WARNINGS

After 30 years of implementation, some issues, such as the dissemination of threat warnings have still to be completely resolved. The bomb, which detonated in the belly of Pan American Flight 103 over Lockerbie, Scotland, forced authorities to rethink the threat warning issue (see Figure 2.3). On one hand, the airlines do not want to alarm passengers unnecessarily. However, many passengers believe that they have the right to know when a credible threat is levied against a specific aircraft or airline. In addition, it was later determined that some people within the system knew of the specific threat. Consequently, the real issue revolves around the idea of whether the right people get the right information when they need it to provide first-rate security. In October 1988, a similar Toshiba radio cassette player-type bomb was found in the possession of the Popular Front for the Liberation of Palestine. A second bomb was discovered inside a Toshiba Boom beat Model 453 in the automobile of a member of another terrorist group. It contained the same barometric triggering device used in the Pan American bombing. The FAA did send out a warning on 18 November 1988, a month before the Lockerbie bombing. However, at least one important Pan American airline official did not see the bulletin because he had been on vacation. The warning had gone out to all U.S. embassies and consulates, but the official that really needed the intelligence did not receive and react to avoid the tragedy in Scotland. Procedures now require carriers to provide written confirmation of receipt of the threat information. How they handle the dissemination of the information is still under debate.

RECOMMENDATIONS OF THE PRESIDENT'S COMMISSION

The Government Printing Office published the Report of the President's Commission on Aviation Security and Terrorism, dated 15 May 1990, which suggested more than 60 recommendations for improving airport and aircraft security procedures, as part of the aftermath of the Lockerbie tragedy. The committee, of course, concluded that the United States should pursue a more vigorous counterterrorism policy, which was not a particularly controversial recommendation to make. The report did document some other suggested changes including the following:

FIGURE 2.3 Police and investigators look at what remains of the flight deck of Pan Am 103 in a field at Lockerbie, Scotland, in this December 1988 photo. Two Libyan intelligence agents were eventually tried in a Scottish court in the Netherlands for this terrorist act. Only one was convicted. He was sentenced to 20 years imprisonment.

1. The federal government, not local government, should manage security at domestic airports through federal security managers, obviating any issues of jurisdiction between law enforcement agencies.
2. The State Department should pursue further negotiations with foreign governments to permit U.S. carriers to comply with U.S. law overseas requiring 100 percent screening and other security measures, even when they conflict with local law.
3. The FAA should launch a priority research program to improve technological means to prevent terrorism, placing the costs of research and development on the federal government.
4. Public notification of threats to civil aviation should be made where appropriate.
5. Victims should qualify for special financial compensation.
6. The State Department must take major steps to ensure that the families of victims receive prompt, humane, and courteous treatment and service from airlines.

Some of these ideas sound worthy on paper but would not necessarily be easy to effectuate. For example, the United States cannot demand that overseas airports comply with U.S. laws. The art of diplomacy is needed in persuading them of the needs involved. Some are more easily convinced than others. Additionally, public notification is riddled with problems. Who determines if the threat is real and who decides what action to take are really thorny issues that remain unresolved. Furthermore, the issue of jurisdiction between law enforcement agencies came back to haunt the nation in September 2001. Once again the concept of federal managers was openly discussed and now implemented over a decade later.

AVIATION SECURITY IMPROVEMENT ACT OF 1990

Based on the above-mentioned recommendations, the U.S. Congress moved swiftly. They enacted the Aviation Security Improvement Act of 1990, P.L. 101-604, dated 16 November 1990; a mere 6 months after the Commission issued the report. The act contributed to the successful implementation of many new and innovative security procedures. Title I of the law deals with general aviation security and Title II with appropriate U.S. responses to terrorism affecting Americans abroad. In the aftermath of the Lockerbie disaster, the White House was eager to show the public that the government was responding to a perceived need. One of the findings contained in the new law was that "the safety and security of passengers of United States air carriers against terrorists threats should be given the highest priority by the United States Government." Second, "the report of the President's Commission on Aviation Security and Terrorism, dated 15 May 1990, found that current aviation security systems are inadequate to provide such protection" (Internet: http://cas.faa.gov/reports/pl101604/pl101604.html).

First, the legislation established a number of new offices and positions. Within the FAA and the DOT, it created a Director of Intelligence and Security as well as numerous federal security manager positions authorized to implement security programs throughout the United States. The Director of Intelligence and Security reported directly to the Secretary of Transportation. The director's duties included the following:

- Receipt, assessment, and distribution of intelligence information relating to long-term transportation security
- Development of policies, strategies, and plans for dealing with threats to transportation security
- Other planning relating to transportation security, including coordination of countermeasures with appropriate federal agencies
- Serving as the primary liaison of the Secretary with the intelligence and law enforcement communities
- Such other duties as the Secretary may prescribe as necessary to ensure, to the extent possible, the security of the traveling public

The Act amended the Federal Aviation Act of 1958 (49 U.S.C. App 1341-1358). By doing so, it also created an assistant administrator of Civil Aviation Security. This individual became responsible for the day-to-day management of the FAA field security resources. The duties included, but were not limited to, the enforcement of security-related requirements, identification of research and development requirements of security-related activities, and assessment of threats to civil aviation, as well as the inspection of security systems. In essence, the position was designed to have one individual accountable for measures to strengthen air transportation security.

The legislation also sanctioned the positioning of federal security managers at all Category X U.S. airports and liaison officers at designated airports outside the United States. The general idea was to review and coordinate security on a global basis. The legislation also required an annual report to Congress, which solicits information on the successfulness of security at all levels of airport operations. Section 105 mandated background checks on airport and airlines personnel. Additionally, Section 107 ordered a program to accelerate research and development and the rapid implementation of new technologies and procedures to counteract terrorist acts against civil aviation. In further response to the President's Commission, the law also required that U.S. air carriers provide the Department of State with the passenger manifest for any flight involved in an aviation disaster within one hour of notification, thereby accelerating timely notification to the next of kin.

THE FEDERAL AVIATION REAUTHORIZATION ACT OF 1996

More legislation followed, with Congressional passing of the Federal Aviation Reauthorization Act of 1996. President Clinton approved Public Law 104-264 in October 1996. Title II contained Section 301 entitled Aviation Security, and included the "Report On Proposed Legislation On Funding for Airport Security," which mandated that the FAA, in cooperation with other appropriate agencies, conduct a study and submit to Congress a report on "whether and if so how to transfer certain responsibilities of air carriers under federal law for security activities conducted onsite at commercial service airports to airport operators or to the federal government or to provide for shared responsibilities between air carriers and airport operators or the federal government" (P.L. 104-264). The study examined the evolution of aviation security responsibilities. Overall, the study concluded that a system of shared responsibilities was the best model. It did not conclude, to the dismay of many local officials and airline corporate officers, that a transfer of air carrier responsibilities to another agency, entity, or the federal government was appropriate. This conclusion rankled those seeking to centralize security responsibilities within the federal government.

To soften the recommendations, the study details the incremental increases in federal government involvement in aircraft and airport security measures and predicts that the proliferation of assistance would increase, especially in the area of security training. The study also tackled the tough question of who pays for appropriate levels of security at American airports. In essence, legislators reasoned that any security measures taken or required in the future should be paid for by the users of the system, i.e., the traveler. In reality, travelers in the long run will determine just how much intrusion they will tolerate and just how much they are willing to pay for it via the legislative process. As a result of the compromise bill passed by Congress in November 2001, passengers can expect to pay the costs of the increased security. After January 2002, taxes and fees for passengers include a security fee of up to $10 per round trip ticket, a 7.5 percent domestic ticket tax, a $3.00 per person per flight segment fee, and a maximum of $18 in airport passenger facility charges. Taxes and fees can amount to 50 percent of the cost of the ticket. Additionally, airlines are required to pay about $4.00 per passenger to the government to cover security screening costs (*Air Transport News*, 16 November 2001).

At the time of the study, annual U.S. air carrier passenger traffic in the domestic system alone rose from 424 million to 523 million (Internet: http://cas.faa.gov/reports/98study/98study.html, pg. 5). The commercial aircraft fleet had risen to 4916 aircraft in 1996. The current aviation security regulations apply to 165 U.S. air carriers, 164 foreign carriers, and numerous freight forwarders. For perspective, during the study (Fiscal Year [FY] 1996), FAA aviation security special agents conducted 6317 U.S. air carrier inspections and 643 foreign air carrier inspections at U.S. airports. They also performed 870 U.S. airport facility inspections, 267 facility security inspections, and 123 foreign airport assessments in addition to 223 random freight-forwarder inspections. The TSA has already assumed this function.

It is indisputable that fairly stringent security measures had been in place for flights departing the United States for many years. As the President directed in July 1996, air carriers are performing preflight security inspections on all international flights, "on every plane, every cabin, every cargo hold, and every time" (Internet: http://cas.faa.gov/reports/98study/98study.html). During the mid-1990s, the FAA and the Office of the Secretary of Transportation worked closely with the National Security Council to refocus federal government attention on the needs to improve airport security. They were also successful in creating the Aviation Security Advisory Committee (ASAC) of the Baseline Working Group (BWG) on 17 July 1996, which has the unfortunate honor of sharing its inception date with the TWA Flight 800 disaster. Unfortunately, as is well documented, the security procedures in place proved insufficient, either because the rules were deficient or the implementation left a great deal to be desired.

CIVIL AVIATION SECURITY

The Federal Aviation Administration's Civil Aviation Security (CAS) Division was tasked with keeping civil aviation safe from terrorist attacks. The mission was to "ensure and promote a secure and safe civil aviation system." Its goal was to be recognized as the world leader in civil aviation, identifying and countering aviation-related threats to U.S. citizens worldwide. The Office of the FAA Associate Administrator for Civil Aviation Security developed and implemented regulatory policies, programs, and procedures to prevent criminal, terrorist, and other disruptive acts against civil aviation.

The organization was divided into two main sections, one handling internal issues and the other tasked to manage external security issues. The internal division had the responsibility for all security-related issues within the agency and included the following programs: internal investigations, drug investigation support, personnel security, industrial security, identification media, physical security, and communications information security. The internal division was responsible for establishing and enforcing regulations, policies, and procedures for all these areas. They were also tasked to identify specific potential threats and establish appropriate countermeasures, deploy federal air marshals on selected U.S. flights, and provide overall guidance to ensure security at airports. FAA personnel monitored and inspected air carrier and airport security and had the authority to assess civil penalties. The "investigations" program was considered an internal affairs division of the FAA and coordinated all matters, which may have involved the misconduct or malfeasance of an employee. In coordination with security specialists assigned to security divisions at each FAA region and center, the unit ensured the agency complied with public laws, national directives, and DOT policies that influenced FAA security practices. The specific overall objective was to create an FAA environment that reduced the risks posed by espionage, sabotage, theft, vandalism, terrorism, and other criminal acts.

CAS special agents constituted an internal police force for the scrutiny of employee involvement in any criminal activity to supervise those that are supposed to be protecting the public. The potential for bribery, extortion, and intimidation of FAA employees by criminals is a constant threat. Organized crime will always pursue FAA employees who may be able to facilitate the introduction of contraband into civil aviation or other criminal activity. FAA employees are not immune from the financial pressures of the world or from the sophisticated and often brutal intimidation methods of drug cartels. Protecting its own assets and policing itself contributes to the maintenance and safety of the entire commercial aviation system. The job is huge and requires constant vigilance.

The drug investigations support program existed to assist and supplement law enforcement personnel in the ongoing efforts to control the gigantic flow of illegal drugs through many U.S. airports. CAS agents sought to assist local, state, and federal law enforcement agents in all cases where civil aviation is involved. They were specially trained and provided law enforcement with additional expertise in aviation-related cases requiring a unique knowledge of carrier operations, both on the ground and in the air. They worked in very close cooperation with U.S. Customs, the Drug Enforcement Agency, and the Federal Bureau of Investigation.

The personnel security program assessed the integrity of new employees. The program is responsible for "background checks" of prospective agency employees. The agency also ensured that designated personnel at air route control centers, terminal radar approach control facilities, and other staffed facilities are properly trained and equipped in security matters. Criminal and financial checks were routine, and military and medical records are also reviewed when appropriate. In conjunction, the industrial security program was tasked with providing security clearances for industry officials and companies that contract with U.S. civil aviation. The program is supposed to ensure that contracting companies maintain the security of sensitive FAA information. The potential for serious security violations is always present when civilian contractors are involved. This program attempted to keep civilian contractors aware of the need to maintain a constant state of security awareness and remain focused. Operational security requirements are often ignored for the sake of

expediency and whenever the concept of profit versus expenses for security come into play. The old adage that "Loose lips sink ships" can be easily forgotten in today's world of mass communications, cell phones, computers, and wireless communications.

The identification media program was assigned the task of developing and controlling all identification materials used by FAA employees. According to the Web site, there are currently no less than 16 different types actively in use. The changes in technology in this field occur frequently, and the ability to counterfeit identification badges is a constant threat. The task of staying on top of changes and improvements is a daunting endeavor and presents some unique challenges. Access control is an essential part of any program, and just staying on top of the changing technology is a task unto itself.

The physical security program is in charge of keeping all FAA assets secure, including both tangible assets and personnel. The property and equipment in use by the FAA is of exceptional value and range from Tactical Air Navigation (TACAN) testing facilities to aircraft. The possibility of loss from theft and sabotage is an ever-present danger, and constant vigilance is mandatory. In addition, the personnel in this program must be able to assess the threat both internally and externally.

The FAA is also a communications intensive organization. The communications security program guarantees that the integrity of the FAA's telecommunications is maintained. This program is also involved in highly technical cryptographic operations to deny unauthorized users access to FAA communications. This particular function is absolutely critical to the safe operation of air traffic control operations and flight operations in general. The FAA also strives to provide effective air traffic control voice and data communications security as well as effective navigation system security, including global positioning systems, or GPSs. Again, the rapid changes in technology make this task a daunting one. Sometimes the "bad guys" have more sophisticated equipment than the "good guys."

Arguably, one of the most important liaisons existed between the FAA and the Office of Intelligence and Security in the Office of the Secretary of Transportation. They coordinated security and intelligence between agencies. Continuing cooperation had been further encouraged by the formation of a DOT Security Working Group under the direction of the Director of the Office of Intelligence and Security. The FAA Office of Intelligence provided intelligence analysis of the threats to civil aviation as the basis for determining the application of aviation security measures. Similar to military intelligence units, the division routinely published synthesized intelligent and threat assessment information. These products were used to evaluate security programs both domestically and internationally. Information was collected from open sources and from U.S. government classified sources.

Information of this type is disseminated to airport operators and airlines by means of documents called "information circulars" and "security directives" as provided for by FAR 108.18 or 14 CFR Sec 108.18. If a specific threat cannot be countered, either the specific flight will be canceled or public notification will be made. When this does occur, airlines are not pleased with the ensuing loss of passengers and profits.

Since 11 September 2001, the FAA's Civil Aviation Security organization has been integrated into the newly founded TSA. President Bush signed the Aviation and Transportation Security Act (ATSA, PL 107-71) on 19 November 2001. It, in part, created the TSA within the DOT. For the first time in history, even though considered as an option a decade earlier, transportation security is being performed and monitored by the federal government. As a direct federal responsibility, an Undersecretary of Transportation Security who will formally report directly to the Secretary of Transportation, will manage the program.

Specifically, the TSA was mandated to operate the passenger-screening process, but its overall mission is broader. It is tasked with analyzing threats that pertain to the entire transportation infrastructure, aviation related and otherwise. The agency's budget for FY 2003 was 4.8 billion U.S. dollars, but the President's Budget for FY 2006 requested 5.3 billion U.S. dollars, which was a net increase of $156 million over the FY 2005-appropriated monies (see Figure 2.4). The revised budget structure

Change from FY 2005 Enacted Appropriations to FY 2006 Request

Program	FY 2005	FY 2006	Change
Aviation security*	$4.57B	$4.98B	$406M
Screener workforce & equipment	[3.75B]	[3.91B]	[160M]
Aviation direction & enforcement	[827M]	[1.07B]	[246M]
Surface transportation security	115M	32M	(83M)
Transportation security support	712M	545M	(167M)
Total	$5.40B	$5.56B	$156M

* FY 2005 and FY 2006 columns include $255M and $250M, respectively, in mandatory authority. FY 2005 reflects enacted amount.

FIGURE 2.4 TSA appropriations to fiscal year 2006. (Source: TSA. www.tsa.gov)

shows major programs and associated costs more clearly, among Aviation Screening Operations, Aviation Security Regulation and Enforcement, and Transportation Security Enterprise.

Later, Senate Bill No. 509, introduced in the 110th Congress, would extend and reauthorize certain federal programs related to aviation security that are primarily implemented by the TSA within the Department of Homeland Security (DHS). The Congressional Budget Office (CBO) estimates that implementing the legislation would result in new discretionary spending of 6.8 billion U.S. dollars over the 2008 to 2012 period, assuming appropriation of the necessary amounts. In addition, S. 509 would affect direct spending by authorizing TSA to collect, over the 2008 to 2028 period, 250 million U.S. dollars annually in fees from airline passengers and spend those amounts to improve security measures at airports. CBO estimates that such fees would initially exceed spending, resulting in a net reduction in direct spending of $225 million in 2008 and $500 million over the next ten years. Those savings would eventually be fully offset by corresponding increases in direct spending after the agency's authority to collect fees expires in 2028, resulting in no net change in direct spending over the long run.

The TSA assumed all passenger and carry-on baggage screening by 19 November 2002, replacing contract personnel with federal employees at most of the nation's commercial airports. Additionally, all major airports were operationally using explosive detection equipment to accomplish 100 percent screening of all passenger cargo by the end of December 2002. At the time, airports and airlines again indicated that total compliance with the mandate was unfeasible. Like the 1970s, airports were scrambling to comply. The equipment was very expensive, and sufficient numbers of them still needed to be manufactured.

The agency also selected new security managers for the nation's major airports. Unfortunately, they seem to be hiring individuals with impressive backgrounds but with little day-to-day aviation security experience. How successful these people continue to be is critical to the security of the entire aviation transportation network.

AVIATION SECURITY RESEARCH AND DEVELOPMENT DIVISION

The Aviation Security Research and Development Division, previously within the FAA, was created to conduct research and development programs related to civil aviation security. It was created as early as 1974 and has accomplished a great deal. The goal was to develop and implement equipment designed to counteract criminal and terrorist attacks against civil aviation. The division is technology oriented and is divided into four interrelated sections: Explosives and Weapons Detection, Aircraft Hardening, Human Factors, and Airport Security Technology Integration.

The Division continues to promote research and development, especially in the area of detection of explosives and weapons and their placement on board aircraft and inside airports. Other programs are focused on automated aviation security systems for the screening of both passengers and cargo that provide for the highest throughput in the least intrusive manner. Still other programs are directed at methods to harden aircraft to mitigate the damaging effects of bombs, weapons, missiles, and electromagnetic interference. Detection and deterrence are the ultimate goals, and they are achieved by developing systems that address all potential vulnerabilities at the airport, pertaining to passengers and cargo, and at air traffic control facilities.

COSTS

Since the 1970s, the federal government has proffered the argument that the costs related to aviation security are just another cost of business for the airlines. In the years when hijacking seemed to be a constant and everyday threat, the airlines were less reluctant to argue with the government over who should bear these expenses. However, for quite a long time, the airlines had engaged in an extensive lobbying campaign for an expansion of a federal security force to pick up the responsibilities legislated to the airlines. The government had repeatedly refused to accept accountability for this type of security despite making sweeping declarations regarding terrorism and the nation's airways as constituting a vital national interest. In a bold statement, Senator Lautenberg, a member of the President's Commission on Aviation Security and Terrorism, stated in a speech on 1 August 1996:

> "Congress, our nation's airlines, and our airports have been unwilling to make the investments necessary to protect the public. Terrorism is an act of war against an entire nation, with civilians on the tragic front lines, and we have got to confront it with the same commitment and fervor that we must reserve for other threats to our national security." (Senate Floor, 1 August 1996) His words seem hauntingly prophetic.

The concept of the nation's airways as a national asset and consequently a national security issue had been made for quite some time. However, without the constant threat of imminent hijackings, the public was not inclined to add the expense of adequate airport and airline security to federal budget requirements. This is particularly true in light of the level of the current federal debt. Because the threat of acts of domestic terrorism at U.S. airports did not appear real to most Americans until 11 September 2001, they were highly disinclined to pay for current needs, let alone future requirements. The White House Commission, as early as 1996 in its final report, went so far as to say, "The federal government should consider aviation security as a national security issue, and provide substantial funding for capital improvements. The Commission believes that terrorist attacks on civil aviation are directed at the United States, and that there should be an on-going federal commitment to reducing the threats they pose. (Final report to President Clinton, Internet: http://cas.faa.gov/reports/Whc97rpt.htm).

Despite all the rhetoric, not enough resources were committed in time to prevent the 11 September tragedy. Renewed posturing has forced the U.S. government to readdress the issue. Concerns over the proficiency of airport screeners and who should pay their salaries and training have now been addressed in P.L. 107-71. Time will only tell how this plays out in the future, but the increasing costs will have to be shared by the aviation industry, the traveling public, and the federal government.

WHITE HOUSE COMMISSION ON AVIATION SAFETY AND SECURITY —THE DEPARTMENT OF TRANSPORTATION STATUS REPORT

During the 1990s, the White House did take an active role in investigating ways to improve security for travelers at all transportation hubs. As mentioned, much debate was exchanged and bantered back and forth on the appropriate policy positions that the U.S. government should take. For example, should the government consider aviation security as a national security issue? If the government should reach this conclusion, it would follow that they should also subsequently provide substantial funding for capital improvements to the aviation industry infrastructure.

It was also suggested that the FAA should establish federally mandated standards for security enhancements for such concepts as explosive detection. The Aviation Security Improvement Act of 1990 (P.L. 101-604) mentioned above states that prior to a requirement for a deployment of explosives detection systems (EDSs), the FAA must certify that EDS performance meets standards based on the amount and types of explosives likely to be used to cause catastrophic damage to commercial aircraft. In 1992, the FAA issued the draft EDS standard, and the National Academy of Sciences completed the final protocols a little less than a year later. In December 1994, the *Invision* CTX-5000™ became certified as the first explosive detection system approved by the FAA.

The Commission also reflected on the persistent problems pertaining to screening the U.S. mail. Security experts had recommended that the U.S. Postal Service (USPS) should advise customers that all packages weighing over one pound should be subject to examination for explosives if they are to be moved by air. The USPS initially responded negatively to the obligation and suggested that the procedure would impede the postal service's ability to provide timely, reliable low-cost mail service. The USPS was also concerned whether or not the public would accept further intrusion on the privacy of mail, let alone routine intrusion. The USPS's Aviation Mail Security Committee continued to debate these issues.

In 1997, based on advice from the Aviation Security Advisory Committee Baseline Working Group, the White House report also reviewed the issue of needed improvements in the area of cargo security. Consequently, on 14 May 1997, the FAA proposed amendments to standard security programs for U.S. carriers, couriers, freight forwarders, and cargo consolidators, as well as a model security program for foreign air carriers. The whole issue of cargo acceptance and handling procedures has been discussed on numerous occasions with lots of input from numerous sources being considered. Regardless, according to many experts, cargo continues to present a major vulnerability (White House Commission on Aviation Safety and Security, the DOT Status Report, 2001).

AVIATION AND TRANSPORTATION SECURITY ACT—P.L. 107–71

As stated, President Bush signed into law the ATSA in an effort to improve the nation's transportation security system. The Act is intended to fundamentally change the way security is performed and overseen as regards the entire transportation industry. The Act contains some specific deadlines for its new administrators. One such deadline was to issue new qualification standards for airport screeners. On 31 December 2001, Secretary Norman Mineta, U.S. Secretary for Transportation at the time, announced the new, but very similar to the already mandated, requirements for federal airport screeners. They included the need for U.S. citizenship, possession of a high school education or equivalent, the ability to pass a background and security investigation, including a criminal records check, and the necessity of passing a standardized examination. The standards have proven problematic.

Resorting back to the private sector for assistance, the TSA and FAA also published training plans for the new aviation security personnel, meeting the Congressional mandate of doing so within 60 days of the Act. The TSA hoped to also meet the deadline of 19 November 2002 to deploy 30,000 trained screeners at over 400 airports and has since claimed to have done so. The challenge is a daunting one, and they have run up against the same problems encountered by the private security firms originally doing the job. The TSA planned to do the following:

- Screen all persons, baggage, and cargo
- Provide stress management conflict resolution programs
- Implement policies for professional interaction with passengers

The agency had previously issued requests for proposals (RFPs) devoted to screener and law enforcement personnel qualification, recruitment, experience, and screener training. They sought to develop an appropriate training regimen including a minimum of 40 hours of instruction. As a first step, as of 30 April 2002, 200 federal employees were deployed at Baltimore Washington Airport marking the initiation of the program.

The airlines also were required, within 60 days, to amend their training programs to incorporate the TSA standards. All airline personnel, particularly aircrews, must receive the training within six months from enactment of the new legislation. The agency also published the procedures for airports to seek portions of the 1.5 billion U.S. dollars authorized by Congress to fund security improvements at airports.

IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007 (H.R. 110-1, P. L. NO:110-53)

In short, the Implementing Recommendations of the 9/11 Commission Act of 2007 provides for realization of the recommendations of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission). Signed by President Bush on August 3, 2007, this law requires screening of all cargo on passenger planes within three years and sets a five-year goal for scanning all container ships for nuclear devices before they leave foreign ports. The legislation also authorizes more than 4 billion U.S. dollars over four years for rail, transit, and bus security; establishes a new electronic travel authorization system to improve security for visitors from countries participating in the visa waiver program; strengthens privacy and civil liberties protections; requires the President and Congress to disclose total spending requested and approved for the intelligence community; provides civil immunity to those who in good faith report suspicious activities that threaten the safety and security of passengers on a transportation system or that could be acts of terrorism; and requires the President to confirm that Pakistan is making progress combating al'Qaeda and Taliban elements within its borders before the United States provides aid to that country (GovTrack.us. H.R. 1--110th Congress, 2007). The bill also calls for a larger percentage of homeland security grants to be given to states most at risk, creates a grant program for emergency communications at the DHS, mandates that the DHS conduct vulnerability assessments of U.S. infrastructure every year, and requires the DHS to create an initiative to enhance emergency preparedness efforts in the private sector. Furthermore, additional funding would be provided "to support United States foreign policy objectives during a crisis abroad," and sanctions would be imposed on individuals and countries in an effort to crack down on the black market for nuclear technology.

THE NATIONAL STRATEGY FOR AVIATION SECURITY

The White House, March 26, 2007.

The strategy recognizes the events of September 11 and the Heathrow plot of August 2006, as well as the fact that the economic prosperity of the world is dependent on a secure aviation system. Simply put, the Secretary of Homeland Security, based on NSPD-47 and Presidential Directive 16 was placed in charge of operational implementation of the strategy. The directive charged the Secretary with integrating public and private efforts to detect, deter, prevent, and defeat threats to global aviation as well as coordinate efforts to reduce vulnerabilities and expedite recovery from any future event. The strategy is supposed to incorporate the basic principles of risk management and layered approaches to security.

Seven supporting plans are to be developed to address the specific threats and challenges identified in NSPD-47/HSPD-16.

The supporting plans include an Aviation Transportation System Security Plan, Aviation Transportation System Recovery Plan, Air Domain Surveillance and Intelligence Integration Plan, International Aviation Threat Reduction Plan, Domestic Outreach Plan, and International Outreach Plan. Work continues on the plan.

SECURITY GUIDELINES FOR GENERAL AVIATION AIRPORTS

Transportation Security Administration, May 17, 2004

In an attempt to provide greater consistency of local security requirements for airport owners and tenants and aircraft operators, these guidelines were designed to establish nonregulatory standards for general aviation airport security and to help prevent the unauthorized use of a general aviation aircraft in an act of terrorism against the United States. The specifics are contained in government phamphlet A-001. The mandates contained in A-001 represent a far cry from the security checks legislatively required for commercial airlines. Some members of Congress, however, advocate that small private planes and similar type of aircraft in the general aviation community be more rigorously inspected.

At a Senate Commerce, Science, and Transportation Committee hearing in 2007, Senator Jay Rockefeller (D–WV), postulated that about three quarters of flights within the United States fall into the general aviation category. Rockefeller used the example of former New York Yankees pitcher Cory Lidle, who in October 2006 was killed when his small plane drifted off course and hit a Manhattan highrise, to remind TSA Chief Kip Hawley that even single engine planes can cause significant damage. Rockefeller suggested that the agency bolster its staff so it can devote more resources to general aviation. Hawley responded that TSA is "looking at steps" to improve its general aviation tactics and indicated that "a more robust plan" was being considered. It must be recognized, however, that Cory Lidle's small airplane did little damage in comparison to the effects a large commercial airliner would cause (Internet:http://www.govexec.com /story.page.cfm?articleid =35883&dcn=to daysnews).

CONCLUSION

The need to develop aircraft and airport security functions became readily apparent in the early 1970s. Various jurisdictions took various approaches to counter the threat. In the United States, the Federal Aviation Regulations Parts 107 and 108 specifically addressed these issues. Those regulations were differentiated based on the size of the aircraft and the size of the airport. The public was somewhat slow to recognize the requirement to bypass individual 4th Amendment rights, and controversy still surrounds airport screening procedures. Additionally, specific incidents of abuse catch the media's attention and bring the issues to the forefront.

The TSA seeks to provide, in its own words, "excellence in public service." It hopes to protect the nation's transportation infrastructure and to ensure freedom of movement of people and commerce. It took 30 years for the nation to recognize and to implement federal control of security at airports. It remains to be seen how effective administration of the system becomes under long-term federal supervision. The TSA faces incredible challenges and has been criticized heavily. The responsibility is almost too massive to imagine, and critics will be quick to jump on the slightest infraction or outright failure. Additionally, bureaucracies tend to perpetuate themselves, often to the detriment of the agency's original mandate. The public's attention span is also quite short, especially if they perceive that the threat has dissipated. A return to apathy is a major problem. Just as important a problem occurs when a democracy goes too far in the name of security. Fundamental constitutional freedoms still need ever vigilance to protect and preserve. It is a very slippery slope to forget the

democratic principles on which this nation was founded — all in the name of perceived external or internal threats. The next chapter will cover international attempts to address the problems.

A new national aviation security plan has helped to consolidate efforts to increase protection of the entire aviation network and to become realistic regarding the cost effectiveness of existing programs and the initiation of new ones. The plan seeks to utilize the aspects of risk asset management after the government came to the realization that there simply are not enough available resources to engage every security protocol available or proposed. One hundred percent security will never be achieved, and hard decisions need to be made to determine what protection devices and procedures are the most workable and can be budgeted and implemented. Risk management must determine potential adversaries, critical assets, levels of threat, and appropriate countermeasures, all within a cost effect matrix.

REFERENCES

Air Transport News, 16 November 2001.
Anderson, Theresa, "Airport Security," *Security Management,* pp. 73-74, February 2000.
Associated Press, Jet Hijackings Decline but Still a Threat, 1 Jan 2000.
Aviation Daily, 202:42, 11 July 1972.
Aviation Daily, 205:114, 14 January 1973.
Aviation Daily, 205:267, 10 February 1973.
Aviation Daily, 205:233, 13 February 1973.
Aviation Daily, 205:319, 28 February 1973.
Brennan, Frank, "Anti-hijacking: Who Pays the Bill?" *Chicago Daily News*, 23 Feb 1973.
Federal Aviation Administration, Criminal Acts Against Civil Aviation, Appendix F, 1996, pg. 79.
Federal Register 37:2500, Docket 11432.
Federal Register, 37:4904, 7 March 1972.
Federal Register, 37:5689, 5691, 18 March 1972.
Final report to President Clinton, http://cas.faa.gov/reports/Whc97rpt.htm, Sec 3.1, pg. 20.
GovTrack.us. H.R. 1--110th Congress, 2007: Implementing Recommendations of the 9/11 Commission Act of 2007, *GovTrack.us (database of federal legislation),* http://www.govtrack.us/congress/bill.xpd?bill=h110-1., accessed Jan 19, 2008.
http://www.aclu.org/congress/airtest.htm. pg. 2, March 3, 2001.
http://cas.faa.gov/reports/pl101604/pl101604.html.
http://cas.faa.gov/reports/98study/98study.html, pg. 5.
http://cas.faa.gov/reports/98study/98study.html. pg. 6.
http://www.govexec.com /story.page.cfm?articleid =35883&dcn=todaysnews.
Senator Lautenberg, Senate Floor, 1 Aug 1996.
U.S. Department of Transportation, Federal Aviation Administration, Office of Civil Aviation Security, Criminal Acts Against Civil Aviation, available at http://cas.faa.gov/crimacts/pf/crim2000.pdf, as of Feb. 8, 2002.
White House Commission on Aviation Safety and Security the DOT Status Report, (http://cas.faa.gov/reports/Whc98s1.htm, 1 May 2001.

3 International Solutions and Reactions

NEWS

11 August 1982: Mohammed Rashed plants a bomb on Pan American Flight 830. It explodes just a few minutes before the plane lands in Honolulu. The bombing investigation links the attack to Saddam Hussein. Rashid is charged under the Montreal Convention and stands trial in Athens, Greece.

19 January 2001: Abdel Basset Ali-al-Megrahi and Lamen Khalifa Fhimah are brought to trial in the Netherlands, plead not guilty to prosecutors' claims that they planted a plastic explosive on board the airliner, which blew up 01 December 1988 over Lockerbie, Scotland. On 01 March, a three-judge Scottish Court finds Abdel Basset Ali al-Megrahi guilty of murder, based on more than eight months of trial. He is given a mandatory sentence of life imprisonment. The court also concludes that prosecutors failed to present sufficient evidence to meet the burden of "proof beyond a reasonable doubt" in the case against Lamen Khalifa Fhimah.

26 November 2002: Richard Reid, is indicted in October 2003 of attempting to smuggle a bomb concealed in his shoe on board an American Airlines flight departing from Paris. He is a small-time British convict who converted to Islam while incarcerated. Authorities find plastic explosives with a triacetone triperoxide (TATP) detonator hidden in the lining of his shoes. On 30 January 2003, he is found guilty of terrorism charges at a federal court in Boston, MA and is sentenced to life in prison.

29 July 2005: Three of the four suicide bombers who carried out botched attacks on three trains and a bus on July 21 in London are captured alive. Italian authorities then announce that Bomber No. 4 is in custody. Britain asks for his extradition, and the Italians comply. Prime Minister Tony Blair announces new deportation measures against those who foster hatred and advocate violence, as his government continues to try to counter Islamic extremists born in Britain.

January 2008: After a three-month trial and a seven-day sentencing hearing, José Padilla, the Brooklyn-born convert to Islam whom the government once accused of plotting to detonate a "dirty bomb" in the United States, is sentenced to 17 years and 4 months in prison for his role in a conspiracy to help Islamic jihadist fighters abroad. The case began with his arrest in May 2002 at O'Hare airport in Chicago, after which Attorney General John Ashcroft announces that Mr. Padilla was part of an "unfolding terrorist plot to attack the United States" by exploding a radioactive dirty bomb intended to cause "mass death and injury." He is identified as an "enemy combatant" and held without charge.

CRIMES AGAINST HUMANITY

Of course, terrorism and the aircraft hijacking problem are not limited to the United States. Recently, there have been two trends in international terrorism. The actual number of incidents has been decreasing, but the lethality of incidents has been increasing. After reaching a peak in 1987, the number of international terrorist incidents overall has been declining, according to statistics collected by the U.S. State Department. For example, in 1992 the State Department recorded 364 terrorist incidents worldwide, down from 666 reported in 1987. A number of cooperative international efforts have been accomplished to assist in reducing the threat worldwide. However, as noted previously, the real level of effectiveness of some of these treaties is regrettably low. Depending on the circumstances and despite the original good intentions of the drafters and signatories, many treaties have done little to curtail the scourge.

Clearly, in general the problem of hijacking and "terrorist or criminal acts" against aviation is not the enigma of a single nation. It pervades many peoples and many nations and cannot be effectively opposed by one nation alone. Consequently, multilateral action by the international community has resulted in the drafting and implementation of several treaties. Combined, these treaties have met with some success and at least forced the international community to jointly recognize a global problem.

The term "crimes against humanity" popularized after World War II at the Nuremberg trials did not originate in the context of the laws of war but with laws used in peacetime. Centuries before, the term had been used to describe acts of piracy. Sir Edward Coke, an English jurist during the reign of James I, described pirates as hostis humanis generis. The Latin term is generally translated as common enemies of mankind (Friedlander, 1979)

Early U.S. case law substantiates the concept of piracy as an international crime. In 1820, the Supreme Court in United States versus Smith, (18 US 5 Wheat. pg.71) determined that piracy was "an offense against the law of nations" and referred to pirates as enemies of the human race. The concept was affirmed in the World Court in the famous Lotus case (PCIJ Series A, 1927). Piracy at sea and piracy in the air have historically been treated in a similar manner although not exactly the same. It took centuries to codify the law of the sea, and piracy at sea is clearly universally accepted as an international crime.

On the other hand, air piracy has received sporadic intensive attention, usually after some weighty tragedy. Three major and several minor agreements on aircraft hijacking have been signed and utilized to combat terrorism. They have met with varying degrees of success. Three main challenges to each convention revolve around determining exactly which nation has jurisdiction, defining the prosecutable offenses, and establishing effective procedures for extradition. A collateral but important goal is to somehow force or encourage nations to actually enforce the treaties they have committed to uphold.

The following section identifies the major terrorism conventions and protocols and provides a brief summary of each. In addition, other international agreements are relevant but are outside the scope of this text. They include bilateral extradition treaties, the 1961 Vienna Convention on Diplomatic Relations, the 1963 Vienna Convention on Consular Relations, and a number of related United Nations Security Council and General Assembly Resolutions. Any reference list on terrorism or aviation-related terrorism should minimally include the following:

- 1963 Tokyo Convention on Offenses and Certain Other Acts Committed on Board Aircraft
- 1970 Hague Convention for the Unlawful Seizure of Aircraft
- 1971 Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation
- 1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents

- 1979 Convention Against the Taking of Hostages
- 1979 Convention on the Physical Protection of Nuclear Material
- 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (supplements the 1971 Montreal Convention)
- 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection
- 1997 Convention for the Suppression of Terrorist Bombings, signed by the United States on January 12, 1998, submitted to the Senate for advice and consent to ratification on September 8, 1999
- 1999 Convention for the Suppression of the Financing of Terrorism signed by the United States on January 10, 2000 and submitted to the Senate for advice and consent to ratification on October 12, 2000

THE TOKYO CONVENTION

One of the first international aviation agreements was drafted and ratified as early as 14 September 1963 and applies to acts affecting in-flight safety. In essence, the treaty authorizes the aircraft commander to impose reasonable measures, including restraint when necessary, to protect the safety of the aircraft. This treaty recognizes the inviolability of a hijacked aircraft and passengers, regardless of where the aircraft may be forced to land. The signatories to the convention ultimately agreed that, in the event of a hijacking, the country where the aircraft lands must permit the aircraft, passengers, crew, and cargo to proceed to its destination as soon as practical. Precisely, the *Convention on Offenses and Certain Other Acts Committed on Board Aircraft,* or Tokyo Convention of September 1963, contained provisions detailing a commitment by the signatory nations to take custody of the alleged perpetrators of criminal acts aboard aircraft and expedite the continued journey of the aircraft, crew, and its passengers. P.L. 91- 449 realized the law in the United States, but the treaty was also signed into law in 122 other countries.

The treaty made an attempt to define some jurisdictional sore points between nations. Exactly who has legal authority to exercise control in any given situation is often disputed. Obviously, the hijacking of an aircraft is a criminal act that usually takes place enroute between more than one country. On top of that, the aircraft may well be registered to a third country. Therefore, Article 3 of the Convention provides that the state of registration has primary jurisdiction. However, a significant loophole was inadvertently legislated. The treaty failed to force that nation that had jurisdiction to actually prosecute the offenders. Therefore, a nation could accept jurisdiction and simply neglect to prosecute. Later conventions sought to remedy this situation, but nations that stubbornly intended not to prosecute continued to do so.

Another recognized shortcoming of the Convention revolves around a second jurisdictional issue. In legalese, the fact that aircraft in flight are legally regarded as part of the territory of the state of registration of the aircraft, the state where the aircraft lands will treat offenses committed on board during the flight as committed on foreign territory unless it is the state of registration of the aircraft. In cases of piracy, this created heated jurisdictional disputes. For example, in cases of passenger misconduct not rising to the level of a hijacking, minor offenses will usually not be investigated or prosecuted at all. Basically, the Tokyo Convention obligates the contracting states to establish jurisdiction over offenses and crimes only when committed on board aircraft of its own nationality. In essence, a jurisdictional gap exists when it comes to less serious crimes and creates at least concurrent jurisdiction in others.

HIJACKING CONVENTION: CONVENTION FOR THE SUPPRESSION OF UNLAWFUL SEIZURE OF AIRCRAFT

Due to the increased incidents of seizure of aircraft in the late 1960s, many concerned nations met in 1970 at The Hague, Netherlands, for another discussion of the persistent problem. As a result, the Convention for the Suppression of Unlawful Seizure of Aircraft was completed on 16 December 1970. The terms of the Convention became effective 30 days after ratification by the tenth country. With the acceptance of the treaty by the U.S. Senate, ratification in the United States was completed on 14 September 1971 and proclaimed by the President on 18 October 1971 (PL 93-366). The Convention entered into force on 14 October 1971.

Overall, this agreement sought to tackle the difficult issues of extradition and prosecution of offenders neglected in the earlier Tokyo Convention. The main provision requires that every signatory state in which a hijacker is discovered must either extradite the offender to the State whose aircraft is hijacked or prosecute the hijacker; potentially subjecting them to severe penalties. Problems have been encountered even among nations willing to take a strong stand against terrorism. For example, some nations vehemently opposed to the death penalty will not extradite terrorists to the United States on moral grounds. The convictions and sentences of the perpetrators of the Lockerbie disaster are a perfect example.

Theoretically, the signatory states must also provide "severe penalties" for the criminal offense of hijacking. As is common regarding international treaties, the exact interpretations of certain specific clauses in this treaty are also controversial. What the term "severe penalties" precisely means to one nation might not seem so to another. Other interpretations are also open to dispute. For example, the trial of two suspected Libyan terrorists, both former intelligence officers who were accused of bombing Pan American Flight 103 over Scotland created much debate over the sufficiency of the findings of the court. As previously mentioned, both individuals were eventually tried in the Netherlands where the death penalty is illegal. One individual was actually acquitted, and the other received a life sentence much to the disappointment of many of the surviving relatives and legal observers in the United States. However, the ability of one country to get another country to do what it wants has been a thorny diplomatic issue for centuries.

The Treaty definitively requires that each nation make the offense of unlawful seizure of an aircraft a crime. Article 1 offers a definition of the actions that may constitute the offense of hijacking. Specifically, Article 1 states that any person commits an offense who, on board an aircraft in flight, does one of the following:

- Unlawfully, by force or threat thereof, or by any other means of intimidation, seizes or exercises control of that aircraft, or attempts to perform any such act
- Performs as an accomplice of a person who performs or attempts to perform any such acts

The Convention also revisited the issue of jurisdiction, simply providing that the notion that the state of registration had primary jurisdiction was not working. Delegates decided a system of concurrent jurisdiction might be more effective, and just such a system was formalized. Three states were legally given the responsibility for jurisdiction in a specific order of precedence (Article 1):

1. The state of registration
2. The state of first landing
3. The state in which the lessee has its principal place of business or permanent residence

In more legalese, the Convention mandated that each contracting state take steps to actually establish jurisdiction, if the offender is within its territory and will not be extradited. The intention of the change was to force the signatories to accept jurisdiction and actually take action once a crime has been committed.

The Convention also sought to toughen up language requiring states to consistently prosecute. The language obligates each state to either extradite or submit the case, "without exception whatsoever to its competent authorities for the purpose of prosecution." Many countries were uncomfortable with the language, viewing it as an infringement of sovereignty. Therefore, the Convention did not go so far as to create an absolute obligation to extradite, but it came as close as possible without several countries refusing to sign. It also requires parties to assist each other in connection with criminal proceedings brought under the Convention.

MONTREAL CONVENTION

The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, the third major treaty, entered into force on 26 January 1973. It is also known as the Montreal Convention of September 1971 or the "Sabotage Convention" and applies to acts of aviation sabotage such as bombings aboard aircraft in flight. The specific legislation in the United States gives effect to the earlier Hijacking Convention by providing the President with authority to suspend air service to any country that he determines is encouraging hijacking in opposition to the Hijacking Convention. The law orders the government to provide regulations requiring that detection devices screen all air carrier passengers and carry-on baggage. Also, it requires a federal air transportation security force to be stationed at major airports under the auspices of the FAA. Basically, the convention provides for the precise applications of the overall principles of The Hague Convention to all crimes committed on board commercial aircraft. For example, the treaty (Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 1971) defines acts that are criminally punishable as:

- Acts of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft
- Destruction of an aircraft in service or damage to such an aircraft that renders it incapable of flight or that is likely to endanger its safety in flight
- Placing or causing to be placed on an aircraft in service, by any means whatsoever, a device or substance that is likely to destroy that aircraft, or to cause damage to it that is likely to endanger its safety in flight
- Destruction or damage of air navigation facilities or interference with their operation, if any such act is likely to endanger the safety of the aircraft in flight
- Communication of information that is known to be false, thereby endangering the safety of the aircraft in flight

This particular treaty also mandated that all signatory parties agree to take all practicable measures to prevent the commission of these offenses. This concept has been unevenly implemented depending on the interpretation of the language in the treaty and the financial resources of the host country. It unequivocally mandates the apprehension and prosecution or extradition of aircraft saboteurs and provides for severe penalties for the perpetrators of these crimes. It also dictated that the 128-party signatory nations engage in all practical efforts to prevent hijacking and to forewarn other nations when it had reason to believe a crime might take place within their jurisdiction. Such cooperative efforts are well intentioned but often difficult to effectuate.

THE CONVENTION ON THE PREVENTION AND PUNISHMENT OF CRIMES AGAINST INTERNATIONALLY PROTECTED PERSONS

On 14 December 1973, the United Nations supplemented the *Tokyo Convention* upon recommendation of the 24th Session of the International Law Commission. The Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, including diplomatic agents,

requires each signatory to criminalize the intentional murder, kidnapping, or other attack on the person or property of an internationally protected person. It specifically outlawed attacks on senior government officials and diplomats and also made it a crime to engage in violent attacks on official premises, private accommodations, or the means of transport of such person. Generally, the treaty was offered and supported in response to the activities of the Irish Republican Army (IRA) in the United Kingdom. The commission had been actively studying the question of the protection and inviolability of diplomatic agents and other persons entitled to special protection under international law. The British wanted to have international approval of legal measures taken against suspected IRA members, and this treaty was clearly supportive (U.N. Resolution 3166).

BONN AGREEMENT 1978

Prime Minister Pierre Trudeau of Canada pressed for even more sanctions in the form of a joint declaration against rogue nations. Another effort, the Bonn Agreement of 1978, was thereupon signed by the heads of state of Britain, Canada, France, West Germany, Italy, Japan, and the United States. Corresponding legislatures never ratified this agreement, but the endeavor exhibited an attempt by the leading democratic nations to jointly tighten efforts to combat aviation-related terrorism. An article by the Washington Post dated 18 July 1978 described the agreement as an effort by "the Heads of State and government, concerned over terrorism and hostage taking, to declare that their governments will intensify their common undertaking to fight international terrorism" (Getler, 1978). This effort was the first wherein several nations banded together to arrange to mutually agree that in cases where a rogue country refused to extradite or legally prosecute hijackers or give back aircraft, the respective governments unanimously agreed to take immediate action to cease all flights to that country. Alternatively, incoming flights from the offending country were also to be banned. In a collateral move, the United States urged that the Bonn declaration adopt an annex declaring that all signatories halt air carrier service to nations where attacks on airports and airline offices went unpunished.

Deplorably, except for some saber rattling toward South Africa for offering refuge to the mercenaries who attempted to overthrow the government of the Seychelles and a collective suspension of service to Afghanistan for its failure to prosecute suspected hijackers, the Bonn Agreement has never been collectively used. This is unfortunate in that the concept provided a significant economic tool to combat air piracy.*

Senior Vice President and General Counsel of the Air Transport Association, James E. Landry, suggested the following measures in the United States during a speech to the National Forum Foundation's Conference on Terrorism and Transportation on 12 May 1986. Although his comments fell on deaf ears, he reasoned that additional measures were necessary and recommended the following:

- Expand the scope of the Bonn Declaration to encompass acts other than hijackings.
- Establish the means to monitor incidents to assure proper and timely actions are pursued in other countries.
- Refine and expand appropriate sanctions.
- Collaborate with such organizations as International Civil Aviation Organization (ICAO) for promulgating international security standards, drawing on their expertise to improve countermeasures.

* *Note*: In 1973 after numerous attempts to hijack U.S. carrier aircraft to Cuba, U.S. and Cuban authorities correspondingly and respectively agreed that hijackers were to be "returned to the party of registry of the aircraft or vessel or be brought before the courts of the party whose territory he reached for trial." The Agreement had also stated that Cuba was to facilitate, "without delay the continuation of the journey of the passengers and crew innocent of the hijacking." The Cuban government retracted the agreement a mere four years later. Despite the denunciation of the agreement by Cuba in 1976, there had been a rather substantial record of cooperation between the two countries.

- Authorize and provide resources for ICAO to evaluate the extent and methods of states in applying the Security Standards and Recommended Practices.
- Convene a subsequent sanctions conference.

The Bonn Conference, which was part of a G-7 Summit in July 1978, attempted to encourage the major powers to halt bilateral air traffic with countries that refused to extradite and prosecute hijackers. Essentially it failed. As stated, the agreement was effectively invoked only once in 1982 when Britain, West Germany, and France terminated all air traffic with Afghanistan (Pilgram, 1990). The issue of terrorism is discussed routinely at these conferences. In a collateral treaty during the same time frame, the language of the International Convention Against the Taking of Hostages, signed in New York on 18 December 1979, provided that any person who seizes and detains and threatens to kill, to injure, or to continue to detain another person is subject to the law. Therefore, any person committing an act of hostage-taking was supposed to be either prosecuted or extradited under international law. However, these documents in reality generally achieve little more than the usual condemnation of terrorism and pledge to cooperate.

INTERNATIONAL CONVENTION AGAINST THE TAKING OF HOSTAGES

The international community firmly recognized that the taking of hostages was an offense of grave concern that required that any person committing an act of hostage-taking should either be prosecuted or extradited. They believed it was urgently necessary to develop international cooperation between states in devising and adopting effective measures for the prevention, prosecution, and punishment of all acts of taking of hostages as manifestations of international terrorism (General Assembly Resolution 146, 1983).

Specifically, the Hostages' Convention provides that, "any person who seizes or detains and threatens to kill, to injure, or to continue to detain another person … in order to compel a third party, namely, a State, an international intergovernmental organization, a natural or juridical person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage commits the offence of taking of hostages …" (Article 1.) Furthermore, Article 3 arguably expressly gives the state whose citizen was taken hostage carte blanche to do what is necessary to recover such hostages. (Internet: http://www.unodc.org/unodc/terrorism_convention_hostages.html).

In the United States, Senate Bill 2623, the "Aircraft Sabotage Act" implemented the 1972 Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation. The bill imposed federal penalties for sabotaging civilian aircraft and for endangering civilian aircraft. As previously mentioned, over 100 countries, including the United States and the Union of Soviet Socialists Republic signed the convention. Furthermore, S. 2624, ratified the "Act for the Prevention and Punishment of the Crime of Hostage-Taking, which implemented the International Convention against the Taking of Hostages, a United Nations General Assembly resolution adopted in December 1979, after the U.S. Embassy in Iran was seized. The bill provided for U.S jurisdiction and federal penalties for hostage-taking and extortion of diplomats if the offense was committed in the United States, if the offender or victim is a U.S. national, or if the offender was present in the United States. Senate Bill 2625, an act for "Rewards for Information Concerning Terrorist Acts" established federal rewards for up to $500,000 for persons who provide information leading to the arrest or conviction of individuals who had committed or were considering committing terrorist acts against U.S. persons or property or which may lead to the prevention, frustration, or favorable resolution of a terrorist act against U.S. persons or property. S. 2626, the "Act for the Prohibition against the Training or Support of Terrorist Organizations," also made it a federal offense for a U.S. national, resident alien, or U.S. business to "act in concert with or provide training or support services to recruit or solicit for foreign governments, factions, or international terrorist groups if such actions and services specifically are banned by the Secretary of State."

TOKYO SUMMIT 1986

In May 1986, seven major democracies completed the Tokyo Summit on International Terrorism. In part, they were responding to the misuse of diplomatic privileges by some "rogue nations." The Tokyo Summit attempted to close another loophole in the international maze of international law. Signatories each committed to "make maximum efforts to fight against the scourge." The conference developed the following guidelines, jointly believing that the commission of such crimes is a matter of grave concern to the international community:

- Refuse to export arms to rogue states that sponsor or support terrorism.
- Strictly limit the size of diplomatic missions and other official bodies abroad of rogue states that engage in terrorist activities and to control the travel of members of such, missions and bodies. Close, where appropriate, or make radical reductions in such missions and bodies.
- Deny entry to all persons, including diplomatic personnel, who are suspected of terrorist activities or who have been convicted of a terrorist offense.
- Improve extradition procedures using domestic laws to expeditiously bring to trial those individuals who have perpetrated acts of terrorism.
- Employ stricter immigration and visa requirements with respect to nationals of rogue states that support or sponsor terrorism.
- Improve bilateral and multilateral law enforcement efforts.

In Tokyo the global economic situation continued to remain positive, which allowed the leaders to focus on the "hot" political issues of the time including terrorism and the Chernobyl nuclear disaster. There had been many high-profile terrorist incidents since Bonn, some of which had prompted the U.S. bombing raid of Libya in April 1986. In addition, the Chernobyl accident had occurred only one week prior to the summit. After long hours of negotiation, the participants reached an accord that called for concrete measures to improve cooperation in fighting terrorism. Unfortunately, these recommendations were not immediately acted on. It would take more tragic incidents to get the United States and other nations to more fully cooperate with each other and to improve collective response plans to such incidents.

FURTHER EFFORTS

By 1973, it was clear that the combined treaties had still not stopped the steady stream of hijackings. Taken collectively, the three major treaties should have ensured the safety of internationally registered aircraft, but unfortunately did not. In reality, some countries still simply refused to extradite. Others only imposed slight penalties for crimes "generally-considered" serious offenses by a host of other nations. Still others, like Libya, actually offered a safe haven to terrorists perceived to share a commonly held political persuasion. Some critics also recognized that some signatories had signed the treaties for only political reasons and never had any intention of respecting the spirit of the international law developed. In reality there are no sanctions or enforcement procedures in any of the three treaties. Actual enforcement of any particular treaty has been a problem and will remain so. In essence, they are "gentlemen's agreements" dependent on enforcement on the integrity of each signatory nation. Efforts were made during the ICAO Extraordinary Assembly in September 1973 to achieve some enforcement consensus, but it ended in failure. Furthermore, a proposal to convene another multinational convention creating an international commission with the authority to investigate alleged violations of the three major treaties and to enforce sanctions never came about.

In addition, although well-intentioned, the treaties current at the time still contained some loopholes. For example, they failed to cover procedures relating to airports and ticket offices. Terrorists who chose to simply assault and murder people in the airport terminal did not fall under the treaties,

but instead local law. Consequently, after terrorist attacks at the Rome and Vienna airports in 1987, the Montreal Protocol of 1988 was signed. This additional and additive document provided the means for procedures for handling acts of violence of all civil aviation facilities to include airports and ticket offices and will be discussed later.

MONTREAL PROTOCOL OF 1988

The US Senate ratified the protocol on 21 April 1988. In general it seeks to expand the original treaty to address the safety of passengers in airports and terminals. Article I of the Montreal Convention Treaty is amended in Article II of the 1988 Protocol as follows:

1. In Article 1 of the Convention, the following shall be added as a new paragraph. Any person commits an offense if he unlawfully and intentionally, using any device, substance, or weapon: (a) performs an act of violence against a person at an airport serving international civil aviation that causes or is likely to cause serious injury or death; or (b) destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport, if such an act endangers or is likely to endanger safety at that airport.
2. In paragraph 2(a) of Article 1 of the Convention, the following words shall be inserted after the words "paragraph 1" (Article II, Montreal Protocol of 1988) Signatories also must concurrently establish jurisdiction over these offenses.

DIPLOMATIC CONFERENCE ON AIR LAW 1991

One effort to more easily identify explosives utilizes the concept of taggants. It has proven highly effective while showing how the efforts of ICAO can be an effective means of initiating international aviation cooperation. On 12 January 1990, a subcommittee of ICAO drafted a treaty to require the addition of taggants to explosives manufactured by contracting states. Taggants are additives to explosives that make them easily visible to various scanners. Essentially, the taggants make explosives detectable by use of gas analysis procedures, which are readily available on the market. Taggants can be either chemical or physical compounds. They individually identify explosive devices by manufacturer, lot number, and type. Physical taggants are plastic, metal or ceramic tags directly attached to the device. On 2 April 1990, the United States actively participated in a meeting of the full legal committee of ICAO dealing with this issue. The committee presented the proposed treaty at the full convention in early 1991. The convention accepted the new international treaty on the Marking of Plastic Explosives for the Purpose of Detection in March of the same year.

The treaty was designed to control and limit the use of unmarked and undetectable plastic explosives. Generally speaking, the treaty requires each party to take necessary and effective measures to prohibit and prevent the manufacture of unmarked plastic explosives. Signatories are also expected to prevent the movement of unmarked plastic explosives into or out of their territories and to exercise strict and effective control over possession and transfer of unmarked explosives. The treaty also mandated that all stocks of unmarked explosives, not in possession of the police or the military, be destroyed or marked within three years.

CONVENTION ON THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL 1980

Ten years earlier, the Convention on the Physical Protection of Nuclear Material was signed on 3 March 1980. It required each party to take appropriate steps within the framework of its national law to ensure as far as practicable that during international transportation, nuclear material within its territory is protected to certain minimal levels defined in the Act. Unfortunately, every nuclear nation has unaccounted for nuclear material, including the United States.

G-7 SUMMIT 1995

This conference, held in June 1995, followed on the heels of the bombing at Oklahoma City and the subway gas attack in Tokyo. Summit members pledged to instruct a task force of terrorism experts to report on the best methods of combating terrorism in an offensive mode as opposed to defensive (*Dow Jones International News Service*, 1995). One year later in Lyon, members again addressed the issue of terrorism. This time the conference took place in the wake of the bombing on the U.S. military installation in Saudi Arabia and an IRA bombing in Manchester, England.

LYON SUMMIT 1996

At a conference held in Lyon, France, in 1996, the world's security ministers once again met to discuss international cooperation in fighting terrorism. They were quick to acknowledge the effectiveness of military and spy satellites in tracking down terrorists but recognized the need for even more cooperation between nations and their respective law enforcement and security agencies. The ministers ultimately agreed on approximately 25 measures to further enhance efforts to track down and bring known terrorists to justice.

The group agreed that each nation could improve its counterterrorism cooperation and capabilities. They concluded that nations will have to accelerate the research and development of methods to adequately detect explosives and other harmful substances. In keeping with new laws in the United States, other nations need to investigate organizations and groups that purport to be charitable organizations but in reality serve as a cover for terrorist organizations collecting money for their causes. The government felt these groups must be targeted and outlawed, thereby shutting down a source of legal revenue for terrorist endeavors. The conference noted that many nations still have laws that make it legal to export weapons and explosives without any controls. Export control laws need to be reformed as well as antiterror legislation to give them more teeth.

An important issue discussed was that of political asylum. The conference encouraged countries to ensure that the rights and freedoms of their nation are not taken advantage of by terrorists who seek to plan and finance terrorist activities within their borders. As always, the exchange of information was also considered crucial to the success of antiterrorist cooperative efforts. Direct exchange of information was encouraged with the realization that most intelligence agencies and national law enforcement agencies are hesitant to release such information. The conference identified the information that explicitly needs to be shared. It included:

- The actions and movements of known terrorists
- The discovery of forged travel documents
- Information relating to explosives and arms trafficking
- Detection of the use of state-of-the-art communications technologies by terrorists
- Any information relating to the possible use of weapons of mass destruction including nuclear, chemical, and biological weapons

It is clear that it has been known for decades what needs to be done to prevent the proliferation of terrorism; it is just extremely difficult and challenging to actually have the reforms come about on an international scale.

MINISTERIAL CONFERENCE ON TERRORISM 1996

On 30 July 1996, the leaders of the major world powers announced cooperative action against terrorism. They hoped to tighten security to prevent terrorist activity before it happened. They wanted to make it easier to identify terrorist suspects. The conference adopted a 25 point antiterrorism plan. The plan included coordinated airline security measures, curbs on terrorist fund-

raising, better exchange of intelligence, policing the Internet, setting global standards for detecting bombs, improving extradition arrangements, outlawing possession of biological weapons, drafting a treaty requiring countries to try suspected bombers or extradite them, and tightening border checks (Nichols and McCormick, 1996). The conference overall was a bit of a defeat for U.S. leadership in policymaking. The Europeans and Japanese representatives strongly criticized U.S. support of economic sanctions against countries such as Iran and Libya. U.S. opponents were responding to U.S. action penalizing countries that had traded with Cuba and believed that it was better to target the terrorist group rather than alienating the host country. The European Union has repeatedly objected to the United States penalizing non-U.S. companies in pursuit of U.S. foreign policy goals.

CONVENTION FOR THE SUPPRESSION OF TERRORIST BOMBINGS 1997

The Convention for the Suppression of Terrorist Bombings entered into force on 23 May 2001 and was implemented under the Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002. It sought to create a regime of universal jurisdiction over the unlawful and intentional use of explosives and other lethal devices in, into, or against various defined public places, with intent to kill or cause serious bodily injury, or with intent to cause extensive destruction of the public place. It sought to deny "safe havens" to persons wanted for terrorist bombings by obligating each state party to prosecute such persons if it does not extradite them to another state that has issued an extradition request. In general, this particular convention imposes binding legal obligations upon states' parties either to submit for prosecution or to extradite any person within their jurisdiction who commits an offense as defined in Article 2, attempts to commit such an act, participates as an accomplice, organizes or directs others to commit such an offense, or in any other way contributes to the commission of an offense by a group of persons acting with a common purpose.

INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM 1999

In 1999, in a further effort to combat terrorism, the International Convention for the Suppression of the Financing of Terrorism was drafted. It requires the parties to take all necessary steps to prevent and counteract the financing of terrorists. These preventive efforts are meant to encompass not just those groups that are openly terrorist in nature, both also other more innocuous groups as well. The treaty covers all groups supporting terrorist efforts, whether directly or indirectly, even groups claiming to have just charitable or cultural goals. The treaty also covers groups that also engage in such illicit activities as drug trafficking or arms dealing to finance their terrorist pursuits. In addition to holding those who finance terrorism accountable, the treaty provides for the identification, freezing, and seizure of funds allocated for terrorist activities. Bank secrecy is no longer an acceptable excuse for refusing to cooperate even though it has been tolerated for years.

UNITED NATIONS

Of course, the United Nations has repeatedly condemned terrorist activities. The Security Council, as the principal international organ dealing with international peace and security, has since its inception been involved in the verbal fight against terrorism. Immediately after the 11 September attack on New York City and Washington, D.C., in its resolution 1368 (2001) (http://www.un.org/Docs/scres/2001/res1368e.pdf), it condemned the terrorist attack against the United States and called on all states to work together urgently to bring the perpetrators to justice. With resolution 1333 (2000), it demanded that Afghanistan's Taliban authorities act swiftly to close all camps where terrorists were trained. With resolution 1269 (1999), it unequivocally condemned all acts of terrorism as criminal and unjustifiable, and called on member states to adopt specific measures. With resolution

FIGURE 3.1 The United Nations Security Council voted on a six-month extension of the U.N.humanitarian program in Iraq in U.N. Headquarters. The U.N. has repeatedly intervened in countries that act as sources of terrorism in efforts to combat the roots of terrorism, both in the Middle East and around the world. (Source: United Nations)

1267 (1999), it demanded that the Taliban turn over Usama bin Laden to appropriate authorities so that he can be brought to justice (see Figure 3.1).

Reflecting similar views, The General Assembly on the day of the attack strongly condemned the heinous acts of terrorism, and called for urgent action to enhance international cooperation to prevent and eradicate acts of terrorism (http://www.un.org/documents/ga/docs/56/agresolution.htm). Earlier, after a series of terrorist acts worldwide, the General Assembly unanimously passed a resolution with the following aspects (Henkin et al., 1993):

- Unequivocally condemns, as criminals, all acts, methods, and practices of terrorism wherever and by whomever committed, including those that jeopardize friendly relations among states and their security
- Appeals to all states that have not yet done so to consider becoming party to the existing international conventions relating to various aspects of international terrorism
- Calls upon all states to fulfill their obligations under international law to refrain from organizing, instigating, assisting, or participating in terrorist acts in other states, or acquiescing in activities within their territories directed toward the commission of such acts

Previously, the Security Council had adopted a resolution in December 1985 condemning all acts of hostage-taking and abduction. They also agreed that all states are obligated to prevent such acts. In 1996, the General Assembly readdressed the issue of terrorism. In the Declaration on Measures to Eliminate International Terrorism (General Assembly Resolution 49/60, 1994) they resolved:

States must fulfill their obligations under the Charter of the United Nations and other provisions of international law with respect to combating terrorism and are urged to take effective and resolute measures, in particular:

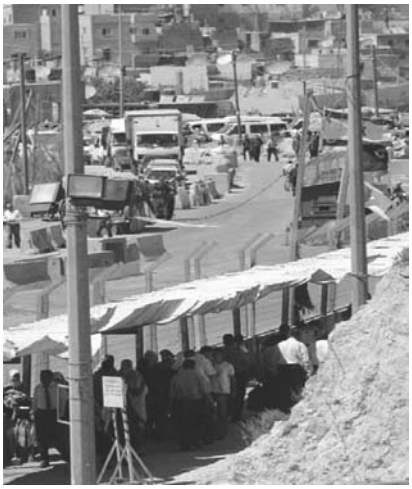

FIGURE 3.2 At the Kalandia checkpoint in the West Bank, Palestinians await entry to Jerusalem. The U.N. has passed several anti-terrorist measures but lacks enforcement capability. The U.N. recognized the Palestinian Liberation Organization with observer status in order to facilitate discussion with the Israeli government and to take note of the Palestinian refugee issue. (UN Photo #UNE15. Source: United Nations)

a. To refrain from organizing, facilitating, financing, or tolerating terrorist activities
b. To ensure the apprehension and prosecution or extradition of perpetrators of terrorist acts
c. To cooperate with one another in exchanging relevant information
d. To take appropriate measures, before granting asylum, for the purpose of ensuring that the asylum seeker has not engaged in terrorist activities

Basically, all the resolutions and declarations made by the United Nations are focused on nation states implementing the provisions of treaties already in existence. The United Nations is attempting to get those countries to actually enforce them or to sign them in the first place. The United Nations has no real enforcement powers of its own, however; they can be a powerful force in the area of delicate international maneuvering (see Figure 3.2).

On 26 October 2001, the United Nations published the requirements that all of its 189 members must now follow when combating terrorism on their own soil. Member states that fail to follow the guidelines will be subject to sanctions under Resolution 1373, which was passed by the Security Council on 28 September 2001. Under the guidelines, all states must demonstrate the legislative and executive measures they have taken to combat terrorism. Specifically, each state must show their law enforcement agencies are making efforts to freeze the assets of terrorists and take appropriate action to punish the supporters or terrorists. Furthermore, the United Nations is asking that countries document their procedures to ensure that terrorists do not seek refuge on their soil and document how they intend to prevent future terrorist attacks. One U.N. diplomat (Hoyos, 2001) has been quoted as saying, "It's a steady raising of the bar."

THE INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO) AND THE EUROPEAN CIVIL AVIATION CONFERENCE

All countries are individually responsible for implementing effective aviation security systems. Because terrorism is an international issue and can affect several nations within the time span of a few hours, nations have banned together to establish standard procedures. Efforts to work out

international civil aviation agreements were first made in Europe at about the same time the Wright Brothers made their historic flight at Kitty Hawke. However, it was not until 1944 that any significant progress was made. In November 1944, over 50 nations met in Chicago to examine the problems of international civil aviation. The result was the Convention on International Civil Aviation. The preamble of the convention stipulates that the ratifying governments have "…agreed on certain principles and arrangements in order that international civil aviation may be developed in a safe and orderly manner and that international air transportation services may be established on the basis of equality of opportunity and operated soundly and economically" (ICAO, 07/12/1944, pp.13-17).

In less than 24 months, the required numbers of nations signed the convention on 4 April 1947, and ICAO was created. It replaced the temporary organization set up in 1944. ICAO has two main elements: the Assembly, which is the policy-making body, and the Council, a governing body, which is responsible to the Assembly. A 27-member council provides overall direction to the organization. The Air Navigation Commission, the Air Transport Committee, and the Committee on Joint Support of Air Navigation Services and a Finance Committee supplement their efforts.

One of ICAO's main duties is to adopt international standards and recommendations and to incorporate them into the convention as annexes. Annex 17 deals directly with airport security standards. No legal action can realistically be brought against violators of the association rules, but if a country does not obey the rules, airliners from that state may be denied landing and other services. Regardless of the success of ICAO and Annex 17 precautions, soon after the Annex was adapted by a majority of nations, there were 31 hijackings in 1978, 27 in 1979, and 40 hijackings in 1980.

The European Civil Aviation Conference (ECAC) is an international organization that works with various governments to develop measures, standards, and recommended practices solely within Europe. It operates with the active support of ICAO. It has been in operation for many years and has three basic principles that sum up the current status of the mutual agreements (Panghorn, 1996):

- That the threat of unlawful interference with civil aviation in its many forms of violence is likely to persist
- That ICAO standards and recommended practices in aviation security have to take into account the widely varying provisions available for their implementation in more than 180 participating countries
- Mutual understanding and close and constant cooperation between all state authorities concerned are necessary to achieve and maintain a high standard of aviation security.

POST JULY 2005 BRITISH LEGISLATION

Britain's existing antiterrorism laws are among the strongest in Europe, but many British strongly believed that they needed to be strengthened further following the London terrorist attacks. There are two main pieces of antiterrorism legislation on the British statute books: the Terrorism Act of 2000 and the Anti-Terrorism Crime and Security Act 2001, which was amended in 2005. Over 700 suspected terrorists have been arrested in the United Kingdom since September 11, 2001; of which just 119 were charged. Just 17 terrorist suspects had been convicted under the Terrorism Act between 2001 and 2005, of which only three were Islamic militants.

However, on 7 July 2005, a series of four bomb attacks struck London's public transport system during the morning rush hour. Three bombs exploded within 50 seconds of each other on three London Underground trains. A fourth bomb exploded on a bus in Tavistock Square. The bombings led to a severe, day-long disruption of the city's transport and mobile telecommunications infrastructure. Fifty-six people were killed in the attacks, including the four suspected bombers, with approximately 700 injured. Police investigators identified four suicide bombers who conducted the suicide bombings thought to have been planned by Islamist paramilitary organizations based in the United Kingdom, possibly affiliated with al-Q'aeda. The bombings came while the United Kingdom was hosting the first full day of the 31st G-8 Summit, a day after London was chosen to

host the 2012 Summer Olympics, two days after the beginning of the trial of fundamentalist cleric Abu Hamza, five days after the Live 8 concert was held there, and shortly after Britain had assumed the rotating presidency of the Council of the European Union.

On 21 July 2005, a second series of four explosions took place on the London Underground and a London bus. However, this time only the detonators of the bombs exploded, and all four bombs remained undetonated. There were no fatalities. All suspected bombers from this failed attack have been arrested by police. In response to this series of events, Britain finalized proposals to deport or bar foreign Islamic radicals. Charles Clarke, the British home secretary, published a catalog of terrorism-related offenses to bar or deport foreign militants accused of fomenting hatred, violence, and extremism.

The British government will now deport and ban people who "foment, justify, or glorify terrorist violence." Clarke said a list of "unacceptable behaviors" includes the use of Web sites, writing, preaching, publishing, or distributing materials that "seek to provoke others to terrorist acts" or "foster hatred." Specifically, Britain barred radical Muslim cleric Omar Bakri from returning to the United Kingdom, saying his presence was no longer "conducive to the public good." The decision came as the country's top legal official defended plans to deport another radical Muslim cleric and nine other foreigners suspected of posing a threat to national security. As a signatory to the European Convention on Human Rights, Britain is not allowed to deport people to countries where they may face torture of mistreatment. Therefore, the government has been trying to sign agreements guaranteeing humane treatment of deportees with 10 countries, including Algeria, Lebanon, Egypt, and Tunisia. The first such memorandum of understanding was signed with Jordan.

INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF ACTS OF NUCLEAR TERRORISM

The convention adopts the approach taken in many previous antiterrorism treaties. It requires state parties to make certain acts criminal offenses in national law, establish jurisdiction over such offenses, prosecute or extradite persons alleged to have committed the defined criminal offenses, and engage in cooperation and mutual legal assistance with respect to objectives of the convention. The frequent use and familiarity of this approach helped the negotiations make progress, but questions exist about the adequacy of this strategy for counteracting nuclear terrorism. The convention addresses the unlawful possession or use of nuclear devices or materials by nonstate actors. It calls for states to develop appropriate legal frameworks criminalizing nuclear terrorism-related offenses, investigate alleged offenses, and, as appropriate, arrest, prosecute, or extradite offenders. It also calls for international cooperation with nuclear terrorism investigations and prosecutions, through information-sharing, extradition, and the transfer of detainees to assist with foreign investigations and prosecutions. With its focus on the investigation and prosecution of individuals, the Nuclear Terrorism Convention also addresses to a limited extent the treatment of detainees (http://www.un.int/usa/a-59-766.pdf).

The Nuclear Terrorism Convention is the first antiterrorism convention adopted since the attacks of 11 September 2001 (see Figure 3.3). The treaty opened for signature 14 September 2005 and entered into force 30 days after it was signed and ratified by at least 22 states. The United States has welcomed the treaty, which could dovetail with the Bush administration's evolving neomultilateralism, characterized by international cooperation among sovereign states, manifested by parallel or joint action toward common goals on a domestic or international level, accompanied by corresponding developments in treaty-based and U.N.-based international law. Consistent with past expressions of Bush policy such as the promotion of the Proliferation Security Initiative, the Nuclear Terrorism Convention does not emphasize the role of international bureaucracies, in contrast to, for example, the International Criminal Court (ICC). At the same time, the Nuclear Terrorism Convention does envision detainee reports in some instances being made to, or through, the U.N. Secretary General.

FIGURE 3.3 The aftermath of 9/11 shocked the world and encouraged many governments to enact stricter anti-terrorism laws. Shown is here a photograph of the World Trade Center following the terrorist attacks.

The Convention gives security a high priority; grounds security in law, including international law; is UN-centered; and is sovereignty-based, calling for international cooperation among independent sovereigns joined in a common cause and acting together or in parallel as sovereign partners. The Nuclear Terrorism Convention speaks to values and themes previously articulated and include:

- Outlawing and condemning terrorist activities and demonstrating global unity in opposition to terrorism
- Treating terrorism as a matter subject to domestic and international law challenging states to use, and if necessary adapt, their domestic legal systems to combat terrorism
- Looking to states to cooperate as sovereign partners in the fight against terrorism, doing so within the context of domestic legal actions, as well as through related international mechanisms such as sovereign-to-sovereign extradition (but, as mentioned above, not by utilizing a free-standing international bureaucracy like the ICC, differences over which have contributed to transatlantic friction)
- Nevertheless using the United Nations as an international forum to develop interstate cooperation, as a gathering place for sovereign partners
- Using international law as a basis and framework for action, and using the United Nations as a forum for developing international law
- Doing so by means of sovereign states voluntarily entering into an agreed international legal framework, through formal treaty-making, voluntarily accepting obligations to take action as independent sovereign states, and manifesting compliance with their treaty-based obligations in parallel through domestic legislation
- Including within this purview statements of the rights of detainees

CONCLUSION

International treaties including the Tokyo, Hague, and Montreal conventions all remain hallmarks of international efforts to combat terrorism. Unfortunately, years of cooperation have proved that once the treaties are in effect, they often fail to be effective. Nations react depending on the attitude of each nation, all of whom can still exercise their own sovereignty over suspected terrorists, regardless of the language in the existing treaties. One of the newest undertakings involves the attempt to track terrorists by following the money trail. After 11 September 2001, cooperative efforts in the financial realm are critical to the success of the ongoing "War on Terrorism." Terrorist operations are expensive, the money has to come from somewhere, and it moves along with the operators. The trail the money leaves is the best way to document who the actual perpetrators were and how they organized the attack. Similar patterns of financing can be monitored to hopefully prevent future attacks.

Efforts will likely continue to fine-tune the treaties as the need arises. However, enforcement, as always, will remain a problem. Even recent efforts by the United Nations to "raise the bar" for its member states recognize that efforts to combat terrorism will suffer from an inability to enforce any sanctions levied against violators of the guidelines. A silver lining to the tragic events of 11 September, however, is the renewed attention of the global community for the need to actively pursue the perpetrators of terrorism jointly. Hopefully, the enthusiasm to stop terrorism at an international level will not turn to verbal apathy again but will remain active.

REFERENCES

Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed in Montreal on September 23, 1971.

Friedlander, Robert, *Terrorism: Documents of International and Local Control*; Dobbs Ferry, NJ: Oceana, 1979, pg. 18.

G-7 Summit Chechnya War: *Dow Jones International News Service*, 17 June 1995.

General Assembly Resolution 146 (XXXIV), United Nations GAOR, 34th Sess., Supp. No. 46, at 245, U.N. Doc. A/34/46, 1979; *entered into force* June 3, 1983.

General Assembly Resolution 49/60. UNGAOR 6th Comm. 84th meeting, UN Document A/49/743, 1994.

Getler, Michael, "Move to Combat Air Piracy is Viewed as Toughest Yet", *Washington Post*, 18 July 1978, pg. A1.

Henkin, Louis, et al, *International Law: Cases and Materials*, 3rd ed., 1993, West Publishing Co., St. Paul, MN. pg 392.

Hoyos, Carola, "UN Sets out rules for states battling terrorism", *Financial Times*, 28 October 2001, pg. 3.

ICAO, 07/12/1949, pp.13-17, http://www.icao.int/icaonet/dcs/7300.html.

http://www.unodc.org/unodc/terrorism_convention_hostages.html.

http://www.un.org/documents/ga/docs/56/agresolution.htm.

http://www.un.org/Docs/scres/2001/res1368e.pdf.

http://www.un.int/usa/a-59-766.pdf.

Nichols, Bill and Jay McCormick, "Anti-Terror Action Slows; Plan Outlined in Paris," *USA Today*, 31 July 1996, p. 1A.

Panghorn, Alan, "How Far Has Europe Come Since Pan Am 103?" *Intersec*, Three Bridges Publishing, London, 5 May 1996, Vol. 6, pg. 195.

PCIJ Series A, No. 10, 2 Hudson World Court Rep 20, 1927.

Pilgram, Caleb M., "Terrorism in National and International Law," 8 *Dickinson Journal of International Law 147*, 198, 1990.

4 Growth and Change
Aircraft As Missiles

NEWS

30 May 2001: CNN announces that an Algerian terrorist, arrested after he attempted to smuggle explosives into the United States in December 1999, admits he intended to blow up the Los Angeles International Airport.

6 August 2001: The CIA briefs President Bush that al'Qaeda operatives might try to hijack U.S. aircraft.

10 August 2001: Phoenix FBI agent writes letter noting that Middle Eastern men are attending flight schools and that bin Laden may have sent them. The memo proposes a nationwide canvass of flight schools.

11 September 2001: American Airlines Flight 11 crashes into the North Tower of the World Trade Center, United Airlines Flight 175 crashes into the South Tower, and American Airlines Flight 77 crashes into the Pentagon.

April 2002: About 130,000 former law enforcement officers, federal agents, and general citizens have applied to become federal air marshals since 11 September 2001 when the government began advertising the jobs.

17 August 2005: CNN conducts an interview with Col. Tony Shaffer, the DIA liaison officer to the Able Danger operation who has gone public to tell what he knows about the identification of Mohammed Atta as an al'Qaeda terrorist more than a year before 11 September. Able Danger, created in 1999, used open source "data mining" technology to identify and track terrorists. A year later, Atta and his fellow jihadists—Khalid al-Mihdhar, Marwan al-Shehhi, and Nawar al-Hamzi—carry out the 11 September attacks.

EARLY CRIMINAL HIJACKINGS

One of the earliest known acts of air piracy or skyjacking occurred in 1930, when hijackers took over a Peruvian aircraft. The incident received little attention and never resulted in any international efforts to combat a potential threat to international aviation. In fact, some authorities, depending on their own political viewpoints, actually praised some hijackers based on purely political sympathies even in the West. To illustrate, numerous individuals that attempted to escape across the Iron Curtain were welcomed with open arms by Western European governments. Any attempt to flee perceived Soviet oppression was accepted as legal and praiseworthy conduct. Of course, the attempts were not viewed from the Eastern bloc countries with the same perspective. Similarly, support for air piracy continues from rogue countries supportive of terrorism in the Middle East and elsewhere. The terrorists are received as heroes in the fight against perceived Western tyranny and past repressive colonialism.

From 1930 to 1967, only 12 U.S. commercial aircraft hijackings were attempted, and only 7 were semi-successful. However, in 1968 a deluge of hijackings began to plague the nation. Many

Americans traveling in the Caribbean were repeatedly detoured to Havana, Cuba. Of the 22 hijackings in 1968, 19 were directed to fly to Cuba. By 1969, the number of U.S. passengers and crew members that made the Cuban detour totaled 1359 Americans, and the airlines that often suffered the financial loss of the aircraft, were increasingly agitated. Something clearly had to be done. It was merely too easy to board an aircraft and commandeer it. As is often the case, there are two sides to every story. Many nations and specific groups perceived hijackings as permissible expressions of political viewpoints warranting their support. Some of these nations continue to attempt to ignore the criminality of such conduct.

There have been hijackings of general aviation aircraft as well. In 1962, two individuals kidnapped at gunpoint the pilot of a private Cessna 172 and compelled him to transport them from Florida to Cuba. The perpetrators were charged with commission of "aircraft piracy" in violation of a 1961 Amendment to Section 902 of the Federal Aviation Act of 1958 (49 USC Supp. IV Section 1472 I). As used in this subsection, the term aircraft piracy was defined as "any seizure or exercise of control, by force or violence or threat of force or violence and with wrongful intent, of an aircraft in flight in air commerce." The defense argued that a private plane was not an aircraft in flight in air commerce. The lower court initially held for the defendants and dismissed the indictments; however, the Supreme Court disagreed (United States versus Healy*, 376 U.S. 75, 1964*). They reasoned that the phrase "an aircraft" is on its face an all-inclusive term. They went on to express the opinion that Section 902 (l) of the amended act (49 USC Supp. IV Sec 1472 [l]) made it a crime to carry a concealed weapon "while on board an aircraft being operated by an air carrier in air transportation." By that language the court concluded that Congress knew how to choose words to solely refer to commercial airlines when it wanted to do so.

At the other end of the Cuba hijackings, although not really sympathetic to the plight of the passengers, crew, or airline (usually Eastern Airlines), the Cuban authorities were not really hospitable to the hijackers either. They made no distinction between large aircraft and small aircraft hijackings. Considering the political realities between the governments of Cuba and the United States, little cooperation between the two initially took place. However, the hijackers were not welcomed with victory parades. An armed reception committee generally greeted the hijackers, and they could expect months of interrogation and harsh imprisonment. Furthermore, the interrogation and imprisonment were often under severely brutal conditions. Almost all the hijackers were kept under close arrest despite their professed Cuban sympathies and later often expressed extreme disillusionment with their chosen refuge.

Worsening the problem for the United States, Fidel Castro initiated the Mariel Boatlift in April 1980. Castro had decided to empty his prisons and mental hospitals and literally export them to the United States. He hoped to relieve his own government of the obligation to support them. Approximately, 125,000 refugees, mostly those convicted of crimes or who were mentally unstable, eventually made it to U.S. territory, often under extreme hardship. Many individuals, however, were not pleased with their forced change in homelands and sought to return to Cuba by any means possible. The boatlift consequently prompted a series of "homesick hijackings," especially at Christmastime. The emotional drive to return to family and friends was unexpectedly great. The problem was so distinct and created such a nuisance that the situation reached a point where the Federal Aviation Administration (FAA) even put commercials on TV in Florida, warning would-be hijackers that Castro's response to hijacking was jail and not "*Feliz Navidad.*" These initial "emotional" hijackings were the prelude to more severe terrorist activities to come.

TERRORIST HIJACKINGS SPREAD

The early 1970s saw a continuing series of aircraft hijackings. In a coordinated effort, on 6 September 1970, a terrorist group hijacked Trans World Airlines Flight 707 on a scheduled flight from Frankfurt to New York. The flight was full, carrying 145 passengers plus the crew. The group seized the plane over Belgium and ordered the pilot to fly to Jordan. On the same day, Palestinian

guerillas also hijacked a SwissAir DC-8 flight outbound from Zurich and a Pan American 747 aircraft out of Amsterdam. A SwissAir DC-8 aircraft was commandeered over France and also ordered to fly to Dawson Field in Jordan. The Pan American flight turned out to be an afterthought. Earlier, the terrorists made an attempt to hijack an El Al flight enroute from Tel Aviv to Amsterdam. The original hijack team, including Leila Khaled, Patrick Arguello, and a third Arab initiated a violent conflict when the pilot refused their demands. One flight attendant was shot, and an Israeli sky marshal managed to kill one of the hijackers. The other two hijackers were subdued and eventually flown to London. Left off the original plane, the remaining members of the team hijacked the Pan American flight.

Three days later a BOAC VC-10 was hijacked; completing the series. The Pan American flight was directed to Beirut and Cairo where the plane was eventually destroyed. The other aircraft were forced to fly to Zarca in the Jordanian desert by members of the Popular Front for the Liberation of Palestine (PFLP). The nearly 500 passengers and crew suffered six days of terrible confinement inside the plane. The remaining three planes were blown up in full view of media cameras. This was the first extensively televised terrorist hijacking. Terrorists had discovered the media. Some reports of the incident even claim the terrorists prepositioned the cameras. After more than 20 days of negotiations, the Jordanian army freed the last of the hostages, while the seven political prisoners that the hijackers demanded be released were in fact released. The highjackers had also demanded the release of three members of the PFLP in a Swiss jail, other terrorists being held in West Germany, and the release of Leila Khaled in London. The British, with Prime Minister Edward Health at the helm, were in turmoil over the events. The hijacked BOAC V-10 aircraft had 110 British citizens on board. The British capitulated and released Khaled but vowed never to submit to terrorism again.

Hijacking an aircraft greatly appealed to extortionists and terrorists with a cause that they sought to publicize. The incidents were accomplished to achieve both political and personal gains and were successfully used as a dramatic method of attempting to enforce demands. The sensationalism of an aircraft being blown up or captive hostages huddled in an aircraft cabin was an assured draw for the cameras. In addition, the Palestinians wanted to send a statement to the Egyptian government. They wished to express displeasure with Egypt's participation in a Middle Eastern peace plan.

The U.S. government's response to the threat was swift but not totally effective. Initially, the government response, publicly announced by President Richard Nixon, proposed the placement of "specially trained, armed U.S. government personnel on flights of U.S. commercial airliners." In reality, the placement on all "threatened" aircraft was unattainable. It simply was not possible to put an agent on every flight. On top of that, the costs were prohibitive, and the airlines balked at the "freeloaders" on board. His administration's plan also called for the use of electronic screening equipment at airports and urged the Department of Transportation (DOT), Department of Defense, (DOD), Department of Treasury, CIA, and FBI to accelerate present efforts to develop security measures. Research and development in the field of access control, explosive detection, and screening equipment began to proliferate.

INITIAL PUBLIC RESPONSES

Initially, much was written and debated as to how best to deal with the growing problem. Suggestions ranged from the reasonable to the bizarre. The public was even asked to forward suggestions to authorities in the hopes of canvassing methods, which would have broad-based public appeal. One unique proposal opined that the planes should be equipped with a sleeping gas that would be pumped into the cabin in the event of an attempted hijack. Thankfully, cooler heads prevailed and the Joint Airline–Government Task Force, commissioned at the time to analyze possible solutions, warned that a gas strong enough to disable hijackers could cause the death of passengers with certain chronic diseases. Such a method was not feasible or even reliable and was quickly discarded.

Any and all ideas were considered. Some of the more unusual examples now appear humorous. For instance, one suggestion involved the use of a hypodermic needle filled with a poison or drug,

which would be installed in each airline seat. Should a hijacker or hijackers seek to take over an airborne aircraft, the pilot could activate the mechanism and disable the perpetrators. How this was to work if the terrorists were standing up when they seized the aircraft was unclear. Regardless, the idea appealed to some, but the potential liability associated with misuse or accidental use soon caused the rejection of such an idea. The potential for inadvertent use on regular passengers, of course, also doomed this idea from the beginning.

Another humorous, although impractical, proposition suggested that all passengers strip down naked prior to flight. Each passenger would then be required to wear an issued flight suit, thereby supposedly eliminating the ability of a passenger to smuggle a weapon or explosive device onto the aircraft on their person. The issue of discovering dangerous weapons potentially hidden in body orifices was never addressed. Again the concept of changing clothes fell into disfavor.

By far the author's favorite and most hilarious idea was proffered on the former sitcom "All in the Family". The family patriarch, Archie, believed that each passenger should be issued a gun, thus enabling the entire plane of passengers to deal with the bad guys. As much as this sounds pretty far-fetched, the concept of passengers becoming involved in subduing terrorists or simply unruly passengers is an issue worthy of discussion. The idea of life imitating art has unfortunately occurred. The concept of passenger involvement in the subduing of unruly passengers was later to have some significant negative repercussions when fellow passengers inadvertently killed a passenger in an attempt to control him. The overtaking of the hijackers of United Airlines Flight 93, which crashed into the Pennsylvania countryside on 11 September 2001, reflects a positive example of passenger involvement. But such "cooperation" by passengers is not really to be encouraged except under extreme circumstances.

COCKPIT DOORS

Another more serious proposal argued for the development of an inaccessible bulletproof pilot's compartment. Initially, the Airline Pilot's Association came out in favor of the inaccessible cockpit, but the FAA came to concur with the reasoning that a bulletproof cockpit would be vulnerable to hostage threats. No pilot would realistically let a passenger be sacrificed by refusing to open the cockpit door. Even though today access to the cockpit is supposed to be accessible only to the crew, terrorists and unruly passengers have not found it particularly difficult to successfully overcome this obstacle. In the early years, there were neither really good answers nor appropriate alternatives in a hostage scenario for the pilot. It is still important to consider the dilemma to pilots when a hijacker screams, "open the door or I'll kill ten of the passengers every ten minutes until you do." However, terrorist tactics changed in 2001. Denying terrorist's access to the cockpit to fly the plane themselves and use it as a weapon introduced a completely different potential scenario. The Israeli airlines (El Al) have had secure cockpits for years, and the requirement for denied access has become standard law in the United States in response to this new twist (see Figure 4.1).

The U.S. government, since 11 September, decided to force all aircraft flying through its airspace to make flightdeck doors virtually impenetrable. On 15 January, the FAA published new standards for flightdeck doors to protect airline and cargo crews from intrusion and small arms fire or fragmentation devices. The regulations require the doors to be resistant -to force, small arms fire, and hand grenades. In January 2002, the FAA gave U.S. airlines only 45 days to strengthen the locking devices on current doors. A deadline of April 2003 was set to make all cockpit doors bulletproof and resistant to explosives. The rules also apply to the more than 500 international carriers that provide service in and out of the United States. Beginning on 9 October 2001, the FAA issued a series of regulations that allowed near-term door reinforcement (Internet: http://www.faa.gov /avr/arm/nprm.cfm).

Overseas, the International Civil Aviation Organization (ICAO) stated that its members would install doors that meet security standards similar to those adopted in the United States but not until November 2003. The ICAO also did not require any temporary fixes until that date. As in the 1970s, when rules were also hastily implemented, the airline industry balked regarding the costs. Cargo carriers, such as the United Postal Service, have been particularly vocal, commenting that they

FIGURE 4.1 Denying access to the cockpit could potentially prevent another attack in which a plane is utilized as a weapon.

are at little risk of hijacking. Some airlines had originally estimated the cost per aircraft would be 50,000 U.S. dollars or 35,000 pounds Sterling. The U.S. Transport Association hoped to lobby the U.S. Congress to foot the bill, which they estimated to be about 250 million U.S. dollars.

On 16 September 2001, DOT Secretary Norman Y. Mineta formed a Rapid Response Team on Airport Security. They met and published 17 recommendations in October 2001. The Rapid Response Team decided the following (Internet: http://www.dot.gov/affairs/aircraftsec.htm.):

- Some appropriate flightdeck barrier device must be approved and installed in the entire U.S. fleet, and future design of flightdeck doors must meet newly determined requirements.
- Procedural changes must be made at all airlines regarding identification and access of all personnel to the flightdeck.
- Airline industry, unions, and the FAA should redesign security training with possible implementation of defensive capabilities to address newly identified threats, incorporate changes into the annual curriculum, and provide security training to all crew members.
- Each airline, in cooperation with the FAA or other government entities, must develop a delivery system to provide government security advisories to crew members in a timely manner.
- A task force should determine the necessary modifications to assure continuous transmission of a transponder signal.
- All airlines, pilots, and the FAA should jointly identify procedures in pilot training that could be adapted in an attempted hijacking.

Aviation industry suppliers including Alcoa Aerospace, Boeing, and AAR vigorously competed for the business. AAR claimed to have produced the cheapest, ThreatDefense™ at approximately 18,000 U.S. dollars. In Britain, British Airways used reinforced metal to toughen doors. The government reacted decisively, and in the interim, on 9 October 2001, the FAA published the first of a series of Special Federal Aviation Regulations (SFARs) to expedite the modification of cockpit doors in the U.S. fleet. This “Phase I” fix included installation of steel bars and locking devices. U.S. airlines voluntarily modified the cockpit doors on 4000 airplanes within the first 45 days of the SFAR. Additionally, Virgin Air installed Permaglass armor plating on its 25 aircraft. By January 2002, 98 percent of the airlines had voluntarily installed a Phase I fix. By 1 March 2002, most U.S. airlines completed installation of cockpit door modifications.

To fund the project, the President requested $300 million from Congress. Congress appropriated $100 million. According to the FAA fact sheet (http://www.faa.gov/newsroom/factsheets/2002/factsheets_020905.htm):

- On May 3, the FAA announced plans to distribute $100 million that Congress appropriated for security enhancements to aircraft cockpit doors and cabins.
- The FAA established the pilot program to find the most effective technologies that could be adopted by the greatest number of air carriers in a short time. Any FAA-certified Part 121 air carrier was eligible to apply for the program by 16 October 2001.
- Approximately $3 million was distributed to 11 airlines under a pilot program to install video and other technology for use in the cabin and to implement emergency alerting systems that may be installed in the aircraft or carried by cabin crew members.
- The remaining funds—approximately $97 million—will be given to air carriers to fortify their flightdeck doors. The funding may be applied to locks and other barriers already installed, as well as to the permanent design changes that must be in place by April 2003. Each carrier will receive approximately $13,000 per aircraft, with the total not to exceed the actual costs.

Modifications have now been completed on the doors of all U.S. airliners and the doors on international carriers that serve the United States. In addition, the Transportation Security Administration (TSA) pondered further rule-making to require other measures in the aircraft; including surveillance systems to alert crews of activity in the cabin and an upgrade to ensure the continuous operation of the airplane transponder.

PASSENGER PHOTO IDS

Other security-related suggestions included the initiation of photo indentification (ID) cards. After careful consideration, however, the issuance of photo ID cards to passengers was determined to be a potentially administrative nightmare. Essentially, who should get one and who should not, opens the door for not just harmless administrative errors but also screaming passengers with complaints of discrimination. Decisions regarding who should get "a pass" and how the determination was to be made would likely have been totally mired in a swamp of legal pitfalls. Setting aside the problems of the size of sheer administration of such a program, the likely plethora of accusations of discrimination, which would surely arise, made any attempts to implement such a program impractical. Nonetheless, the former director of Homeland Security has publicly advocated a "trusted traveler" program, and a registered traveler program is currently in use. Passengers agree in advance to submit personal information in exchange for an alleged counterfeit-resistant ID card that would permit them to be exempt from some portion of security. The details were initially unclear and conflicting. Efforts to also use biometric means of identification to provide frequent travelers quick access is undergoing testing under the registered traveler program and will present a new set of challenges.

CREW TRAINING

Soon after 11 September 2001, the FAA also reviewed procedures pertaining to appropriate aircrew training. In January 2002, the FAA formally issued new guidance for training crew members in dealing with potential threats, especially hijackings. The guidance took into consideration a significant change in strategy from passive resistance to a more active response by crew members. The specific contents of the guidance have not been released to the public for security reasons. The guidance did emphasize that the training must now be considered a shared responsibility, meaning increased cooperation between the government, the carrier, and the carrier's employees. In general the FAA emphasized the following (Internet: http://faa.gov):

- The aircraft captain should include any security information specific to the flight or to the airline during the preflight crew briefing.
- Any passenger disturbance, even those seemingly harmless, should be considered suspicious; it could be a diversion for other more serious acts.
- In a threat situation, crewmembers must act as a team. If a threat arises, the cabin crew and flight crew must communicate in clear, concise, plain English.
- In any suspected or actual hijack attempt, the flight crew should land the airplane as soon as possible to minimize the time hijackers would have to commandeer the aircraft and use it as a weapon of mass destruction.

PROFILING

The determination of just exactly what a "hijacker" looks like or acts like constantly lends itself to questions of prejudice based on race, national origin, and religious preference. U.S. law strictly prohibits any such discrimination. Law enforcement, however, continues to argue that some citizens can be identified as potential hijackers, thereby segregating them from the general population. Such a concept is known as profiling.

In the 1970s, an FAA Task Force study encompassed motivational and behavioral characteristics of hijackers, identification of the weapons used, and an analysis of the origin and intended destination of hijacked flights. Later, the FAA adopted a profile-screening program tested by Eastern Airlines due to its apparent consistent vulnerability. The results of the test indicated that between 80 and 90 percent of hijackers appeared to fit the profile established by the commission. Unfortunately, so did a lot of innocent passengers.

Government authorities are constantly relooking at the issue of profiling. Racial profiling is certainly a term that is frowned on by civil libertarians. Realistically, however, security experts argue that profiling should simply be a process in which information in some sort of a database can be used to separate passengers into two groups. The two groups would include those who present little or no risk, and those who merit additional attention from the appropriate security personnel. Profiling has been used successfully by other government agencies including the Federal Bureau of Investigation (FBI) and the Customs Service, although not without generating some heated controversy. Currently, despite recommendations by security professionals that automated passenger profiling be used at airports complementary to other security procedures, the idea remains extremely controversial and has not been universally implemented. Many groups, including the American Civil Liberties Union (ACLU), have argued that such a set of records violates citizens' civil liberties.

Regardless of the controversy, the FAA originally assisted three major airlines in implementing just such a system. The FAA had, through a grant to Northwest Airlines, developed a prototype system known as Computer-Assisted Passenger Screening (CAPS). The automated system used information from the reservation system to screen out passengers for whom additional security procedures were unnecessary. On the other hand, if the system determined that a certain passenger was high risk, that person was subjected to additional security procedures when they arrived at the airport and presented a ticket. The system also randomly selected passengers for additional screening. Even though the criteria for selection were secret, sometimes the criteria selected a person clearly not a threat and embraced some questionable elements. Assuming some of the criteria included one-way travelers, travelers that paid with someone else's credit card, unemployed travelers, last-minute travelers, or simply someone who was not a frequent traveler, "mistakes" seem evident. For example, a young boy selected by CAPS was forced to drink pond water he collected for a science project, which ultimately made him sick.

The legality of any such system potentially faces significant challenges in the courts. Civil rights groups as well as Arab-American groups have specifically raised questions regarding the singling out of minorities, specifically Arab-American passengers. All of these groups raise issues of discrimination and invasion of a passenger's privacy. To address these concerns, the DOT submitted

the entire profiling system parameters to the Department of Justice (DOJ) Civil Rights Division for critical review. In October 1997, the DOJ issued a report. The document concluded that CAPS did not violate the Fourth Amendment prohibition against unreasonable searches and seizures nor an individual's right to personal privacy. The report also concluded that there was no evidence that the system recorded an individual's race, color, national or ethnic origin, religion, or even gender when conducting a profile. It should be noted that these conclusions are contained in a DOJ report and did not necessarily mean they would survive judicial scrutiny. The Supreme Court of the United States will likely get to have the last word on the issue.

CAPPS II

In addition, the former CAPS program needed to be updated and improved. Consequently, CAPPS II (Computer-Assisted Passenger Prescreening System) the second-generation system, was supposed to be up and running by the summer of 2004, but the Department of Homeland Security (DHS) announced in late July 2004 that it would be terminated. The system had already cost almost 100 million U.S. dollars when discontinued. As mentioned, the precursor of the program was initiated in 1998, when Northwest Airlines agreed to participate. The network used the following color codes: green for minimal threat, yellow for those deserving of heightened security, and red for those judged to pose an acute danger and who would be referred to law enforcement for possible arrest.

Later, CAPPS II was scheduled for a test run in the spring of 2003 using passenger data provided by Delta Airlines. Following a public outcry, however, Delta refused to provide the data, and the test run was delayed indefinitely. This program had also been subjected to significant criticism by the public and civil liberties groups.

Congress and private groups again had expressed serious concern over privacy issues, including the concept of commercial databases that would have been used to obtain information, how long it would have been stored, and what appeal processes would have been put in place to address misidentified passengers. Students at the Massachusetts Institute of Technology (MIT) had even concluded that the new system was less secure than random selection. According to the students' research, it would have been fairly easy to learn which passengers were to be designated as a green, yellow, or red threat and to subsequently match the required criteria. However, managed properly, this system could have been a strong weapon in the war on terrorism.

SECURE FLIGHT

Additionally, Section 7 of the Air Cargo Security Improvement Act, passed in December 2003, instructed the Secretary of Homeland Security to submit a report within 90 days to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Transportation and Infrastructure on the potential impacts of the TSA's proposed profiling program. The study was to directly address the effects of the proposed program on the privacy and civil liberties of all Americans. The overall program was designed to use commercial records, terrorist watch lists, and computer software to assess millions of travelers and hopefully target those posing a threat. Many considered the project intruded too deeply into the private lives of ordinary citizens. The Bush Administration stated it might test the program after the election. The TSA introduced Secure Flight in August 2004, shortly after the agency abandoned plans for its predecessor, the second-generation Computer-Assisted Passenger Prescreening System (CAPPS II).

In an unusual twist, the developer of the program, Ben H. Bell III, a former intelligence officer, decided to sell his idea offshore; outside the reach of U.S. regulators. Bahama-based Global Information Group intended to amass large databases of international records and analyze them in the future for corporations, government agencies, and other information services. They had changed the name from CAPPS II to Secure Flight and planned on advertising the concept as a terrorist-risk, identity-assessment tool. Legal scholars contend the program raises some troubling new questions

about the ability of computers in both the government and commercial sectors to collect and analyze personal information in the name of homeland security.

Clearly since 11 September 2001, there has been a widely reported increase in racial profiling at airports, particularly as it applies to people who appear to be Muslim or of South Asian or Middle-Eastern descent. A year-long study conducted by the Domestic Human Rights Program of Amnesty International U.S.A. appears to indicate that the unlawful use of race in police, immigration, and airport security procedures has expanded. The study further alleges that state laws provide insufficient and inconsistent protection against profiling. When the TSA began testing Secure Flight in November 2004, the program would compare passenger records to the expanded "selectee" and "no fly" lists already in use. Passengers whose records matched names on the lists were to be subject to commercial background checks to verify identity. The agency stated that it planned to have a redress process for individuals improperly flagged by Secure Flight, but it was unclear how this process would have worked. Many travelers still believe that the program contains irresolvable privacy and security concerns.

Secure Flight was the TSA's most recent attempt to legalize the use of a federal passenger prescreening program. However, the TSA announced that the program would be delayed until at least 2010 to complete a review of the program's information security measures after two government reports indicated privacy problems. About 140 million U.S. dollars had again already been spent on the program, and it is expected another 80 million U.S. dollars would be needed to address its current deficiencies. One report indicated the program had inconclusive risk assessments and 144 known security vulnerabilities (Internet: http://www.gao.gov/new.items/d06374t.pdf).

The system originally was intended to compare passenger information from passenger name records, which contained information given by passengers when they book their flights, against watch lists maintained by the federal government. In furtherance of this program, the government ordered 72 commercial airlines to relinquish passenger records in November 2004 covering the month of the previous June 2004 to test the system in 2005. Like its predecessor CAPPS II, the test phase of Secure Flight was initially exempted from crucial provisions of the Privacy Act of 1974. This exemption, which would have severely limited the rights individuals typically would have regarding the personal information the government maintains about them, troubled many Americans. In addition, arguably, passengers would have had no judicially enforceable rights to access and correct the personal information maintained about them for the program. In June 2005, however, TSA announced revoking all the Privacy Act exemptions it had initially claimed.

Unfortunately, even members of Congress have found themselves flagged by the watch lists. In August 2004, Senator Edward Kennedy (D-MA) revealed in a Senate Judiciary Committee hearing on border security that on multiple occasions airline agents tried to prevent him from boarding flights because the name T. Kennedy appeared on a watch list. He was halted three times before his staff called TSA. Afterwards he continued to be stalled at the gate even though the likelihood of Senator Kennedy being the IRA member referred to on the list was ludicrous. Senator Kennedy was forced to call Homeland Security Secretary Tom Ridge to clear his name. This, however, is not a readily available option to the average passenger. Reps. John Lewis (D-GA) and Don Young (R-AK) have also been flagged by the watch lists. As stated, TSA chief Kip Hawley told the Senate Commerce Committee in February 2006 that plans for Secure Flight have been suspended until a "comprehensive audit" of the program's information technology security is completed.

NO FLY LIST

The TSA became authorized to maintain watch lists of names of individuals suspected of posing "a risk of air piracy or terrorism or a threat to airline or passenger safety." Although initially denying that such a list existed, the TSA acknowledged its existence in October 2002. The TSA has been heavily criticized about the program and subjected to numerous Freedom of Information Act requests. A lawsuit was also filed seeking to discover TSA's criteria for placing people on the lists, which bar some

passengers and expose others to extensive scrutiny. Opponents also were concerned about complaints from passengers who felt they were mistakenly placed on the list in the first place.

Eventually it was made public that TSA administered two lists: a "no fly" list and a "selectee" list. One prohibits the passenger from flying at all, and the other requires the passenger to submit to additional security measures. The names are provided to air carriers through Security Directives or Emergency Amendments and can be flagged via their computer boarding systems when a passenger gets a boarding pass. Specifically, a "no fly" match requires the agent to call a law enforcement officer to detain and question the passenger. In the case of a Selectee, an "S" or special mark is imposed on their boarding pass, and the person subsequently receives additional screening at the security checkpoint. The number of names on these lists is undisclosed.

The watch list originally was created in 1990, with a list of individuals who have been "determined to pose a direct threat to U.S. civil aviation." The FBI initially administered the list before the FAA and the TSA assumed full administrative responsibility in November 2001. The Transportation Security Intelligence Service (TSIS) currently serves as the clearinghouse for the addition of names to the lists. Since the TSA took over and according to the acting Associate Undersecretary of Transportation Security Intelligence in 2002, the watch list, "has expanded almost daily as intelligence community agencies and the Office of Homeland Security continue to request the addition of individuals to the no-fly and selectee lists" (Internet: http://epic.org/foia_docs/airtravel/memo-10-16-02.pdf). The names are approved for inclusion on the basis of secret criteria. The watch list memo notes that "all individuals have been added or removed...based on the request of and information provided, almost exclusively by [redacted]." This memo is a must read. There does not appear to be any provision for an independent verification that the names are appropriately added or that the system is in compliance with the Privacy Act of 1974. Prospective passengers need to contact their local FBI office to begin the process to be removed from the list. In addition, an ombudsperson within the TSA processes the requests.

Regardless, complaints have proliferated. Most recently, airlines have acutely become aware of the fact that passengers are frustrated with the cumbersome and often seemingly irritating security systems at airports. To date, airport security officers have treated every single passenger as a suspected terrorist until proven otherwise. The alternatives suggested include renewed emphasis on profiling, registered-traveler program, and last but not least, the simple use of common sense.

SKY MARSHAL PROGRAM, FEDERAL AIR MARSHAL PROGRAM

FAA Order 1650.6 formerly governed the program, which had been authorized in the Federal Aviation Act of 1958, the Anti-Hijacking Act of 1947, and the International Security and Development Cooperation Act of 1985 (Public Law 99-83). The program established a covert, armed security force capable of rapid deployment. The precursor of the Federal Air Marshal (FAM) program, known as the Sky Marshal Program, was announced in a Department of Treasury news release dated October 1970. When the perceived need for armed agents first arose, Secretary of the Treasury David M. Kennedy and Secretary of Transportation John A. Volpe were responding to President Nixon's call in September 1970 for armed personnel on U.S. commercial flights. John Cashman (1970) in an article, "Sky Marshals — How They Train and What They Do," wrote that the original members were a temporary force recruited from the Customs bureau, the FAA, the FBI, the Central Intelligence Agency (CIA), and the military. Eventually a permanent force of 1500 civilians was established. The team became known as Customs Security Officers (CSOs) who were trained by the former Bureau of Customs and attached to the FAA.

Unfortunately, it did not work. The program clearly enjoyed some success, but proved incapable of stopping the continuing attempts to hijack aircraft. Early on, the Director of Civil Aviation Security for the DOT, Lt. Gen. Benjamin O. Davis (U.S. Air Force, Retired), recognized the need to switch primary security efforts from the aircraft to the ground. Time would prove that even aircraft with both an FBI agent and a Sky Marshal on board were not immune from incident. Once the

aircraft is in flight, the hijackers are already on board, and the presence of agents did little to deter the attempts. It was therefore determined fairly early that the better security solution was preventive in nature and better pursued on the ground. Prevention of access to the airport or aircraft was and remains a crucial key to security. Apparently, that lesson will have to be relearned.

Furthermore, the airlines considered the coverage too sparse and feared a midair shootout. The debate over the Sky Marshal program in the 1970s raged for many years (Karr, 1971). The FAA responded to complaints from the air carriers by charging the airlines with being solely preoccupied with efforts not to inconvenience the passengers instead of focusing on security. When mandatory 100 percent passenger screening became effective in deterring hijacking, the need for these airborne law enforcement agents seemed to lose support. Eventually the program fell into disrepair. The number of agents was reduced to as little as three dozen active agents prior to September 2001. The government now considers a revitalized training program as key to the success of an upgraded federal air marshal program (see Figure 4.2).

Currently, the FAMs aboard aircraft are some of the best marksman in the world. They are highly trained, and their firearms training requirements are some of the most stringent in law enforcement. The Certified Protection Professional certification program (American Society for Industrial Security) has been acknowledged by the TSA as the only "security management designation" that will be recognized on the application form. Other certifications include sworn civilian law enforcement, emergency medical technician, private pilot, and licensed attorney. As mentioned, it was still considered prudent in March of 1976 to formalize the FAM program, and it continues to provide extra security aboard high-risk routes with renewed vigor since 11 September, with less than enthusiastic support from the airlines. The agents themselves are deputized as Special Deputy U.S. Marshals.

FIGURE 4.2 A pistol wielding Federal Air Marshal runs between seats during a simulated hijacking aboard a retired L-1011 aircraft at the training facility in Pomona, NJ. The program has received extensive funding since the 9/11 tragedy, but has also received considerable criticism regarding its training and scheduling practices.

The program also received a great deal of attention after the hijacking of Trans World Airlines Flight 847 on 14 June 1985. Captain Testrake and his crew were hijacked, and the media plastered the real-time photographs of the event all over the world, indicating to the terrorists that the media and the public could not get enough of it. In response to the dramatic events relating to Flight 847, the FAA drafted and implemented FAR 108.14, which required scheduled carriers and public charter operators to carry federal marshals on a priority basis, without charge, even if it required bumping a paying customer. The new regulation also corrected a gap in the regulations that had not provided for the deadheading of agents, i.e., how did they get back home after completing a working flight in one direction only.

The FAM program currently has its training facility and airline security research facility located at the Williams J. Hughes Airport and falls under the purview of the new TSA (49 CFR Chapter XII Part 1544.223). Using a wall full of computer-generated maps, the TSA tracks the flight path of each flight with an air marshal on board, and supporting documents indicate the travel schedule of each marshal. It currently employs 45,000 people and is financed with a 4 billion U.S. dollar supplemental spending bill from Congress. The agents receive special training and regularly travel on U.S. air carriers on high-risk routes. They represent some of the very few people who are authorized to carry firearms on board aircraft and use them if necessary. Additionally, as federal agents, they are permitted to make arrests without a warrant when certain felony offenses against the United States can be reasonably shown to have been or are in the process of being committed.

Today, the FAM program is just one of the tools used by air carriers, airport security officials, and law enforcement agents in combating the threats to civil aviation. The FAM agents continue to fly millions of miles a year, blending into the crowd of other passengers unbeknownst to a vast majority of them. However, the debate is back. Rep John Sweeney (R-NY) a member of the House Appropriations Subcommittee, has been quoted as saying, "We need to start seeing some results that are equal to the huge investment that we're making" (CNN, 8 May 2002). The program always seems to gain attention and support after a significant event. Administrations use the public's fear to support the need for the air marshals, but after the hullabaloo dies down, the practical usefulness, aside from a perception of security on the part of the traveling public, dims considerably.

More recently, an incident on 7 December 2005, on American Airlines Flight 757; Miami, FL renewed the debate and fueled the arguments on both sides regarding the actual legitimate jurisdiction of the marshals. The aircraft had arrived from Medellin, Colombia, and was on a roughly two hour stopover in Miami before continuing to Orlando. It is alleged that one of the passengers, a 44-year old U.S. citizen claimed to have a bomb in his carry-on luggage. Air marshals confronted the man on the jetway and shot him after he appeared to reach into his bag. The man died sometime later as a result of his wounds. No explosive was found in the bag. It was reported that this passenger had previously arrived in Miami on an American flight from Quito, Ecuador, and had cleared U.S. customs before boarding the Orlando flight. No one else was injured in this event. This is the first time since 11 September 2001, that air marshals have fired a weapon on or near an aircraft. In that international law clearly provides that an aircraft is not in flight until the doors are shut, it became evidently clear that Dade County law prevailed. Should the marshals have used deadly force under the circumstances? The debate continues.

HISTORY OF SIGNIFICANT AIR HIJACKINGS SINCE 1972

Both public and airline officials were eventually forced to recognize the need for balanced, yet more stringent airport and airline security measures as early as the 1970s. However, the battle to control the commercial airways witnessed much tragedy before they jointly reached this conclusion. As is often the case, it takes a tragedy to get the legislative processes moving to implement the necessary security measures and plans to provide an adequate defense against those who would use innocent airline passengers and crews to serve the needs of political causes. The task of ensuring the security of U.S. international and domestic air travel clearly represents a monumental task. Typically,

in one day, security professionals screen more than 1.5 million passengers and carry-on baggage. Both passengers and baggage are now routinely screened for metallic weapons and other dangerous materials. This was unfortunately not always the case. Consequently, the window of opportunity was open to terrorists. In the event of a lack of effective screening, terrorists have recognized the window and boldly stepped through it on repeated occasions.

To better understand why the current procedures are in effect and tolerated; a general review of the hijacking problem is useful. Its evolution and destructiveness has been momentous and has grabbed the attention of the media due to the sensational nature of the incidents. There have been numerous events that have mesmerized the public; however some stand out in importance. News reports reveal that terrorism continues to take different twists and turns. Some security efforts have succeeded, but nonetheless terrorism has not been stopped. Security became in many ways totally reactive and arguably continues to be. Authorities were reacting to the horrific hijackings at the end of the 1960s and early 1970s and now the monumental event of 11 September 2001. It is safe to say the aftermath of the hijackings has changed the face of aviation for years to come. Airports are by their very function open and public places and therefore all that more difficult to protect. Today, the threat extends from the airport facilities, the aircraft, and use of the aircraft as a weapon to even more horrific possibilities.

31 May 1972: Lod Airport

Israel has always been a significant target and will likely remain so. On 31 May 1972 at Lod Airport in Tel Aviv, three Japanese passengers disembarked from an Air France flight arriving in Israel from Paris and Rome. After proceeding to the baggage pickup area, several terrorists retrieved their bags. Inside the luggage were grenades and machine guns. The three terrorists began firing the guns and throwing the grenades randomly throughout the waiting area. The terminal area, however, was crowded with travelers on a Christian pilgrimage vacation and not the intended target of Jewish Israelis. The rampage resulted in the deaths of 26 people and the wounding of another 78. Later, the three seemingly regular travelers-turned-terrorists announced they were members of the Army of the Red Star and claimed the attack was an act of reprisal. The group was pledged to a Marxist revolution and was heavily involved in the Palestinian struggle in the Middle East (Wardlaw, 1982). Earlier that month an Israeli security team killed two Arab terrorists who had failed to hijack a Belgian plane at the same airport. The violence was to contribute to a cycle of attack and reprisal that survives today. Seven hardcore Japanese Red Army (JRA) members remained at large as recently as 2001 (Simonsen and Spendlove, 2000).

27 June 1976: Entebbe, Uganda

In 1976, Israeli commandos executed a raid at Entebbe's airport where they freed 103 Israeli hostages from a plane hijacked by Palestinian and German terrorists. The Air France Airbus was originally enroute from Tel Aviv to Paris but had made a stop in Athens. It was forced to fly to Benghazi, Libya, where it refueled and proceeded on to Uganda's Entebbe International Airport. In conjunction with the rescue effort, 11 Uganda Soviet-made MIG fighter aircraft were destroyed as well as most of the airport. Previously, on 27 June 1976, Palestinian terrorists working with the Baader-Meinhof Gang hijacked an Air France plane enroute from Israel to France. The terrorists had also demanded the release of about 53 of their comrades from prisons in West Germany, France, Switzerland, Israel, and Kenya. The Palestinians freed many of the 258 original passengers who did not appear to be Israeli. Debriefing of these released hostages provided the authorities with vital information on the hijackers' numbers and organization. The remaining 106 hostages, merely suspected of being Jewish, were retained. Because the hijackers had separated those of the Jewish faith from other passengers, the terrorists had brashly indicated their intent to intimidate Israel.

In a bold move, the Israelis decided not to succumb to the terrorists' demands. They decided on a course of action that turned out to be a spectacular rescue operation. On 3 July they dispatched four Hercules C-130 H cargo planes from Ophira Air Force Base loaded with almost 200 soldiers escorted by several F-4 phantom jets. Major General Dan Shomron, the Israeli Director of Infantry and Paratroopers, designed the plan, originally named Operation Thunderball. After successfully flying the 2500 miles to Uganda from Israel, commandos swiftly took back the hostages during a 90-minute raid. The Israeli Defense Forces, in a brilliant tactical deception maneuver, approached the aircraft in a convoy headed by a black Mercedes limousine. They hoped to fool the Ugandan soldiers surrounding the plane into believing that Idi Amin, the Ugandan president, was making a surprise visit. One soldier and three hostages were killed during the operation. The killed hostages apparently did not hear or understand the commando's command to lie down. The only Israeli military casualty was the team's leader, Colonel Jonathan Netanyahu. A Ugandan soldier tragically shot him in the back. The seven terrorists killed included two Germans, Wilford Bose and Gabriele Krocher-Tiedemann, plus five Palestinian members of the PFLP. During the entire incident, disastrously 30 people were killed and 42 were injured because the Ugandans sought to prevent the Israelis from leaving with the hostages. The entire operation lasted only three minutes (Williams, 1985). However, the Israeli's set the tone for any future attempts on their citizens or aircraft. They now have some of the most stringent aircraft and airport security procedures in the world.

14 June 1985: Trans World Airlines Flight 847

In one of the most infamous hijacking scenarios, two Lebanese Shi'ite Muslim terrorists boarded Trans World Airlines Flight 847 departing Athens, Greece, on 14 June 1985. The Boeing 727 was scheduled to fly to Rome when in mid-air, two hijackers seized the aircraft. In a quirk of fate, a third terrorist was unable to get a seat and therefore was not boarded onto the aircraft. President Ronald Reagan had taken a hard line against terrorism, and this incident evidenced a renewed assault against U.S. commercial carriers not seen since the 1970s. Nabih Berri, the spokesman for the Amal Militia, also jumped into the fray and sought to expertly choreograph the entire incident for the best media effect possible.

After being diverted, the plane was permitted to land in Beirut, Lebanon, with 145 passengers and 8 crewmembers aboard. The terrorists demanded that over 700 Shi'ite persons in Israeli jails be released. The hijackers subsequently released 17 American women and two children, but additional gunmen came aboard. The pilot, John Testrake, was forced to fly the aircraft to Algeria where 19 more American women, 1 child, and 3 people of non-Israeli nationality were permitted to disembark. On 15 June, the plane returned to Beirut where yet another 10 Americans were released. However, tragically, after reviewing travel documents and discovering a U.S. military member, the hijackers beat unconscious a U.S. Navy diver, Robert Dean Stethem. They executed him and threw his body out the door of the plane. On the move once again, the plane returned to Algiers. Later, in return for the release of a comrade arrested at the Athens airport, an additional 53 passengers and 5 flight attendants were freed.

On 16 June, after flying back to Beirut again, the hijackers now threatened to blow up the plane if 50 Lebanese sympathizers held in Israeli jails were not released. Simultaneously, the U.S. Navy's 6th Fleet was ordered into the Mediterranean Sea and the elite U.S. Army Delta Force was deployed to the area. The Amal Militia then demanded the release of 800 other Lebanese prisoners, while the hijackers reiterated an earlier demand for the release of 50 Lebanese prisoners, as well as two Shi'ites held in Madrid for attempted murder. At this point, the demands were not met, and the remaining passengers were removed from the plane as hostages, leaving a crew of three on board. Nabih Berri announced that the hostages were to be split up to thwart a suspected rescue mission. To meet the suspected threat, the Amal militia allegedly put 6000 men on alert. Furthermore, the hostages with "Jewish-sounding" names were retained by a radical Iranian terrorist group, Hezbollah, but one ailing American, Robert Peel was released.

The details of the situation were broadcast around the world in real time. Nabih Berri, on 18 June, continued to very publicly pressure Israel into releasing hundreds of Lebanese, most of them Shi'ites. At a news conference, former President Reagan announced that any retaliation would be risky and also chastised the Greek government for lax security procedures. Meanwhile, the British and Italian Ambassadors to Lebanon, as well as the Syrians, declared they were involved in negotiations; while Reagan considered forcing the Lebanese to close the Beirut airport if diplomatic moves failed. The incident received global attention. Even the Russians jumped into the act. Soviet spokesman, Vladimir Lomeiko condemned the hijacking, but suggested that the United States created the conditions that foster terrorism.

Eventually, on 29 June, the Syrians announced they had negotiated a settlement to the crisis. That same evening, the hostages were taken to a hotel for dinner and seen leaving with roses from their captors. The next day, 17 days after the hijacking began, the hostages were handed over to the International Red Cross and driven to Damascus, Syria, where they boarded a U.S. military aircraft bound for Rhein-Main Air Base in Frankfurt, Germany. Two of the hijackers were never caught, although all three, Mohammed Hamadei, Ali Atwa, and Hasan Izz Din had prior outstanding arrest warrants issued in 1985. Mohammed Ali Hamadi, 22, later was arrested trying to enter West Germany with liquid explosives on 15 January 1987. Approximately two years after that, the German Hesse State Supreme Court convicted him of hijacking, the murder of Robert Stethem, and the possession of explosives. He received a sentence of life imprisonment. Eventually, efforts to use international law, namely, The Hague and Montreal Conventions, all failed, and two of the three have never been brought to justice.

21 December 1988: Pan American Flight 103

The actual aircraft for Pan American Flight 103, a Boeing 747, N739PA, had originated in San Francisco. Many of the passengers arrived from Frankfurt, West Germany on a Boeing 727 that had been positioned on stand Kilo 16 next to the Boeing 747. The passengers were transferred with their baggage to N739PA, which was to fly to New York. After a 6-hour turnaround, the aircraft left Heathrow airport at 6:04 PM with 243 passengers and a crew of 16 on board. The aircraft also carried 20 tons of cargo and 43 bags of military mail. As it was approaching the Burnham VHF omni-directional radio (VOR), it took up a radar heading of 350 degrees and flew below the Bovingdon holding point at 600 feet. At 31,000 feet, slightly northwest of Pole Hill VOR and approximately seven minutes later, Shanwick Oceanic Control transmitted the aircraft's clearance. This transmission was not acknowledged. Subsequently, radar showed multiple primary returns fanning out downward.

The aircraft literally exploded over Lockerbie, Scotland, (55 degrees 07 minutes N, 003 degrees 21 minutes W) and fell to the ground in pieces, killing 11 more innocent souls on the ground. Major portions of the wreckage fell over the town of Lockerbie and to the east. Smaller debris was strewn along two trails, the longest, which extended approximately 130 kilometers to the coast of England. A complete primary wing structure, incorporating the center section of Pan Am 103, impacted on the southern edge of Lockerbie. The weight of the material displaced by the wing structure was estimated to be well in excess of 1500 metric tonnes. The impact of the crashing plane was so strong that the British Geological Survey recorded a seismic event measuring 1.6 on the Richter scale. The crash received international attention. The families of the victims banded together and have pursued the facts and issues surrounding the crash with the tenacity of a bulldog. This aspect alone makes this particular crash especially unique (see Figure 4.3).

Responsibility was originally thought to fall on the PFLP because of radiocassette bombs discovered in the hands of the Popular Front for the Liberation of Palestine—General Command (PFLP-GC) prior to the bombing. Many intelligence analysts were convinced that the Iranians were retaliating for the accidental shooting down of one of their commercial carriers by an American naval ship. The latest evidence, however, indicates Muammar Khadaffi, the notorious dictator of

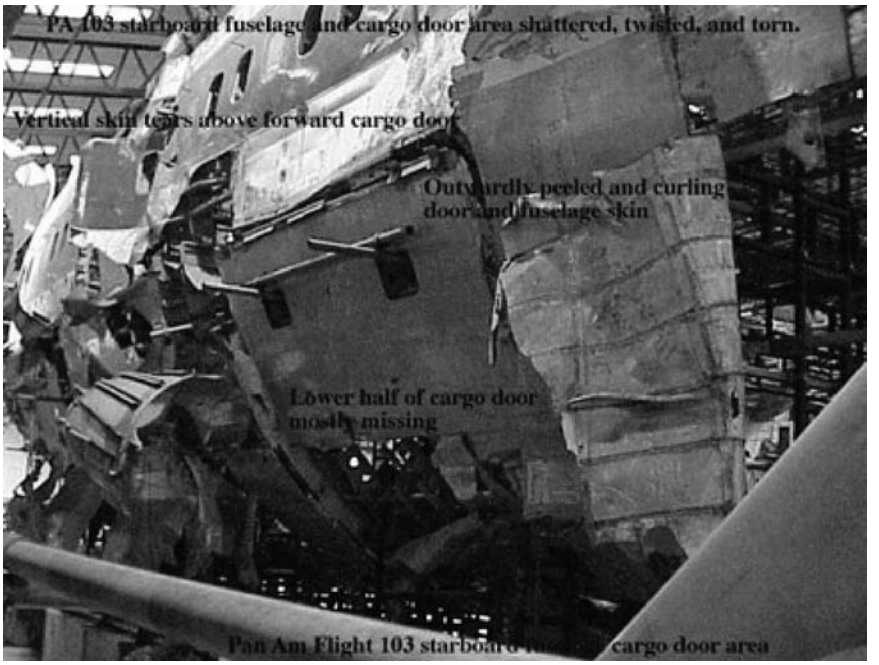

FIGURE 4.3 The Pan Am flight 103 airliner with its destroyed shell in Scotland. This photo from the National Transportation Safety Board shows the cargo door. The photo is a pictorial reminder of the need to focus attention on cargo security and the consequences of neglecting to do so. (Source: NTSB, www.ntsb.org)

Libya was really responsible. Law enforcement later discovered a significant clue. A link was established between an obscure case involving the arrest of Mohammed Marzouk and Mansour Omran Saber, both Libyan Intelligence agents, at Dakar, Senegal airport in 1988 and the Lockerbie explosive device. It turns out they had in their possession 20 pounds of Semtex plastic, TNT explosives, weapons, and some triggering devices. One of the triggering devices matched a microchip fragment from the Pan American bomb. The circuitboard fragment recovered from the crash was actually part of a sophisticated electronic timer. Senegalese authorities discovered the same type in the possession of the two Libyan terrorists who had been arrested in February 1988. Meister et Bollier, a Swiss electronics firm, specially manufactured the timers, designated as MST-13, and confirmed that all 13 timers had been delivered to the Libyans.

Further investigation revealed that Abdal-Basit Al-Megrahi, a senior Libyan intelligence official and Lamen Fhimah, the former manager of the Libyan Arab Airlines office of Malta, conspired to bomb Pan American Flight 103. The perpetrators made use of the Czech-made explosive and Semtex. A double detonator device was used. The first trigger was activated by barometric pressure, which in turn activated a timing device. The actual bomb was encased in a Toshiba radiocassette player. The terrorists were able to obtain and attach an appropriately marked Air Malta tag that enabled the luggage to circumvent baggage security measures and to be directly routed to the Pan American feeder flight.

Forensic experts identified the bag that contained the bomb as a brown, hard-sided Samsonite suitcase. One of the defendants, Al-Megrahi, arrived in Valletta's Luqa airport, with the other defendant, Fhimah from Libya on the evening of 20 December 1988. Because Fhimah had been the former manager of the Maltese airport, he had somehow retained full access to the airport. Scottish investigators traced the clothing that had been packed in the bag to a shop in Malta. Frankfurt airport

records revealed that an unaccompanied bag was routed from Air Malta Flight 180 to Frankfurt where it was eventually loaded onto the Pan Am Flight 103 feeder flight, as per arguably legal procedures in effect at the time. The bomb was perfectly placed immediately next to the outer skin of the aircraft, indicating possible assistance from a ground handler when the plane was being loaded.

A warning bulletin describing the device was sent by the FAA on 18 November 1988. The bulletin was delivered to U.S. embassies and consulates around the world. However, the one airline official, designated to read such material at Pan American, first saw the bulletin after a 3-week vacation and well after the crash. The issue of who should be advised of these warnings continues to be controversial. For example, many telephone threats are fraudulent and it is often difficult to separate the real threats from the false ones. As a result, such procedures have been changed so that carriers now provide written acknowledgment to government authorities of the receipt of such bulletins and the action being taking. Procedures have not significantly changed regarding who actually has access to the information.

Other safety and security issues were also involved. Apparently a telephone threat, received from an anonymous caller on 5 December 1988, at the American Embassy in Helsinki, Finland, warned of the impending disaster. The caller claimed a Finnish woman would carry a bomb aboard a Pan American flight from Frankfurt to the United States sometime during the next two weeks. The U.S. State Department sent out diplomatic traffic notifying its own personnel. Even though notice again was disseminated to all U.S. consulates and embassies, because Finnish police determined it was a hoax, the information was not passed to the FAA. The procedure of nondisclosure, which emerged from this incident and was persistently raised by the families of the victims, questioned exactly who should be advised in the event of credible threat information. The recommendation of the President's Commission on Aviation Security and Terrorism in May 1990 was in favor of public notification of threats to civil aviation. However, security officials and the air carriers had reaffirmed an overall policy of nondisclosure. Nonetheless, Section 109 of the Aviation Security Act of 1990 now directs that Title II of the Federal Aviation Act of 1958 be amended to provide that the President shall develop guidelines for ensuring notification to the public of threats to civil aviation in appropriate cases. What the term "appropriate cases" means is not quite clear.

The Lockerbie incident also raised the issue of passenger-baggage reconciliation. The President's Commission reported and concluded that passenger-baggage reconciliation is a bedrock component of any heightened security program. In 1988, Pan American was x-raying all interline bags rather than identifying and physically searching unaccompanied interline bags. Pan American additionally claimed it had FAA approval to do this even though the FAA insisted it did not. Investigation disclosed the presence of an extra bag when the flight left Frankfurt, which had not been physically searched. Also, as a direct consequence of the Lockerbie tragedy, the Air Carrier Standard Security Program (ACSSP) now requires both a positive match and an x-ray or a hand search of all checked baggage in specific designated countries.

11 September 2001

In an unprecedented act of massive terrorism, a hijacked commercial airliner, American Airlines Flight 11, was purposefully diverted to impact the north tower of the World Trade Center in New York City. A second hijacked aircraft, United Airlines Flight 175 from Boston, crashed into the south tower and exploded on impact. At approximately 9:17 AM the FAA shut down all New York City airports and the Port Authority of New York and New Jersey ordered all bridges and tunnels in the New York area closed. A few minutes later, the FAA halted all flight operations at all U.S. airports nationwide. For the first time in U.S. history commercial flight operations in the United States came to a screeching halt. On top of the devastation in New York, at 9:43 AM, American Airlines Flight 77 hurdled into the Pentagon in Washington, D.C. At 10:05 AM the south tower of World Trade Center collapsed, and five minutes later United Flight 93 was hijacked and crashed in Somerset County, Pennsylvania, after several passengers forcibly sought to reclaim the jet from

the hijackers. In another unprecedented move, the FAA diverted all transatlantic flights inbound from overseas to the United States to Canada. Suddenly, the 50 remaining aircraft still aloft in U.S. airspace was a cause of concern as possible targets of hijacking as well.

Soon thereafter, in a massive release of debris and smoke, the north tower of the World Trade center collapsed. Americans and members of 62 other nations lost friends and family in the ensuing devastation. Whatever the exact total loss of life amounts to, it was unbearable. That evening, Americans and the rest of the world learned that the well-coordinated, well-financed, and unfortunately well-executed attacks were likely the work of Usama bin Laden's al'Qaeda terrorist network. Apparently, three to five hijackers commandeered each aircraft armed simply with knives and box cutters.

Prior to the tragic events, there were clues; however, they were not adequately connected to prevent the attacks. In the April-May timeframe the government learned that Usama bin Laden's network was targeting the United States. In July 2001, the FBI advised law enforcement agencies of threats to U.S. interests overseas and domestically. Additionally, the Phoenix FBI office notified Washington that men of Middle Eastern heritage were attending flight schools in Arizona and that it was likely that Bin Laden was involved. About a month later, the CIA formally told the President that al'Qaeda operatives could be targeting the U.S. aviation industry. Soon thereafter, Zacarias Moussaoui was arrested in Minnesota on a visa violation. He had raised suspicions at an Eagan, Minnesota flight school after he was seeking training on a 747 jet but did not even have a pilot's license. Minnesota's FBI office was denied permission to search his computer. It was later found to contain references to al'Qaeda operatives in Malaysia and Germany, the 11 September hijackers, and crop dusting aircraft. On August 17, a Minneapolis FBI agent even surmised in a prophetic letter to headquarters that Moussaoui might be the type of person who would fly an aircraft into the World Trade Center. The National Security Agency had also intercepted messages the day before the attack referencing some big event but had failed to translate them until later in the week.

After the attacks, the President of the United States announced that the U.S. government will make no distinction between the terrorists who committed the acts and those who harbor them. Considering the horrific events, which were labeled "acts of war," a new war on terrorism began. The public was also made aware of the fact that the effort to combat all forms of terrorism will not be a short one. The consequences of the attack linger on with lawsuits, arguments over the fate of the impact site in New York, and traumatized people.

For example, former United Airlines flight attendant Deborah Jackson reached an undisclosed settlement with the airline after she accused her former employer of firing her after she could not work due to posttraumatic stress disorder (PTSD) following the 2001 terrorist attacks. Jackson, a flight attendant with United for 17 years, barely escaped being one of the flight attendants on one of the hijacked jets that slammed into the World Trade Center on 11 September. She was offered furlough after the event, which caused her to feel guilty because she was supposed to be on the doomed flight. She took the furlough, but when she was called back to work in 2005, she was again paralyzed with fear and unable to work. She asked for an extension of her furlough, but was fired in November of the same year. Jackson recovered from PTSD and asked the airline to rehire her, but so far the carrier has refused.

OTHER HIJACKINGS IN RECENT DECADES

1977: German GSG-9 storms a Lufthansa airliner in Mogadishu, Somalia, after a five-day standoff during which Palestinian guerrillas kill the pilot and three hijackers, while 86 hostages are freed.

1981: A Pakistan International Airlines jet is hijacked and taken to Kabul, Afghanistan where one passenger is killed. The plane flies on to Damascus; the hostages are finally released 13 days later when the Pakistani Government agrees to free more than 50 political prisoners.

1984: Two Americans are killed after Shia gunmen divert a Kuwait Airways flight to Tehran; the standoff ends six days later when Iranian security forces disguised as cleaners storm the plane.

1985: Fifty-nine people die when Egyptian commandos storm an EgyptAir plane seized by Palestinians and flown to Malta.

1986: Twenty-two people die when Pakistani security forces storm a Pan American flight carrying 400 passengers and crew after a 16-hour siege.

1988: Two Kuwaitis are killed in 1988 when Shia gunmen hijack a Kuwait Airways flight from Thailand and force it to fly to Algiers with more than 110 people on board. The hijack ends when the hijackers free the 16 remaining hostages.

1991: Singaporean commandos shoot dead all four hijackers who seize a Singapore Airlines flight.

1993: Two hijackers and a woman passenger die when security forces storm a hijacked Ethiopian Airlines plane in eastern Ethiopia.

1998: Pakistani commandos overpower and arrest three hijackers of a Pakistan International Airlines plane at Hyderabad airport; all 29 hostages are freed.

1999: Kashmiri militants hijack an Indian Airlines aircraft and force it to divert to Kandahar in Afghanistan; one passenger is killed, and a week-long standoff ensues before India agrees to release three jailed Kashmiri militants in exchange for the safe release of the remaining hostages.

February 2000: Afghans seeking to escape the Taliban regime hijack an internal Ariana flight with 164 people on board and force it to divert to Stansted airport near London. A three-day standoff takes place before the hijackers give themselves up without harming any of the hostages.

October 2000: Two Saudis seeking to highlight alleged human rights abuses in their country divert a Saudi Arabian Airlines plane to Baghdad before surrendering to the Iraqi authorities.

March 2001: Saudi Arabian security forces storm a Vnukovo Airlines plane at Medina airport after it is taken over by Chechen separatists during a flight from Istanbul to Moscow. More than 100 passengers and crew are freed, but three people—one of the hijackers, a Russian air stewardess, and a Turkish passenger—are killed.

CONCLUSION

As hijackings continued to increase, authorities explored the options available to them to combat it. The Federal Aviation Security Regulations were eventually proposed and implemented. The Federal Aviation Act of 1958 had to be amended accordingly. The regulations have repeatedly been amended to accommodate innovations in technology and to close previously missed loopholes. All sorts of alternatives to improve the program have been openly discussed over the years. Some have been adopted and some quickly and thankfully discarded. Eventually the public came to recognize that some drastic measures were required. Security programs, the Federal Air Marshal Program, and passenger screening were all initial attempts to control the threat at both domestic and international airports. It is still unsettled just how far the public and the courts will permit security officials to go to protect the air transportation industry, including both cargo and passengers, profiling being one of those methods continually being reviewed.

The U.S. government has repeatedly sought to maintain and upgrade security standards at airports. The early rules may have been implemented in haste, but they have subsequently been revised and amended to fill loopholes and improve security at the nation's airports. Initially, the rules met with significant resistance from the airlines and even from some consumer groups. However, the U.S. government has continuously sought to improve the safety and security of U.S. airports. Both

the Aviation Security and Improvement Act and the Federal Aviation Reauthorization Act of 1996 have appropriated money to be used in implementing the latest technology available in the field of airport security. Exactly who or what agency is responsible to foot the bill for the nation's airport security will remain under debate. The newest legislation addresses some of those questions, but not all. The airlines have repeatedly argued that terrorism is a threat to national security and should be addressed and financed by the government. The government, on the other hand, had insisted prior to 11 September 2001 that the cost of security is another cost of doing business in America and should be absorbed by the airlines, and hence the traveling public. Of note is the fact that the newest technology is also the most expensive technology.

The TSA is now challenged with overseeing the programs that assess whether airlines and airport operators provide adequate security measures at all airports. They assess both U.S. and overseas facilities. They also continue to propose changes to the federal regulations, as they deem appropriate. The most recent issues involve cargo, airmail, background checks on screeners, and explosive detection equipment. The government will also continue to assess the level of threat and to disseminate that information to the airlines.

Despite the hijackings of 11 September and interim efforts to place National Guardsmen at the nation's airports, significant long-term changes have yet to be fully implemented. Additional resources will have to be committed, and more analysis as to what will be successful in the future will need to be researched. The Aviation and Transportation Security Act of 2001 represents another knee-jerk reaction to air piracy. It was hastily enacted post 11 September and will likely undergo needed changes as certain realities set in.

Air piracy remains a security threat to international air travel. A constant trail of incidents evidences the point right up to the present. Repeated instances of hijacking over the years have proven time and time again that aircraft and airports are public, accessible, and somewhat easy targets for terrorists. They seek to publicize their cause and are guaranteed instant media coverage for their efforts. Politically volatile regions continue to produce emotionally driven terrorists who feel their actions are justified. Some very tragic results have been viewed by millions of people exposed to the media frenzies that follow major incidents. No geographic region has escaped the problem. However, responses from governments have varied from jurisdiction to jurisdiction. There is no question that additional hijackings or other forms of attacks will plague the aviation industry. As mentioned, new forms of using the transportation industry to disrupt the U.S. economy are likely. The use of aircraft to torpedo symbols of American democracy and strength were expanded to include not only hijacking and attacking airport terminals, but also to include commandeering aircraft to destroy major targets. The governments of the world are therefore challenged not only to provide adequate security at all airports, but also to address the underlying causes of the terrorism in the first place. The next chapter will explain the historical bases of these problem regions that generate terrorist conduct.

REFERENCES

Cashman, John, "Sky Marshals—-How They Train and What They Do," *Parade,* 19 November 1970, pg. 7.
http://www.dot.gov/affairs/aircraftsec.htm.
http://epic.org/foia_docs/airtravel/memo-10-16-02.pdf.
http://faa.gov.
http://www.faa.gov /avr/arm/nprm.cfm.
http://www.faa.gov/newsroom/factsheets/2002/factsheets_020905.htm.
http://www.gao.gov/new.items/d06374t.pdf.
Karr, Albert R., "Policing the Skies," *The Wall Street Journal*, Vol. II, No 238, 21 September 1971.
Simonsen, Clifford E. and Spendlove, Jeremy R., *Terrorism Today, The Past, The Players, The Future*, Prentice Hall, Upper Saddle River, N. J., 2000, pg 240.
Wardlaw, Grant, *Political Terrorism, Theory, Tactics and Counter Terrorism*, Cambridge University Press, London, 1982, pg. 38.
Williams, Major Louis, "Thunderball at Entebbe," *Israeli Defense Force Journal*, May 1985.

5 Terrorism
The Roots Remain

NEWS

January 2001: A trial begins in the Southern District of New York of four suspects in connection with the bombings at U.S. embassies in Kenya and Tanzania. Three of the four were extradited to the U.S. in 1999 to stand trial.

8 October 2001: Three small bombs explode in Zamboanga City in the Philippines, allegedly detonated by Abu Sayyaf, a group of Islamic militants with ties to Usama bin Laden.

May 2002: Spurred by concerns about terrorism, federal authorities are investigating whether private guards hired by major airlines in Los Angeles have smuggled passengers from the Middle East into the United States. The State Department also brands Iran and six other countries as promoters of terrorism: Iran, Sudan, Libya, Cuba, Iraq, North Korea, and Syria.

28 November 2002: A suicide bombing at the Israeli-owned Paradise Hotel near Mombasa kills 16 people, including the three attackers. On the same morning, a failed missile attack on an Israeli airliner taking off from Mombasa airport is carried out.

9 January 2003: Islamic Jihad claims responsibility for a suicide bombing that kills 17 Israelis, including 13 soldiers, at Megiddo junction in northern Israel. The attack prompts Palestinian Authority President Yasser Arafat to order the arrest of leaders of the militant group.

7 August 2005: This date marks the 7th anniversary when U.S. embassies in Nairobi, Kenya and Dar es Salaam, Tanzania were bombed. More than 200 Americans, Kenyans, and Tanzanians died in these attacks, and approximately 5000 people were injured. Mohamed Rashed Daoud Al-Owhali, Mohammed Odeh, Wadih el Hage, and Khalfan Khamis Mohamed are convicted of perpetrating the Nairobi bombing and are sentenced to life imprisonment without the possibility of parole.

INTRODUCTION

Throughout the world, terrorist organizations often threaten any possibility of peace among and within nations. Terrorism itself has a deep history, and when analyzed, each terrorist group has a unique historical view of its own. Whether groups hold emotional left-wing, right-wing, or single-issue perspectives, the problems for reconciliation are often slim. Each is similar in that they will fight mercilessly for their own causes. This fight has historically included many instances of hijacking, airport raids, and in 2001; commandeering aircraft for use as passenger, fuel-filled missiles.

The *sine qua non* of terrorism is the media. The airplane provides a capsule container of ready-made hostages, all organized, sitting in rows, strapped into their seats, and basically defenseless. Terrorists have sought frequently to exploit this made-to-order situation to publicize causes. From a terrorist's viewpoint, aircraft are a preferable target because of their international flavor and the likelihood the press will focus on the incident. Overall, most terrorist incidents in the United States have been bombing attacks involving detonated and un-detonated explosive devices, tear gas, pipe

bombs, and fire bombs. The targets are not limited to aircraft and airports, and the effects can vary significantly from loss of life and injuries to property damage and disruptions in services such as electricity, water supply, public transportation, and communications. The primary way to reduce vulnerability to terrorist attacks is by increasing security at airports and other public domains. The aviation industry, however, remains at particular risk.

Generally, the concept of terrorism has been defined as the use of force or violence against persons or property in violation of the criminal laws for purposes of intimidation, coercion, or ransom. No one definition has been universally accepted, and the diversity of the term defies one simple definition. The Federal Bureau of Investigation (FBI) categorizes terrorist activity as either domestic or international. Domestic terrorism involves groups or individuals whose terrorist activities are directed at elements of government or population without foreign direction. International terrorism involves groups or individuals whose terrorist activities are foreign-based and directed by countries or groups outside the United States or whose activities transcend national boundaries. The State Department defines terrorism as "premeditated, politically motivated violence against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience" (Title 22 USC Section 2656f(d)). Clearly, it is a difficult concept to express in one definition.

Ironically, the term terrorism first appeared during the years of the French Revolution (1789-1795). Edmund Burke, a British philosopher in the 1700s used the word to describe the political scene in revolutionary Paris. The violence became known as the "reign of terror" and applied to the conduct of the legal government at the time. The concept of terrorism has been around since the discovery that people can be influenced by intimidation. The earliest documented terrorist group was arguably the *Sicarii*, a Jewish group that used savage methods against the occupation force of the Roman Empire around 70 C.E. The Ismaili, or Assassins, lashed out against perceived religious oppression from the 11th to the 13th Century throughout the Islamic world. Today, the U.S. Congress requires the Department of State to provide Congress a full and complete annual report on terrorism regarding those countries and groups deemed involved in such activities. The law requiring the report was amended in 1996 to also require information on the extent to which other countries cooperate with the United States in apprehending, convicting, and punishing terrorists responsible for attacking U.S. citizens or interests. The report also contains information describing the extent to which foreign governments are cooperating or have cooperated during the previous five years in preventing future acts of terrorism.

Experts have attempted to differentiate the difference between historical terrorism and modern terrorism. According to many scholars, modern terrorists strike at governments by killing guiltless citizens, not just at government or military targets. For example, they strike at aircraft containing innocent noncombatants with no vested interest in the outcome of whatever political goal the terrorists are seeking. Simply put, modern terrorists sensationalize the murder of innocents, and capturing an aircraft encompasses a dramatic way of doing it. The causes behind the terrorism vary from region to region and country to country. To combat the problems, a basic knowledge of the issues, policies, and causes are important. The following sections summarize the historical reasons why many of the world's most notorious terrorist groups created themselves and eventually felt it necessary to jump from verbal rhetoric to violence.

CAUSES OF TERRORISM

Acts of terrorism directed at aircraft and airports were once again placed on page one of U.S. news reports in May 2001, when an Algerian terrorist admitted he was smuggling explosives across the United States-Canadian border back in December 1999. He had intended to attempt to blow up the Los Angeles International Airport. His conduct reinforced the concept that the threat was still significant, and authorities could not afford to relax security procedures already in place and enter into a state of apathy. Terrorism was documented as alive and well. In the interim, the threat continued to increase, although arguably without much notice by the public and not enough notice by the

authorities. For example, there were major clues that went unnoticed prior to 11 September 2001 that unfortunately were missed. Before discussing many of the groups actively engaged in terrorism, it is relevant to point out U.S. policy in negotiating with terrorists. The stated policy (Patterns of Global Terrorism—2000, April 2001) is as follows:

1. Make no concession to terrorists and strike no deals.
2. Bring terrorists to justice for their crimes.
3. Isolate and apply pressure on states that sponsor terrorism to force them to change their behavior.
4. Bolster the counterterrorist capabilities of those countries that work with the United States and require assistance.

A thorough understanding of the background of some of the most treacherous groups will assist students and practitioners in this field in efforts to remedy potentially dangerous and lethal situations. As mentioned, experts in the field have pondered the best definition of the term terrorism. Many agencies and scholars have sought a workable definition for their respective investigative purposes, and all agree it is an illusive term to pin down. The Omnibus Diplomatic Security and Anti-Terrorism Act of 1986 defines terrorism as the unlawful use of force or violence designed to intimidate or coerce a government or a civilian population in the furtherance of political or social objectives. Later legislation further defined a terrorist group as any organization that engages in, or has engaged in, terrorist activity as defined by the Secretary of State after consultation with the Secretary of the Treasury. Law enforcement agencies including the FBI, the Central Intelligence Agency (CIA) as well as the United Nations all have distinctive definitions that have been tailored to their respective missions.

MIDDLE EAST

The current crisis in the Middle East directly resulted from the political maneuvering by the West immediately preceding and during World War I. The Europeans sought to defeat Turkish influence in the area and to establish European footholds. To do so, they were willing to make promises they could not keep. At the turn of the century, the American naval strategist Alfred Mahan first coined the term Middle East. Since that time, the violence in the region has been extraordinary in the sense that it has had repercussions around the world and continues to do so. Many Westerners have failed to understand the basic historical, social, religious, and economic factors that are the cause of such violence. First of all, the region constitutes the focal point of three of the world's major religions. That fact alone provides the local populations, and the faithful living elsewhere, with the fuel to rapidly incite emotionally charged responses to all sorts of political and economic issues.

To better understand terrorism in the Middle East and the subsequent requirements to promote security at worldwide airports, one must first appreciate some highly pertinent historical turning points. For 30 years prior to the establishment of the State of Israel, the Middle East conflict was a constant drain on Great Britain's ability to protect its national interests. The results of European imperialism and intervention comprised one of the primary causes of the continuation of an almost express universal hatred of Israel in the region. Efforts to resolve the issues have always failed because the grounds for compromise acceptable to the parties involved have not been reached, and the superpowers have been either unwilling or unable to impose solutions from the outside. Both sides blame the other and pinpointing the real causes of the terror can be compared to the phrase deciding what came first: the chicken or the egg.

During World War I, the Turks were allied with the Germans. Consequently, the British encouraged the Arabs to revolt against the Turks. In return for this revolt, the Arabs were promised freedom. In reality, the British never really had any intention of ever granting full autonomy to the Arabs. In point of fact, the Europeans sought to carve up the riches of the region, especially oil reserves, and

create new imperial colonies. As history has shown, the British not only deceived the Arabs, they also misled the Jews. Partially in response to the Zionist movement, the British also promised the Zionists a Jewish homeland in Palestine. Meanwhile, at the other end of the geographic region, the British approached the Russians with a deal to divide modern Iran into three parts. The Russians were to control the northern part and the British the south, leaving only the center to the Iranians. When World War I ended, the Middle East had become a powder keg of competing interests. It remains so today.

RIVAL CLAIMS

For more than 50 years, the critical issue has been, and continues to be, who is entitled to live in the land historically called Palestine. Even though the British had verbally made a promise to the Arabs to support an independent Arab state, they did so without the consent of the French. The French had an independent set of goals and eventually signed the Sykes-Picot Agreement with the British that divided the Middle East into spheres of interest. In the alternative, the British also publicly issued the Balfour Declaration, promising Palestine as the future Jewish homeland.

At the end of the war, several traditional Arab families sought to unite Islam under a single banner. The result was the establishment of Syria, Iraq, Saudi Arabia, Jordan, Egypt, and Libya as the most powerful emerging Arab states. All considered the creation of a Pan Islamic state as a goal, but none of them was willing to concede its own chances to be the leading voice of this concept in the region. On top of traditional Arab families rivaling each other for control, Great Britain also acquired permission from the League of Nations to create the Protectorate of Transjordan. The British received their wish to be an influence in the Middle East, but it came at a hefty price. Neither the Arabs nor the Jews were satisfied with the arrangement. In addition, the insecure political atmosphere in the Arab states, born of many years of weakness, frustration, and mutual suspicion, precluded the emergence of even a moderate consensus among the Arabs.

It was tragic that the Arabs could not reach agreement among themselves even though it was clearly within the region's best interests. The tragedy was further compounded by the failure of the great powers at the time to help. The moral and diplomatic support given by President Harry S. Truman to Israel has proven to be shortsighted. It has had the effect of making a permanent moral commitment from the United States to the eventual State of Israel. Throughout the next several decades, although American presidents have sometimes opposed Israeli actions, when it comes to the fundamental question affecting the existence of the Israeli state, no American president has been in a strong enough position to call Israel's basic politics into question. The United States is still dealing with the repercussions of this initial commitment.

Both Jews and Arabs fought the British, but each envisioned a Palestine without the other. In 1936, the Arabs openly revolted. It was outwardly toward the British, but hatred of the Jews festered and grew. At the time of the Balfour Declaration, the actual population of Palestine was about 600,000 Palestinians and approximately 70,000 Jews. However, in late 1945, thousands of Jews sought a place to settle after the Nazi holocaust. The British had officially banned Jewish immigration, but pressure was building to open Jewish settlement of Palestine. The United Nations eventually partitioned the area in 1947 because the situation was, in reality, out of British control. Today, the Middle East is witnessing a reverse Zionism on behalf of the Palestinians who are insisting on the right to return to what they consider an ancient and traditional homeland.

Prior to 1947, the Jews were also in open revolt against the British. The Irgun Zvai Leumi, a Jewish terrorist organization, attacked both British soldiers and Arab Palestinians alike. Menachim Begin, founding member of the Irgun, masterminded an attack on the King David Hotel in Jerusalem in 1946. The explosion left 91 people dead. He went on to become a member of the Knesset serving from 1949 to 1984 and later performed as Prime Minister (George Rosie, *The* 1987). The Arabs formed terrorist groups as well. By 15 May 1948, the United Nations recognized the modern State

of Israel. The Palestinians, now themselves displaced, sought to get the land back by what ever means it took; including hijacking aircraft.

PALESTINIAN LIBERATION ORGANIZATION (PLO)

As discussed, much of the conflict in the Middle East started during the 1800s when revolts by nationalists, Turks, and Arab familial groups inflamed the region while they pursued individual interests. The conflict ultimately was a battle over who would control Palestine and who would be the voice of the Palestinians. The situation was further complicated by the thousands of Jews seeking a homeland after the Nazi Holocaust. When Zionists occupied Israel, the Palestinians fled traditional lands. Al-Fatah, later the Palestinian Liberation Organization (PLO), was born. After the Six-Day War in 1967, the Arab cause was in disarray. No one except the PLO was inclined to fight the Israelis. The PLO was prepared to fight back regardless of being underequipped and essentially being no match for the Israeli army. They attacked the Israelis in unconventional ways including "terrorist acts" against school children, farms, and whatever they could reach.

Initially, the PLO had organized and matured while members hid out in Jordan and clandestinely sneaked into Israel to raid settlements in the Gaza strip and West Bank. However, in a bold gesture, the Israelis struck back and attacked a small village known as Karamah. The Israelis were repelled with the help of the Jordanian Army. King Hussein of Jordan was not necessarily interested in protecting the PLO, but he was interested in protecting Jordanian sovereign territory from invasion. Afterward, despite the fact that he may not even have been present and his forces were really not victorious on their own, Yasser Arafat became a hero. He was born Abdel-Rahman Abdel-Raouf Arafat at-Qudwa al-Hussein. In time he would be viewed both as a revolutionary hero and as a bloodthirsty terrorist, depending on your perspective. Whatever your viewpoint, the PLO would bring violence and terror to the region.

Al-Fatah was made up of holy warriors or fedayeen. The founders included Yassar Arafat, Salah Khala, and Khalil Wazir. They were young, active, and humiliated after the 1967 Six-Day War. Its members did not often agree on how to respond to the perceived threat from Israel. Meanwhile, King Hussein was becoming more and more apprehensive about the PLO's continued presence in his country. Arafat, however, ignored the King's warnings to stop infiltrating Israel. In reality, Arafat increased his operations. In September 1970, after the PLO had successfully attacked civilians, hijacked aircraft, and assassinated quite a few people, King Hussein had had enough. Much to Arafat's surprise, King Hussein attacked the PLO and forced the organization to flee to Lebanon. The event became known historically as Black September.

Soon thereafter, a militant faction of the PLO assumed the same name, Black September, commemorating the eviction from Jordan. They eventually attacked the Israeli athletes at the Munich Olympics in 1972 and as a result were hunted down by the Israeli Mossad and assassinated. The conflict raged on for years with splinter groups seeking the assistance and support of rival Arab nations, all hoping to be the true voice of the Arab world. Many individuals within the PLO began to consider Yassar Arafat a liability, considering him soft on Israel. About this time, Iraq recruited Sabri-al-Banna, who later became known as Abu-Nidal. Abu-Nidal was to later lose his strictly Palestinian political motivations and turn mercenary. He even made several attempts on Arafat's life.

The overall situation defied compromise. The Israelis decided to forcibly remove the PLO from southern Lebanon and invaded that country. Thousands were massacred at Sabra and Shatila. Arafat once again was forced to flee. This time he went to Tunisia. Many experts at the time thought him finished; however, he was to repeatedly surprise everyone.

In 1987, the Intifada, or Arab, uprising took place. The uprising represented a spontaneous revolt by young Palestinians frustrated with life in refugee camps. The U.S. media, in reporting on the Palestinians pictured them as stone-throwing youths fighting heavily armed Israeli military members. The West suddenly viewed the Palestinian revolt in a more sympathetic light. The United Nations even recognized the PLO as the official representatives of the Palestinian people. The fast-paced

changes were too much for Arafat. In fact in 1988, he recognized Israel and denounced terrorism. On 13 September 1993, a Declaration of Principles between the Israelis and the Palestinians was signed establishing a tentative peace at best.

In 1993, PLO Chairman Yasser Arafat recognized the State of Israel in an official letter to its prime minister, Yitzhak Rabin:

> The signing of the *Declaration of Principles* marks a new era…I would like to confirm the following PLO commitments: The PLO recognizes the right of the *State of Israel* to exist in peace and security. The PLO accepts *United Nations Security Council Resolutions 242* and *338*. The PLO commits itself… to a peaceful resolution of the conflict between the two sides and declares that all outstanding issues relating to permanent status will be resolved through negotiations…The PLO renounces the use of terrorism and other acts of violence and will assume responsibility over all PLO elements and personnel in order to assure their compliance, prevent violations and discipline violators…The PLO affirms that those articles of the *Palestinian Covenant* which deny Israel's right to exist, and the provisions of the Covenant, which are inconsistent with the commitments of this letter, are now inoperative and no longer valid. Consequently, the PLO undertakes to submit to the *Palestinian National Council* for formal approval the necessary changes in regard to the Palestinian Covenant.

In response to Arafat's letter, Israel recognized the PLO as "the representative of the Palestinian people." Arafat was the Chairman of the PLO Executive Committee from 1969 until his death in 2004. He was succeeded by Mahmoud Abbas, or Abu Mazen.

Others were not to follow his leadership. The tangled web of Middle Eastern terrorism involves many more players than the members of the PLO. Terrorism was to continue and to repeatedly interfere with the peace process. Groups like Abu Nidal, Hamas, Hezbollah, and Islamic Jihad were to flourish. Any future negotiated peace settlement would always depend on the control or placation of still extremely militant factions active in the region.

ABU NIDAL

Names like Al-Iqab (the punishment), Al-Asifa (the storm), and many others represent one group named for a single leader, Abu Nidal. This group, known especially for its brutal acts of terrorism, has managed to survive nearly three decades. The group's history, ideology, and structure revolve around a Palestinian formerly known as Sabri-Al-Banna. Al-Banna, known today as Abu Nidal, was the sole leader and proprietor of a highly volatile terrorist organization.

Soon after Sabri entered the fourth grade, the Al-Banna family was forced from Jaffa as a result of the 1947 partition of Palestine and the fighting that followed. The family was eventually forced into a refugee camp after their homes and holdings were confiscated by the Zionist government. This experience was likely the driving force behind Sabri's violent and angry future. Later he joined the Ba'ath party of Jordan and the Fatah, both illegal in Saudi Arabia. He was eventually arrested, imprisoned, tortured, and expelled. After the 1967 Six-Day War, a formerly passive member of the Fatah turned into Abu Nidal, a master terrorist.

Within months of his arrival, Abu Nidal began to ignore directives from Fatah leaders. With the help of the Iraqis, he had established his own terrorist organization by 1973. In 1974, he was expelled from Fatah and sentenced to death for ordering an assassination attempt on Yasser Arafat. Nidal's defiance of the PLO was the result of Nidal's perceived laxness of PLO policies toward Israel. He was drawn to Baghdad because of its rejectionist approach to Israel. Using the resources provided by the Iraqi government, Nidal began his own terrorist campaign. Together, Nidal and the Iraqis rejected all peaceful attempts to resolve the Palestinian problem. In his first major campaign, he hijacked a British airliner enroute from Dubai to Tunis.

With the structure of his group in place, Nidal began to focus on his two main objectives. First, he wanted Israel destroyed, and second, he wanted the punishment of all those who disagreed with him. No one was safe. From his base in Iraq, his organization focused on the moderate Arab states

of Syria and Jordan, destroying embassies and assassinating Arab leaders. In the late 1970s, he moved his operation to Syria after being ejected from Iraq. He executed hundreds of terrorist acts both in Israel and Western Europe; targeting Israeli and Jewish sites. It is alleged that Abu Nidal had carried out operations in over 20 countries and caused the death of over 900 people. As part of this effort the group coordinated an attack at two major international airports, Rome and Vienna in December 1985. The group intended to discredit Arafat and the PLO. Later, after also alienating himself from the Syrians, he moved the entire operation to Libya, seeking financial support from Muammar Khadhaffi.

The group's most notorious attacks were on the El Al ticket counters at Rome and Vienna airports in December 1985, when Arab gunmen doped on amphetamines opened fire on passengers in simultaneous shootings, killing 18 and wounding 120. Patrick Seale, Abu Nidal's biographer, wrote of the attacks that their "random cruelty marked them as typical Abu Nidal operations" (Seale, 1992).

According to Atef Abu Bakr, a former senior member of the Abu Nidal Organization (ANO), Libya asked Abu Nidal to organize a series of revenge attacks against the United States and Britain, in cooperation with the head of Libyan intelligence, Abdullah al-Senussi. Abu Nidal allegedly suggested to Senussi that an aircraft be hijacked and destroyed. On 5 September 1986, an ANO team hijacked Pan American Flight 73 at Karachi Airport on its way from Bombay to New York. The gunmen held the hostages, 389 passengers and crew, for 16 hours in the plane on the tarmac before shooting and detonating grenades inside the dark cabin. Someone was able to open an emergency door, and passengers covered in blood tumbled down the vinyl chute; 16 died and over 100 were wounded. British media immediately reported in March 2004 that Libya was behind the hijacking (Melman, 1986).

As stated, Abu Nidal is considered by many as nothing more than a mercenary group. During the 1990s, Abu Nidal was reported to be dead or dying. It was also reported he had been captured by the Egyptians in 1998. The rumors were premature and the group continued to terrorize the Middle East although he had been behind the scenes for many years. However, in August 2002 he apparently died in Damascus, Syria. It was reported he had committed suicide, but it was unclear why the body had four bullet wounds. The explanation for his death more likely relates to orders from Saddam Hussein.

HAMAS

One of more militant groups still active is the Islamic Resistance Movement or Harakat-Al-Muqawama Al-Islamiyyah, also known as Hamas or literally translated from Arabic as "zeal." To its members the destruction of Israel is the only answer to the tenuous situation in the Middle East. They see Israel, and anyone that recognizes Israel, as the enemy, and they will never recognize any claims the Israelis have to also have a right to a homeland in Palestine. They represent a continuing struggle and one headquartered in the Gaza Strip. The Israelis incarcerated the founder, Aheikh Ahmed Yassin, in 1989 for killing Palestinians that collaborated with the Israeli Army. He was later released in a trade for two Israeli agents held in Jordan. It is composed of charitable, political (Al-Majd), and military (Izz Al-Din Al Qassam) elements. It originated in the 1980s as part of the Palestinian Muslim Brotherhood, another rejectionist organization; one that is not likely to relinquish its desire to be the voice not only of Palestine, but also of all the Arab peoples.

Hamas has grown to be the largest and arguably the most influential Palestinian militant movement. In January 2006, the group won the general legislative elections of the Palestinian Authority (PA), defeating Fatah, the party of the PA's president, Mahmoud Abbas, and creating a power struggle. Hamas has continued its refusal to recognize the state of Israel, leading to economic sanctions and a desperate psychological and physical struggle between the two entities. Hamas had maintained a cease-fire brokered in March 2005 until the whole tenuous relationship significantly deteriorated in June 2006 after some questionable conduct of the Israeli Defense Forces (IDF). The IDF denied any wrongdoing, but the cauldron had already boiled over.

As stated, Hamas grew out of the Muslim Brotherhood, a religious and political organization founded in Egypt with branches throughout the Arab world. It acted as a legitimate social services network for many years in conjunction with its more radical side clearly involved in terrorist activities in Gaza and the West Bank. In fact, Hamas devoted much of its estimated $70-million annual budget to funding schools, orphanages, mosques, healthcare clinics, soup kitchens, and sports leagues. However, after the first Intifada, Sheikh Ahmed Yassin, established al-Mujamma' al-Islami (the Islamic Center) as a political arm of Hamas in December 1987 to coordinate the Muslim Brotherhood's political activities in Gaza. Over the next six years, the distinctions between the PLO and other more radical groups like Hamas became even more evident. The first Hamas suicide bombing took place in April 1993, a mere five months prior to the Oslo accords.

Historically, Hamas has operated as an opposition group, but in its new role as the legislature's controlling party, the change has forced the group to reconsider the function and scope of its operations. Many had hoped that political legitimacy and accountability would push Hamas away from using violence to achieve its goals. But to date, the group has shown little interest in stopping the kidnappings and rocket fire that continue to draw Israel's ire. In general, the group's political philosophy combines Palestinian nationalism with Islamic fundamentalism. Its founding charter commits the group to the destruction of Israel, the replacement of the PA with an Islamist state on the West Bank and Gaza, and to raising "the banner of Allah over every inch of Palestine." Its leaders have called suicide attacks the "F-16" of the Palestinian people.

The Hamas movement considered Arafat a traitor. They support complete Israeli withdrawal from the occupied territories. Hamas has dispatched most of the 92 suicide bombers that have killed hundreds of Israeli's. They have the ability to perpetually disrupt any efforts for a peaceful compromise in the Middle East. They are well financed and extremely well organized. In 2002, they published the following statement on their website: "We call on the Arabs and Muslims to burn the land under the feet of the American invaders, especially our brothers in Saudi Arabia because this war is not against Iraq, it's against the Islamic nation" (Internet: http://www.hamas.org.uk/).

IRANIAN SUPPORT OF TERRORISM

The United States government maintains a list of seven foreign governments that they accuse of sponsoring international terrorism. Of those seven nations, Iran remains one of the most active sponsors of international terrorism. The sponsoring of international terror remains the main reason that Iran is still isolated from the mainstream international community to the degree that it continues to be. That reputation and the fear that Iran will provide nuclear capability to terrorists also raises the degree and level of world suspicion.

The roots of Iranian terror can be traced back to the Iranian revolution and the rise to power of the late Ayatollah Khomeini. Starting in the early 20th Century, Iran sought to be free of imperialistic rule. Fearing that if Iran went about eliminating imperialism incorrectly, they would become a communist state, the CIA and the U.S. government decided to help the Shah. Although Americans felt that they were helping Iran, the Iranian population "viewed America's actions as part of the long history of imperialism" (White, 1998). Because of how discontent his followers were becoming with the Shah's actions, the Shah created a secret police to destroy his enemies, the SAVAK. The SAVAK was one of the first Iranian-sponsored terrorist organizations. They would often kidnap the Shah's political enemies and either torture or murder them. The SAVAK was also famous for arresting and beating demonstrators. Often those demonstrators would be imprisoned for long periods of time. In what proved later to be a fatal mistake, one of those prisoners, Hojatalislam Khomeini would come back to haunt the Shah. Instead of executing Khomeini, the Shah had him deported to Iraq.

From Iraq, Khomeini's influence over Iran began to grow. While in Iraq, he ran a campaign to rid Iran of the Shah, and he was promoted to the rank of Ayatollah. After the election of Jimmy Carter as President, Khomeini increased his anti-Shah campaign because he felt the West held excessive sway over the Shah. About this time, Khomeini was forced to leave Iraq and moved his base of

operations to Paris. While in Paris, ironically he grew even stronger because he now had a direct phone connection to Teheran. Khomeini eventually returned to Iran in 1978, and by February 1979 he was in power. Once in power he initiated a "holy war against the West and the traitors to Islam (White, 1998).

An understanding of Islamic fundamentalism is critical to an understanding of Iranian sponsorship of terrorism in the Middle East. Some basic precepts include the following:

- Islam is the answer to all the problems of their society, country, and region. Relative weakness compared to the West; slow or stagnant economic development; the failure to destroy Israel; domestic and inter-Arab disunity, inequality, and injustice; and anything else are all due to the failure to implement Islam.
- Implementing Islam and resolving the huge problems of the people and states requires the seizure and holding of power by radical Islamic groups, and not by any other type of government or political group.
- The only proper interpretation of Islam is the one offered by a specific political group and its leaders (Rubin, 1998).

The religious views of Iran are only one of the reasons that Iran continues to be a sponsor of terrorism. By supporting terrorism through the 1980s, Iran gained important strategic, political, and economic assets. One of the main benefits resulted in the removal of American and French troops from Lebanon; enhancing Iranian standing in the Middle East and all over the Muslim community, at least from their perspective.

In 1996, while addressing officers of the Iranian Air Force, President Ali Kameini, was quoted as saying, "The government and people of Iran are of the opinion that the Israeli entity is false and artificial. In fact, there is no nation named Israel. The Zionists scraped together some people from all over the world, and based on racism, brought about the Zionist regime by virtue of the conquest of Palestine" (Israeli Foreign Ministry, 2000).

In March 2006, U.S. Secretary of State Condoleezza Rice said, "Iran has been the country that has been in many ways a kind of central banker for terrorism in important regions like Lebanon through Hezbollah in the Middle East, in the Palestinian Territories, and we have deep concerns about what Iran is doing in the south of Iraq" (http://www.cfr.org/publication/9362/). U.S. Director of National Intelligence Michael McConnell has mirrored this opinion by commenting in June 2007 that there is "overwhelming evidence" that Iran supports terrorists in Iraq and "compelling" evidence that it does the same in Afghanistan.

The Iranians will continue to export terrorism as long as they believe it serves the national interest. Historically, the U.S. government first listed Iran as a terrorist sponsor in 1984. For example, intelligence has supported the contention that Iran: had prior knowledge of Hezbollah attacks, such as the 1988 kidnapping and murder of Colonel William Higgins, a U.S. Marine involved in a U.N. observer mission in Lebanon, and the 1992 and 1994 bombings of Jewish cultural institutions in Argentina. Furthermore, Iran still has a price on the head of the Indian-born British novelist Salman Rushdie for what Iranian leaders call blasphemous writings about Islam in his 1989 novel *The Satanic Verses*. It has also been alleged that Iran supported the group behind the 1996 truck bombing of Khobar Towers, a U.S. military residence in Saudi Arabia, which killed 19 U.S. servicemen.

More importantly, Iran has hundreds of Scuds and other short-range ballistic missiles. It has also manufactured and flight-tested the Shahab-3 missile, which has a range of 1300 kilometers. Moreover, Iran is developing missiles with even greater range, including one that could be used to launch satellites or used as an intercontinental ballistic missile. In March 2006, Iran claimed it had successfully tested a missile capable of evading radar and of hitting multiple targets.

HEZBOLLAH

No terrorist organization in the world has received more assistance from Iran than Hezbollah. The International Policy Institute for Counter-Terrorism describes the group as the "spearhead for Iran in its use of terrorism in general, and its fight against Israel in particular" (Ranstorp, 1994). Each year, Hezbollah receives millions of dollars from the Iranian government to help what they believe is the legitimate struggle against Israel. Some have estimated the support to reach levels of 80 to 100 million dollars every year.

Hezbollah's main goal specifically focuses on ending Israel's occupation of southern Lebanon. Israel had become militarily involved in Lebanon in attempting to rout the PLO, which had moved into southern Lebanon after the Jordanian Army evicted the group from sanctuary in Jordan. The PLO had been attacking Israel from southern Lebanon in the lead-up to the 1982 Lebanon War, and as a result Israel had invaded and occupied southern Lebanon. Hezbollah has repeatedly attempted to drive Israel completely out of Lebanon over the past several decades. Initially, the group used suicide attacks against the IDF and against Israeli targets just outside of Lebanon.

Hezbollah eventually evolved into a paramilitary organization and became equally equipped as one, including having Katyusha and other types of rocket launchers in addition to other types of sophisticated weaponry. The group now functions as a regular military engaging in activities considered by such groups as Amnesty International and Human Rights Watch as war crimes against Israeli civilians, much like the IDF has been accused of war crimes against Lebanese civilians. The battle continues to be an emotional one on both sides.

Supporters of Hezbollah justify Hezbollah's attacks as legitimate retaliation for Israel's occupation of Lebanese territory, Israel's aggression in the Middle East, and in furtherance of defensive jihad. Many of these attacks took place while Israel occupied the southern part of Lebanon and seized it as a security zone despite U. N. Security Council Resolution 425, although Israel did withdraw from Lebanon in 2000, as later verified by the United Nations. To complicate matters further, Lebanon now considers the Shebaa farms, a 26 km² (10-mile²) piece of land captured by Israel from Syria in the 1967 war to be Lebanese territory.

The United States, Israel, and a few other countries consider Hezbollah wholly or partly a terrorist organization. The European Union does not list Hezbollah as a "terrorist organization," but does list the late Imad Mugniyah, a senior member and founder of Hezbollah, as a terrorist. (Council Decision, 2005). In 1985, Hezbollah's manifesto, contained in "An Open Letter: The Hezbollah Program," proclaimed the three objectives of the organization as the following:

- To expel Americans, the French, and their allies definitely from Lebanon, putting an end to any colonialist entity on our land.
- To submit the phalanges to a just power and bring them all to justice for the crimes they have perpetrated against Muslims and Christians.
- To permit all the sons of our people to determine their future and to choose in all the liberty the form of government they desire. We call upon all of them to pick the option of Islamic government that alone is capable of guaranteeing justice and liberty for all. Only an Islamic regime can stop any future tentative attempts of imperialistic infiltration into our country.

Since its inception in the 1980s, Hezbollah is attributed with conducting the following acts of terrorism:

- April 1983 U.S. Embassy bombing
- 1983 Beirut barracks bombing in which 241 Marines were killed as they slept
- Numerous kidnappings of Western, especially American, targets and 41 suicide attackers killing 659 people

- 1985 hijacking of Trans World Airlines Flight 847 by a group with alleged links to Hezbollah
- 1992 Israeli embassy attack in Buenos Aires, Argentina
- 1994 AMIA bombing of a Jewish cultural centre in Argentina
- 15 January 2008 bombing of a U.S. embassy vehicle in Beirut

Hezbollah is also active in the United States. FBI agents arrested 18 Hezbollah supporters in North Carolina in July 2000. An FBI affidavit said investigators were searching for evidence that the defendants were providing resources to the terrorist group. The resources included night-vision goggles, global positioning systems, and digital photo equipment and computers. The goal of Hezbollah is to establish an Islamic state in Lebanon (Yonah, 1994). As stated, Hezbollah efforts were and are completely supported by the government of Iran, still controlled by radical Shi'ite clerics. They represent an additional wild card in the region, capable of disrupting any efforts toward peace. Additionally, they have recently been tied to the al'Qaeda organization.

AFGHANISTAN: USAMA BIN LADEN

Usama bin Laden is discussed separately from the other Middle Eastern terrorists because of his uniqueness (see Figure 5.1). He is an Arab who headquartered in Afghanistan, but his cause is purely anti-Western. He was born into a wealthy Saudi family and is the 17th son of 52 children and attended Abdul Aziz University. While at the University, he was influenced by one of his instructors, Sheikh Abdallah Azzam, who was extremely disenchanted with the alleged corruption of the PLO. Bin Laden along with Azzam was interested in the intertwined worlds of Arab politics and religion. The Soviet Union's invasion of Afghanistan embroiled bin Laden in a guerilla conflict backed by Saudi money and U.S. weapons. He became an ardent anti-Western advocate and a seasoned combat veteran.

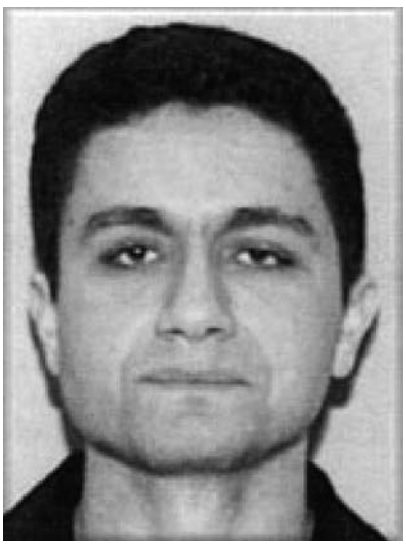

FIGURE 5.1 This FBI mugshot of Mohammed Atta was released Wednesday 11/12/01. It was taken from a State of Florida, Division of Motor Vehicles photo. Atta is one of two men who received flight training in Florida and was one of the master minds behind the 9/11 attack.

Bin Laden's father, Mohammed bin Laden, moved his family from Yemen to Saudi Arabia and gradually built the largest construction company in the country. In turn, the Saudi royal family gave the bin Laden family exclusive rights to all construction of a religious nature, whether in Mecca, Medina, or Jerusalem. From this background, Usama somehow became obsessed with the U.S. presence on the Arabian Peninsula. Bin Laden believes that the United States has been occupying the lands of Islam in the holiest of places, including Jerusalem, Mecca, and Medina. The goal for bin Laden is to unite all Muslims and to establish an Islamic government in the entire Middle East. When the war against the Soviets in Afghanistan ended, bin Laden was seen generally as a leader of religious fundamentalists who oppose non-Islamic governments.

In the mid 1990s he cofounded an organization with Azzam named the Maktab-al Khidamat (MAK). Allegedly, the MAK acted as a recruiting center and clearinghouse for Islamic charities worldwide, but it has a more sinister quieter goal directly related to terrorism. Unbelievably, the MAK had offices in Detroit and Brooklyn. Bin Ladin has since issued a fatwa or religious decree against the United States. (Chen and Eberhardt, Internet: http://www.apbonlin.com/newscenter/majorcases /binladen/index.html). The Fatwa makes it the duty of every Muslim to kill Americans and their allies. They are instructed to do it in any country in which it is possible to kill to liberate the Alqsa Mosque and others from the grips of the West.

In 1989, a car bomb killed Azzam. The extremist faction of MAK directly allied with bin Laden's efforts, and they relocated to the Sudan. After being associated with several terrorist events, bin Laden was stripped of his Saudi citizenship. The Sudan eventually expelled him under pressure from the West, after which he relocated his entire organization (al'Qaeda) back to Afghanistan. The Taliban regime protected him for years. Despite efforts by the United Nations to force the Taliban government to assist in his apprehension, they failed to do so. Pressure was increased after the bombing of two U.S. embassies in Africa. It later became clear that he was behind the World Trade Center bombing in 1993 and the attack on the U.S.S. Cole in Yemen. The conviction in May 2001 of four members of the group responsible for the U.S. African embassy bombings bolstered the U.S. government's legal battle to bring down bin Laden. Barry Mawn, the assistant FBI director in charge of the New York office said after the trial, "The verdict puts on notice any individual or group of individuals who seek to attack U.S. persons or interests abroad, that the rule of law is more powerful than any terrorist bomb" (Jones and Moorem, 2001). The 1998 bombings of the U.S. embassies in East Africa marked the declaration of jihad that sparked a relentless campaign aimed at the indiscriminate killing of Americans.

The World Trade Center bombing in 1993 and the convictions of others charged with plotting to plant bombs around New York City revealed that the international terrorist threat within the United States was more serious and more extensive than before. The events of 11 September 2001 made this a certainty. Bin Laden has a well-organized and extremely well-financed organization with an infrastructure still capable of attacking targets inside the United States. Those infrastructures also still include airports (GAO/RCED-94-38, 1994). The group likely acquired its real operational sophistication around 1998 when it merged with other radical groups. For example, it significantly strengthened its ties with the Armed Vanguards of Conquest, an Egyptian cell of extremists whose leader, Ayman al-Zawahri, was involved in the assassination of former Egyptian President Anwar Sadat in 1981. Perhaps the most lethal turn in bin Laden's criminal and terroristic conduct was his decision to financially and logistically support the efforts of these other groups. U.S. intelligence now speculates that Mohammed Atta was likely one of the prime coordinators and initiators of the 11 September attack. He had taken his plan to al'Qaeda and bin Laden, and his senior advisors had approved and supported it (see Figure 5.2).

He has since been indicted in United States federal court for his alleged involvement in the 1998 U.S. embassy bombings in Dar es Salaam, Tanzania and Nairobi, Kenya, and is on the U.S. FBI's Ten Most Wanted Fugitives list. Although bin Laden has not been indicted for the 11 September 2001 attacks, he has claimed responsibility for them in videos released to the public.

FIGURE 5.2 Saudi dissident Usama bin Ladin in an undisclosed location inside Afghanistan before the fall of the Taliban regime. He remains elusive and on the top ofthe world's most wanted list for his part in the September 2001 attacks in New York and Washington as well as elsewhere. (Source: FBI Most Wanted List)

Numerous claims as to the location of bin Laden have been made since December 2001, although none have been definitively proven, and he has repeatedly been in different locations during the same timeframes. Specifically, a 11 December 2005 letter from Atiyah Abd al-Rahman to Abu Musab al-Zarqawi indicates that bin Laden and the al'Qaeda leadership were based in the Waziristan region of Pakistan at the time. In the letter, translated by the U.S. military's Combating Terrorism Center at West Point, "Atiyah" instructs Zarqawi to "send messengers from your end to Waziristan so that they meet with the brothers of the leadership … I am now on a visit to them, and I am writing you this letter as I am with them…" (Combating Terrorism Center at West Point, 2006).

Reports alleging his death have circulated since late 2001. In the months following the 11 September terrorist attack, many people believed he was indeed dead, based on his documented serious health problems. Regardless, as of 2008, the FBI continues efforts to locate and apprehend him. The Rewards For Justice Program, U.S. Department of State, is offering a reward of up to $25 million for information leading directly to his apprehension or conviction. An additional $2 million is being offered through a program developed and funded by the Airline Pilots Association and the Air Transport Association.

EUROPE

Germany

By the 1960s, the threat of terrorism unfortunately had spread beyond the Middle East. Some of the most dramatic terrorist events took place in Europe, where transition from authoritarian rule to democracy after World War II had been traumatic to say the least. The terrorists sought to bring about the collapse of European governments and hoped to establish a new order based on the teachings of Karl Marx and Mao Tse Tung.

During the 1970s, terrorism in Europe was one of the greatest scourges facing both the United States and its NATO allies. Marxist groups, anxious to spread their message, engaged in a campaign of killings and terror attacks against civilian and military targets. One of these groups in Europe, the West German Red Army Faction (RAF), or the Baader-Meinhof Gang, originated among a group of militant extremists at the Free University of Berlin. Students, Andreas Baader, Gudrun Ensslin, and Ulricke Meinhof joined together and agreed on a campaign of direct action. They repeatedly robbed banks and kidnapped and assassinated political leaders as well as wealthy business leaders. Most notably they cooperated with Palestinian terrorists in the murder of Israeli athletes at the Munich

Olympic Games and with the hijacking of an Air France plane to Entebbe, Uganda. The German police slowly began to close in on the gang, and the Baader-Meinhof gang would begin a cycle of collapse and rebirth extending into the 21st Century.

Born out of the student protest movements of the 1960s, the RAF was a contradiction unto itself. Although the creators of the RAF espoused the downfall of capitalism, they were generally the children of successful and wealthy parents. The RAF eventually became a model on which new generations of terrorist groups would base new organizations.

The RAF launched itself in the summer of 1967 when Andreas Baader and Gudrun Ensslin met. While Baader was a purported thief and protestor, Ensslin was a leader of student protest movements. On 2 April 1968, the two young revolutionaries had begun a reign of terror by bombing upscale department stores in Frankfurt. Instead of staying in Germany, however, the group eventually traveled to Jordan, where they received a variety of training. On returning to Germany, the Baader-Meinhof Gang again began robbing banks, causing both fear and panic in Germany, especially among the banking industry.

Although Baader and Ensslin were the masterminds behind the criminal operations, Meinhof was nonetheless able to spur the cause through her literary talent. In 1971, Meinhof wrote *The Concept of the Urban Guerilla*, a mixture of strategic and tactical doctrine for terrorist activities in cities. Although the ideas may not have been entirely original, formulating them in one comprehensive manual was. The doctrine for asymmetric warfare discussed in the manual is still used today, providing would-be terrorists with a concise manual designed for achieving devastating results on a budget with limited resources.

At the same time as Meinhof began writing the manual, the Baader-Meinhof Gang officially became the RAF. Although the name change may seem purely aesthetic, it actually meant a broader change for its members. For the first time, the RAF could now publicly support its cause of Marxist revolution, rather than portraying itself as a group of small-time criminals. Although as quickly as the RAF adopted its new name, the German police, frustrated with uncoordinated and unsuccessful efforts to catch the group, formed the Bundeskriminalamt (BKA), or Federal Criminal Investigation Office. For the German people and its government, the creation of the BKA was a dynamic shift in domestic policy. For the first time since World War II, Germany now had a unified federal policy agency, with more power and discretion than local departments. This was the first time the allies permitted the Germans to have a unified national police force since the downfall of the Nazi regime and the SS.

In some ways, the creation of the BKA was exactly what the RAF wanted. Part of the manual stipulated that the short-term goal of terrorist activities was to force the government to take repressive measures. To the people of Germany, terrified of the not forgotten historical examples of a strong, unified police force, the creation of the BKA should have evoked feelings of resentment and fostered a sense of rebellion toward the government. However, just the opposite happened. Instead of the public despising the government, it fully supported efforts to stop the activities of the RAF. The RAF had overstayed its welcome, and the novelty of its purported cause had worn off.

As the BKA began to close in on the RAF, an all-out war ensued through 1971 and 1972. Over the course of 1971, shootouts between the police and members of the RAF were a monthly occurrence, with both sides taking casualties. In the month of May, five separate bombing incidents shocked the citizens of Germany and the American servicemen stationed in the country. Of the five incidents, two were directed at American installations. The speed and stealth with which the bombings were carried out demonstrated the resolve of the RAF and the effectiveness of their tactics.

Devastated by the ferocity of the RAF's attacks, the BKA began to use radical tactics to close in on the leaders. The public, scared and tired of the RAF, supported the actions of the police. Finally, in June, after months of searching for the leaders, the police managed to catch Baader, Meinhof, and Ensslin. In 1975, following the imprisonment of the leaders of the RAF, the Baader-Meinhof laws were passed, repressing the rights of prisoners and defendants in Germany. Although the laws

represent the type of repressive measures the RAF wanted, the people of Germany again supported the government's tactics despite the threat to personal civil liberties of the German people.

In September 1977, desperate to free the RAF leaders, the remaining members of the group kidnapped Hans-Martin Schleyer, a wealthy businessman and president of the Employers Association. In an attempt to amplify earlier kidnapping successes, the RAF began conducting joint operation with Palestinian terrorists. Meinhof eventually committed suicide, and Baader and other leaders shot themselves after a rescue attempt by their compatriots failed. Following the death of the RAF leaders, the remaining members of the group executed Schleyer, and the group started to disintegrate. Regardless, the group continued to exist, and in the 1980s it refocused itself on an anti-NATO campaign with a new generation of terrorists. Trying to regain their previous status, they attempted several terrorist acts with Action Direct (a French terrorist group), bombing three NATO buildings in the 1980s. After the fall of the Berlin Wall and the reunification of Germany, the public continued to largely ignore and disapprove of the methods behind the RAF's messages.

The group again gained momentum in the 1990s after a member of the Grenzschutzgruppe-9 (GSG-9), an elite counterterrorist unit, executed a captured RAF member after he had been arrested. In 1993, to further demonstrate that it was still capable of attacks and was still alive, the RAF destroyed a brand new women's prison. Although the attack was a success, the perpetrators behind it were captured soon after the attack. It appeared that the RAF was breathing its last breath even though renewed anti-American and anti-NATO attitudes remained strong in Europe.

Later, efforts to round up left-wing terrorists in Europe were enhanced by the uncovered files of the East German police, the Stasi, after the fall of communism in Eastern Europe. The Baader-Meinhof Gang, or RAF, no longer presents a viable threat; however, its terrorist activities greatly contributed to public support for various governments around the world to enhance airport security. For many years, pictures of the members of the group were posted in public places throughout Germany and the world. Their legacy includes the beginning of permanent implementation of stringent airport security measures and a national police force for Germany.

Italy

Italy has experienced a decline of terrorism, at least from radical left terrorists as opposed to Mafia-type acts of terror. In Italy, the Red Brigade launched brutal attacks on politicians, police, and journalists. The most widely publicized attacks resulted in kidnapping and murder of former Italian Prime Minister Aldo Moro and the kidnapping of Brigadier General James Dozier. The founders of the group, Renato Curcio and Margherita Cagol, were students in the sociology department at Trent University, and they sought to make the cities of Italy unsafe. Originally, the group was mostly centered in Milan. Later, the group was thought to have approximately 500 members and another 1000 passive supporters. The Italian Red Brigade eventually disintegrated as police arrested most members of the group. However, like the Baader-Meinhof gang the group seemed to repeatedly rise from the ashes. The vestiges of the group continued its left-wing objectives even after the demise of its original leaders. They even conducted a series of terrorist attacks in reaction to efforts by Italian law enforcement to arrest leading Mafia figures.

Italian terrorist groups had literally perfected the art of kidnapping, somewhat with the help of Italian insurance companies who were willing to issue insurance against such events. The kidnapping of the leader of the Christian Democratic Party, Aldo Moro, turned the nation against the group. Moro was a creature of habit and followed exactly the same route to work everyday. He was easily ambushed on 16 March 1978. The well-organized attackers shot his five bodyguards. Italy's firm policy of "no deals" with terrorists, which ironically had been introduced by Moro himself, forbade the Italian government from negotiating for his release. Moro, 54 days later, was found dead in the trunk of a car in Rome. The Red Brigade had also kidnapped Brigadier General James Dozier, then Deputy Chief of Staff of NATO. He had admitted some professed "plumbers" to his apartment after which they captured him. He was held in Padua above a grocery store. In an extremely

well-executed rescue attempt, he was eventually freed. It was the beginning of the end for the Red Brigade (Gutteridge, 1986).

Spain

The struggle for independence and autonomy is something that the Basque people have been fighting for since the Sixth Century. At that time, the Visigoths drove the Basque tribe into the mountainous regions of north-central Spain. The Basques were a very unique and individualistic people and are said to be the oldest surviving ethnic group in all of Europe. The Basque country (Euzkadi) remains located in the northern region of Spain and southwestern France. Historically the area dominated by these people encompassed seven different provinces, four of which are in Spain. Although the Basque of France are struggling for survival, the Basque of Spain are flourishing in a wealthy and expanding industrial economy. The Basque people make up about five percent of the population, but remarkably produce about ten percent of the country's exports.

Student activists established the ETA, Euskadi Ta Askentasuna, in 1959. With loose ties to Marxism, the group wished to create an independent homeland in Spain's Basque region. Prior to this, Generalissimo Francisco Franco closed all Basque schools and newspapers, and even outlawed the Basque language. In 1937, he enlisted the help of Hitler's Luftwaffe and demolished the Basque historic city of Gernika. The Spanish Civil War took the lives of 50,000 Basques and sent another 300,000 more to prison and exile.

General Franco died in 1976, and a new democratic government came to power. The Basques regained some lost autonomy. However, the ETA sought complete independence. They turned violent in 1968 and separated into political and military branches. Members have ordinary jobs during the week as lawyers, academics, and journalists. Unique among most terrorist organizations, they engage in terrorist activity usually only on weekends. One author has stated, "Most members only engage in terrorism for three years…before returning to their full-time occupation" (White, 1998).

Clearly, the ETA constitutes a highly structured and organized unit. In 1997, the ETA was listed by the U.S. State Department as one of the best organized terrorist groups in the world (Internet:http://www.ict.org.il/, 1999: pg.1). At the time, the ETA had about 20 hard-core members and hundreds of supporters. According to self-produced publications, the ETA targets, "the oppressive symbols of the Spanish State." Additionally, the ETA was armed, trained, and supported by the Russian KGB during the Spanish civil war. After Soviet aid stopped, it was rumored that Muommar Khaddafi has been supplying the ETA with assistance.

Allegedly, the Grupos Anti-terroristas de Liberacion (GAL) existed for many years as a covert police operation set up to kill members of the ETA. From December 1983 to February 1986 a series of assassinations and kidnappings were undertaken in which 27 people were killed and another 30 injured by activities of the GAL. After many changes within the Spanish government and changes in policy toward the Basques, the Basque people would eventually be able to use the Basque native language, maintain aspects of a unique culture, and even have representation and participation in the Spanish Parliament. Such accommodations have greatly reduced tension in the area, but they are still relatively high. Anxiety is still prevalent, and the ETA has also become quite proficient at attacking airports. Their intent was to disrupt tourist flights along the coast during the summer season, scaring thousands of vacationing Spanish tourists. In one incident, after sending warnings to the local papers, the ETA put one of three explosive devices in a paper bag inside the airport's woman's bathroom. All together 24 people were injured.

Over the years, the ETA and the Spanish government have negotiated several ceasefires. In the interim, a "counterterrorist" law put suspected terrorist cases under a central tribunal, Audiencia Nacional in Madrid. Under Article 509 of the Spanish penal law, suspected terrorists are now subject to being held "incommunicado" for up to 13 days, during which they have no contact with the outside world at all.

In 1992, ETA's three top leaders were arrested in a northern Basque town, which led to changes in ETA's leadership and direction. However, after a two-month truce, ETA adopted even more radical positions and began to menace leaders of other parties besides rival Basque nationalist parties. In 1995, the armed organization again launched a peace proposal, even though the proposal accompanied a failed ETA car bombing attempt directed against a conservative politician who was leader of a then-opposition party and an abortive attempt on the life of King Juan Carlos I. Later a prominent council member was kidnapped and his death was threatened unless the Spanish government would bring all ETA's inmates to prison within the Basque Country within two days after the kidnapping. After enormous public demonstrations seeking the councilman's release, the demand was not met by the Spanish government, and he was found shot dead when the deadline expired.

Soon thereafter, ETA declared a unilateral truce or ceasefire and began a process of dialogue with Spain's government. The dialogue continued for some time, but ETA resumed assassinations in 2000, accusing the government of being "inflexible." Later acts of violence such as the 6 November 2001 car bomb in Madrid, which injured 65, and attacks on soccer stadiums and tourist destinations further alienated the group from the Spanish public. The 11 September 2001 attacks dealt another hard blow to ETA, owing to the toughening of "antiterrorist" measures, the increase in international police coordination, and the end of the toleration some countries had, up until then, extended to ETA. With ever-increasing frequency, attempted ETA actions have been frustrated by Spanish security forces and condemned by the Spanish people.

Northern Ireland

Even though the Irish Republican Army (IRA) has not been known to routinely hijack aircraft, they constitute a major terrorist organization and deserve some attention in the study of airport security. Additionally, although Ireland is one large landmass, it is split into two sections, north and south, both by the diversity of its people and by British mandate. The Irish Republicans, primarily Catholics, occupy the South, and the Unionists, primarily Protestants, reside in the North. The split has existed since the Reformation and continues today.

Ireland's history was filled with turmoil for hundreds of years after the Normans conquered Ireland, subjugating the Irish to British rule. The Protestant Reformation in the 1500s had long-lasting consequences that are still felt in Ireland today. The Reformation was brought about by Henry VIII to allow him to divorce his wife and remarry, after which he hoped to secure the thrown with a male heir. He established the Church of England, which was pretty much rejected by the Irish but embraced by his daughter who eventually became Queen Elizabeth I. She started an English colony known as the Plantation of Ulster in Northern Ireland and granted titled lands to wealthy British and Scottish subjects, thereby displacing native-born Irish from the region.

In the years from 1845 through 1848, Ireland experienced what became known as the potato famine. Millions died, and millions more emigrated. Shortly after the famine, the British proposed a series of home-rule plans. The Unionists who lived in Northern Ireland were opposed to home rule because Northern Ireland was the center of power, and they felt that Ireland would be destabilized. The Republicans, mainly Irish Catholics in southern Ireland, were in favor of home rule, but their wishes were never realized.

In 1916, the British again proffered a plan to grant Ireland home rule. The Unionists and Republicans each feared the opposing side would gain the upper hand. Admittedly, by 1916, Britain had their attention focused on Germany. During Easter 1916, Patrick Pearse and James Connolly led a revolt against the Unionists and British. The Easter rebellion was a huge surprise to the British who were heavily engaged in World War I. Even though the rebellion had successfully taken over some federal buildings in Dublin, the revolt was doomed to failure. The Irish wanted home rule, but the British brutally put down the revolt, which they considered treasonous considering the timing. The Irish Republican Brotherhood surrendered and, as per the surrender document, became known as the Irish Republican Army from that day forward. The people of Ireland originally held Pearse

FIGURE 5.3 The two main dissident groups, which developed after splits within the Provisional IRA, are the "Real" IRA (RIRA) and the Continuity IRA (CIRA). RIRA set the bomb in Omagh in 1998. Ireland remains divided and the seeds of continuing violence persist in spite of diplomatic efforts to conclude this chapter in Ireland's history.

and Connolly responsible for the destruction of Dublin by the British. After defeating the Irish, however, the British military executed the Republican leaders they had captured; creating martyrs for the Republican cause. This proved to be a gigantic mistake. Due to the harshness of the British response, the IRA enjoyed a renewed popularity.

Later, the Provisional IRA developed into an organized, sophisticated, and effective terrorist group. By October 1972, they had allegedly killed 132 British soldiers, and by May of the same year the number had risen to 214. In response, on Bloody Sunday, 30 January 1972, British soldiers killed 13 protesters who were marching in a civil rights parade. The IRA continued the violence by responding in kind. On 21 July 1972, 22 bombs were planted in Belfast, killing nine civilians. With both sides exhausted with the violence, in 1981, Gerry Adams attempted to get the IRA to engage in less violence and more political discussion. The first cease-fire began in August 1994. The British insisted the IRA disarm. Because they refused, the attempted cease-fire lasted only until February 1996 (see Figure 5.3).

In December 1997, the Irish Republican leadership finally met with the British Prime Minister in still yet another attempt to stop the violence. Sinn Féin eventually began participating in a Northern Irish government in December 1999. However, Britain suspended the new government in 2000 and again in 2001 over the IRA's refusal to agree to disarm. In 2001, the IRA allegedly began disarming in secret. A number of incidents in 2002, though, yet again indicated that the IRA had not abandoned paramilitary activity, and home rule was once again suspended. In July 2005, the IRA announced it was ending its armed campaign, and in July, 2006, the British and Irish governments indicated that they believed the IRA also had really taken steps to wind down its paramilitary operations.

The IRA remains well armed and financed. They are also involved in international activities, most recently with FARC in Columbia. Additionally, in August 2002, three suspected IRA members were arrested in Colombia on charges of assisting FARC in improving its explosives capabilities. Formally, most of the IRA's money came from illegal activities including racketeering, extortion, and blackmail. The group's extensive criminal activities reportedly provided the IRA and the political party Sinn Fein with millions of dollars each year. Despite the efforts of many, the IRA was implicated in two significant robberies in 2004, one involving almost $50 million.

Throughout Irish history, the people have been invaded, subjected to foreign rule, and have had little to say about how they have been governed. The IRA, since its inception has taken hundreds of lives to obtain its goal, and now that they have an opportunity to attain it, they refuse to surrender their weapons out of mistrust. This may stem from the way violence has become a way of life for

the Irish people. Violence is glorified in murals, song, and poetry, and martyrs of the IRA's cause are seen as heroes. Despite the repeated instances of terrible tragedy on both sides, the violence continues, somewhat unabated.

JAPAN

The Japanese Red Army (JRA) is a terrorist group that sought the fastest, simplest means to achieve its goals. The JRA had a ruthless and somewhat successful history. Formed out of the 1960s anti-Vietnam War movement, the JRA promoted the end of capitalism influenced by the United States. The group based its philosophy on a mix of feudal Japanese samurai warrior customs and Marxism. In 1971, a young former member of the Japanese Red Army Faction (JRAF) named Fusako Shigenobu broke from the group along with fellow radical Tsuneo Mori. Parting because the JRAF focused more on a national revolution, Shigenobu aimed for a more global transformation in forming the JRA.

As she established her separate goals, Shigenobu decided to relocate in Lebanon's Bekaa Valley to establish closer contacts with the Popular Front for the Liberation of Palestine (PFLP). In doing so, the JRA now relied almost entirely on the PFLP for funds, arms, and training. However, Shigenobu had a central plan to promote the JRA's self-sufficiency by implementing the group's capabilities as terrorist guns-for-hire.

In 1972, the JRA performed its first and perhaps most notorious venture at the Lod Airport in Tel Aviv. Three members, armed with hand grenades and machine guns, attacked the airport in a suicide mission, killing 26 and wounding 78 people in the joint JRA-PFLP mission. Establishing a ruthless reputation, the JRA proved itself in battle and continued its notorious rampage to achieve more funding through several more hijackings. The JRA moved on to extort millions from the French and Japanese governments through such hijackings between 1973 and 1977.

Later in 1988, the JRA attempted an ambitious plan to initiate simultaneous attacks on U.S. military targets both in Europe and the United States to mark the second anniversary of a U.S. air strike against Libya in 1986. This previous U.S. air strike had targeted Tripoli and Benghazi as a result of Libya's purported involvement in terrorist attacks on a West Berlin club popular with U.S. soldiers. Libyan leader Colonel Muommar Khadaffi had turned to the JRA for help, desperate for revenge. However, the plan to simultaneously bomb U.S. military targets failed when a New Jersey police officer arrested JRA veteran Yu Kikumura while enroute to bomb a U.S. target.

The last major JRA incident occurred in Naples in 1988. Shigenobu herself was captured on 8 November 2000 in the small Japanese town of Takatsuki, near Osaka, after she had been on the run for over 30 years. She was charged with suspicion of conspiracy related to her participation in the seizure of the French embassy in The Hague in 1974. She was also charged with attempted murder and passport fraud. While facing the charges of terrorism and passport fraud, Shigenobu announced in April 2001 that the JRA was disbanding. She also declared that she intended to pursue her goals through legitimate political means rather than violence. In February of 2006, she was actually convicted of kidnapping and attempted murder; receiving a 20-year jail term. The JRA was removed from the U.S. State Department's list of Foreign Terrorist Organizations in October 2001. Shigenobu has one daughter, Mei Shigenobu, whose father is Palestinian.

Four other members were returned to Japan in March 2000 after being deported from Lebanon. The Japanese charged them with attempted murder and forgery of official documents. A fifth member of the group, Kozo Okamoto, was not extradited because he received political asylum from Lebanon for his participation in terrorist acts against Israel. However, Yoshimi Tanaka was successfully extradited from Thailand and charged with hijacking a Japanese Airlines plane to North Korea in 1970. As the JRA seems to currently be an inactive terrorist group, their strong beliefs persist among dwindling JRA members.

Aum Shinrikyo

Aum Shinrikyo, most notably, conducted the sarin nerve agent attack in the Tokyo subway on 20 March 1995, becoming one of the first groups to use a chemical agent in a terrorist attack. Members carried sarin; a deadly nerve gas originally produced by the Nazis, in two or three small plastic bags each. They released it into five different subway cars. The plastic bags were covered with newspaper and later punctured by umbrellas to discharge the agent. In 1999 and 2000, a Tokyo court eventually sentenced 11 members of the group to death. An additional participant received a reduced sentence. The professed religious cult leader, Shoko Asahara, claimed to be a reincarnation of the Hindu god Shiva and promised to lead his followers to salvation when impending Armageddon arrived. He also was finally found guilty, and sentenced to death in February 2004. The Supreme Court threw out his final appeal in September 2006. The group has apologized and agreed to pay $40 million in damages to the victims of the attack.

Aum members were not individuals seeking social release or some nebulous political revenge; they were an organized religious cult trying actively to destroy the Japanese government. They included, among many others, a middle-aged surgeon, three physicists, and an electrical engineer, some very bright and educated minds (White, 1998). Their compound, located near Mt. Fuji, included a building known as Satyam 7, which was a large three-story prefabricated structure for the "secret work" of the science unit. The building contained millions of dollars of highly advanced equipment, most of which was purchased openly in the United States.

Cult members received extensive military training. They were also extensively brainwashed. Within the group there existed a strict spiritual hierarchy. Simply joining made the initiate a Zaike, or member, and then the pressure was on to become a Shukke, who theoretically could use supernatural power. Shoko Asahara, the self-professed leader, was supposedly the most enlightened of the group and also head of the vast corporate empire behind the business of religion, including a chain of computer stores (Internet: http://www.pals.msus.edu/cgi-bin/pals-cgi…142/te%20%shinrikyo/di%200001/txt).

Ashara was arrested in 1995 at the headquarters near Mt. Fuji. He was hiding alone in a dark space about the size of a coffin. Police searched for hours before locating a hollow wall containing a hidden compartment about ten by three feet. He had a cassette player, some medicine, and $106,000 in cash. His arrest does not stop the threat from the technological terrorist. Even though technological terrorism is not the course of action of a rational actor, lack of rationality is no barrier to successful terrorist attacks. This was a group that had combined religious eschatology with violence supported by high-tech weapons; a seriously dangerous hybrid. The conduct of this group represents a window on what is to come. It is a loud and clear warning for airports and airport security to be better equipped to handle potential biological, chemical, and maybe even nuclear attacks.

LATIN AMERICA

Tupac Amaru (MRTA)

Terrorist activity has continued in Peru but declined sharply despite the fragile state of the government after the precipitate resignation of President Fujimori. The Tupac Amaru Revolution is a Peruvian Marxist-Leninist revolutionary movement started in 1984 by organizations from the radical left. Its stated objective is to rid Peru of imperialism and establish a Marxist regime. The group, which is estimated to have between 300 and 600 members, operated mainly in the Upper Haulage Valley, a vast jungle area in eastern Peru controlled mostly by guerillas and drug traffickers. Its activities include bombings, kidnappings, and assassinations. They have been known for anti-American sentiments.

MRTA was named for the 18th Century rebel leader who fought the Spanish in attempting to acquire freedom from oppression and colonialism. The goal of the current organization was to replace the representative democracy with the power of the people; a leftist concept. They launched

the armed struggle in San Martin province, where conditions were in their estimation most favorable. In 1987, they were even able, for the first time, to take over a provisional capital, Juan, a city of approximately 25,000 inhabitants.

In addition, Peruvian forces captured their leader, Victor Polay, in 1992. In a rather defiant event, his supporters attacked the Japanese Ambassador's residence in Lima in 1996. Four hundred guests had just sat down for a meal when over a dozen men stormed the compound. The situation was delicate, to say the least; considering all the foreign diplomats involved. Nonetheless, President Fujimori steadfastly refused the terrorists' demands to release Polay. After a four-month crisis, Peruvian special security forces tunneled into the compound. Within less than an hour the terrorists were dead, and the hostages were freed. The group has not conducted a significant terrorist operation since. As of 2002, they have remained focused on obtaining the release of several MRTA members still imprisoned in Bolivia.

However, in September 2003, four Chilean defendants were tried and convicted of membership in the Túpac Amaru Revolutionary Movement. They had allegedly participated in the kidnapping and murder of hostages at the Peru–North American Cultural Institute in 1993. Later, Peru's Truth and Reconciliation Commission determined that the group was responsible for approximately 1.5 percent of the deaths investigated. In its final findings published in 2003, the Commission observed the following:

> Unlike Shining Path, but like other armed Latin American organizations with which it maintained ties, the MRTA claimed responsibility for its actions, its members used uniforms or other identifiers to differentiate themselves from the civilian population, it abstained from attacking the unarmed population, and at some points showed signs of being open to peace negotiations. Nevertheless, MRTA also engaged in criminal acts. It resorted to assassinations, such as in the case of General Enrique López Albújar; the taking of hostages; and the systematic practice of kidnapping, all crimes that violate not only personal liberty but the international humanitarian law that the MRTA claimed to respect. It is important to highlight that MRTA also assassinated dissidents within its own ranks (La Comisión de la Verdad y Reconciliación. 28 August 2003. Final Report).

Additionally, on 22 March 2006, Víctor Polay, the former guerrilla leader of the MRTA, was found guilty by a Peruvian court of nearly 30 crimes committed during the 1980s and 1990s. The embassy compound incident, however, reminds security forces everywhere that diplomats are high-risk targets for those seeking immediate media attention.

Shining Path (Sendero Luminoso)

There were two main rebel groups operating in Peru in the 1980s to 1990s, both leftist: the Maoist Shining Path (known in Spanish as *Sendero Luminoso*) and the Cuban-inspired Tupac Amaru Revolutionary Movement (*Movimiento Revolucionario Tupac Amaru*) just discussed. Peruvian authorities captured one of the last remaining commanders of the Shining Path in April 2000. Jose Arcola Chiloquin or Romano led some significant terrorist acts, mostly in the Upper Haulage Valley where the group continued efforts despite the loss of the leadership. Their founder, Abimael Guzman, received his indoctrination and training in China at the start of the Chinese Cultural Revolution. After returning to Peru, and as a university professor, he was working on research regarding the exploitation of the Peruvian Indians when he recruited his students into the Maoist Party and sent them out to "agitate." (Dillon, 1998). Since that time, he led a highly successful insurgent group bent on creating a classless society in Peru.

The group was particularly vicious in their tactics. They were known to use children to deliver bombs to public buildings and police stations; children who were of course killed in the ensuing explosions. Guzman had created a cult-like atmosphere, and he became known locally as the Fourth Sword of Marxism *The Economist*, 1996). His dream fell apart when he was captured in 1992.

Terrorism in Latin America persists due to poverty, unequal land distribution among segments of the population, and, of course, repressive regimes.

Former Peruvian President Alberto Fujimori waged an aggressive and highly successful campaign against Shining Path and Tupac Amaru. Fujimori, although originally elected, seized near-dictatorial powers in April 1992 and disbanded Peru's congress and courts. He claimed they were limiting his ability to crack down on terrorism. Within a few years, Fujimori had captured most of the leaders of the rebel groups, and terrorism subsequently declined sharply. Thousands of Peruvians were convicted of terrorism-related charges and sentenced to life imprisonment by military courts. Human rights activists accused the Peruvian military of committing widespread human rights abuses during the crackdown, including the jailing of thousands of innocent Peruvians. By the turn of the century, Peru's constitutional court struck down the antiterror laws enacted under Fujimori. Thousands of jailed members of the Shining Path were given the right to request retrials in civilian court, including the group's leader Abimael Guzman.

Although the organization's numbers had lessened by 2003, a militant faction of Shining Path remains active. The government claims that they are simply criminal and are operating in alliance with drug traffickers. In addition, in 2003, the Peruvian National Police broke up several Shining Path training camps and captured many members and leaders. They also freed about 100 indigenous people held as slaves. By late October 2003, there were 96 terrorist incidents in Peru, projecting a 15 percent decrease from the 134 kidnappings and armed attacks in 2002. Attacks have continued through 2007. Shining Path and Tupac Amaru have no known ties to Usama bin Laden's al'Qaeda network, but the danger remains that they will bring their causes to the United States.

RUSSIA

Whereas terrorism is looked on by many as "senseless acts of violence carried out by madmen," there are many instances in which it is brought on by great injustice. According to one author, "A core element in any account of terrorism is that it involves the use of violence to achieve political ends" (Taylor and Quay, 1994). It is not simply a tool used by a single individual to retaliate or eliminate on a personal level. Most terrorist acts have deep-rooted histories that are so in depth and sensitive that no one outside the group can really relate to the feelings that cause people to commit these acts. Like the old saying goes, one person's terrorist is another person's freedom fighter.

To fully understand what is really happening in the Russian-Chechen conflict, one must recognize the history of the region. Chechnya is located in the Caucasus Mountains along its northern slopes. Before the 1994 to 1996 war, Chechnya had a population of about 1.2 million, including 400,000 ethnic Russians. Although this area represents only a sliver of Russian territory, it is strategically located on the route of oil from the Caspian Sea to Europe.

The root of the problems between the Russians and the Chechens goes back as far as three centuries. By 1585, the region had been incorporated into the Ottoman Empire and had adopted Islam. In the early 1700s, Tsar Peter the Great invaded the area and claimed it as part of all the Russias. Between 1785 and 1792, the Moslem Chechens began to rise up against the Eastern Orthodox Russians when the Cossack settlers moved into the region in large numbers. During the first half of the 1800s, Chechnya was one of many groups of Islamic rebels trying to win independence. The Chechens, in fact, led a holy war against Russia as early as 1834 to 1859. They again rebelled during the Russian civil war after 1917. In 1934, the Chechens joined with neighboring Ingusheita to form an autonomous republic. However, Stalin deported 600,000 of them to Siberia and the Far East before World War II. It is documented that nearly 200,000 of these people perished on the way. Stalin feared the Chechens would welcome the Germans and hinder the Russian war effort. The survivors of the exodus were not allowed to return home until 1957, when Nikita Khrushchev finally permitted it. When they did return, they quickly discovered the ethnic Russians had taken over much of their valuable land.

On 2 November 1991, newly elected President Dzhokar Dudayev, a former Russian Air Force General, proclaimed Chechen independence. In response, Russian President Boris Yeltsin announced a state of emergency and sent troops. The Chechens mobilized 60,000 volunteers to retaliate, and the war dragged on through 1996. The Russians have retreated but have not politically given into any Chechen demands. In frustration, the Chechens have turned to terrorism. The hostility of the Chechen people toward Russia is deeply rooted. The viciousness of the war only intensifies the problem and will not be easily ameliorated.

Acts of terrorism continue today, including several hijacking efforts. In December 2002, Chechen rebels took 700 people hostage in a daring terror attack on a Moscow theater that would end with 128 hostages dead, many as a result of the Russian rescue effort. This is significant because the Chechen people believe the world has forgotten them. Former CIA director George Tenet had speculated that Chechnya was breeding a new generation of terrorists who threaten the West, just as many Afghanistan-bred fighters in the 1970s and 1980s went on to become foot soldiers for al' Qaeda. Consequently, air piracy appears to them to be a reasonable means by which to return to the headlines. Another perplexing problem pertains to the former Soviet Union's nuclear stockpile. Clearly, they have been unable to account for all of it. In the hands of terrorists, this provides a powerful tool whether they actually have the weapons or not. The threat is enough.

To gain attention, Chechen terrorists hit a school in Northern Ossetia on the first day of school. On "First September" of every year in every school in the Russian Federation, teachers and students celebrate a holiday known as the "Day of Knowledge." The children are commonly accompanied by parents and dressed especially for the day. In 2004, on First September at School Number One in Beslan, Chechen terrorists attacked parents, teachers, and students alike, resulting in hundreds of people wounded or killed. Most of the attackers wore black ski masks and carried explosive belts. After an exchange of gunfire with police, in which five officers and one perpetrator were killed, the attackers seized the school building taking more than 1300 people hostage. Most hostages were under the age of 18. A security cordon was soon established around the school, consisting of Russian police and army forces, Spetsnaz, including the Alpha antiterrorist team and members of *Ministerstvo Vnutrennih Del* (MVD, or Ministry of Interior Affairs)'s OMON unit. The Russian government initially said that it would not use force to rescue the hostages, and negotiations toward a peaceful resolution did take place on the first and second days.

Eventually, however, Russian Special Forces activated a plan to storm the school to rescue any possible survivors. A massive level of force was used including the regular army and Interior Ministry troops as well as helicopter gunships (including Mi-24 Hinds and Mi-8 Hips) and at least one tank. Many local civilians also joined in the battle, having brought along personal weapons. Regardless, the incident is indicative of the high emotions that paint this Russian-Chechen conflict and the extremes to which terrorists will go to publicize their cause.

Furthermore, the Russian government confirms the involvement of international terrorists and specifically Usama bin Laden associates in Chechnya, in part, experts say, to generate Western sympathy for Russia's military campaign against the Chechen rebels. Of the approximately 200 Islamist militants in Chechnya, the most prominent was Shamil Basayev. He had become Russia's most wanted man, but, on 10 July 2006, he was killed in an explosion in Ingushetia, a republic bordering Chechnya. His death was a severe blow to the Chechen separatist effort. Russian Defense Minister Sergei Ivanov has supported this claim by releasing a videotape of Khattab meeting with bin Laden that had been found in Afghanistan. Most experts put the number of foreign militants in Chechnya at approximately 200 out of several thousand fighters.

U.S. DOMESTIC TERRORISM

The concept of domestic terrorism in the United States changed dramatically after the bombing of the Alfred P. Murrah building in Oklahoma City (see Figure 5.4). The incident proved that it does not take a significantly large number of people to affect history. The United States has seen

FIGURE 5.4 This photo of the devastated Murrah Building was taken in Oklahoma City, OK on April 26, 1995 following the Oklahoma City bombing. (Source: FEMA News Photo)

its own proliferation of prolife terrorists, militias, white supremacist organizations, and environmental terrorists just to name a few. However, since 11 September, hate groups and other anti-government groups have used the horrific events to recruit new members. Additionally, foreign terrorists seek to bring causes to U.S. soil. Either way, security personnel need to study the threat and be prepared.

The Order

The Silent Brotherhood, or "the Order," was formed in September 1983 and was officially known as the Order Bruder Schweigen. Robert Jay Matthews formed the group in upstate Washington. Matthews, whose drive was to "quit talking and start acting" for total Aryan victory, led the group into becoming the most dangerous underground group since the Ku Klux Klan in a little under 15 months (Internet: http://www.front14.org/rac/theorder2.htm). The Order is one of the most well-known right-wing extremist groups in America and is best characterized as neo-Nazi and racist. They consider themselves very patriotic and have labeled themselves as redneck, white skin, and blue collar.

Members of this group believe that God chose white Europeans to be leaders of the Aryan nation. They claim to follow the "14 words" (we must secure the existence of our people and a future for White children). With Matthews as leader, the Order set out on a grand plan. They would exterminate the Blacks, kill all the Jews, and drive the enemy into the sea. They are bound to follow the "88 precepts" as written by David Lane, a follower. Some teachings include the following:

- Any religion or teaching that denies the natural laws of the universe is false.
- In accordance with Nature's laws, nothing is more right than the preservation of one's own race.

- The white race has suffered invasions and brutality from Africa and Asia for thousands of years…so the attempted guilt trip placed on the white race by civilization's executioners is invalid under both historical circumstances and the natural law that denies inter-species compassion.
- The concept of a multiracial society violates every natural law for species preservation.

The group was not opposed to violence. They recorded the largest armored car robbery in history, with the holdup of a Brinks car and the acquisition of $3.8 million. During the Brinks holdup, leader David Matthews dropped a pistol that was traced to another order member's house. Additionally, one of the member's turned FBI informant. Matthews was tracked down, and in a firebombing incident, he was burned alive. After his death, many of his followers were arrested. The continued existence of this particular group is in dispute. The proliferation of white supremacist groups around the globe is not. In a 1999 shooting at a California Jewish community center, the gunman claimed to be a member. Regardless, it is well accepted that much of the $3.8 million continues to fund the activities of white supremacist groups. The Aryan Nation, Militia of Montana, and many other extremists associated with right-wing groups and special interest groups will persist in challenging security officials.

NUCLEAR TERRORISM

Most Americans are well aware of the fact that terrorists are capable of executing a nuclear, biological, or chemical attack against the United States. However, most Americans are also very apathetic about the possibility. In 1996, a nationwide survey found 72 percent of the population believes there is a chance that terrorists could use a weapon of mass destruction to attack a U.S. city, but only 13 percent worry a great deal about this, and 27 percent are somewhat worried. A full 59 percent profess not to be worried at all (Internet: http://www.fas.org/irp/threat/terror.htm). Times have changed considerably.

The issue of mass destructive terrorism has caused concern to an unprecedented degree in the post-Cold War era. It is the argument of such scholars as Gavin Cameron that the real driving force behind the heightened danger of nuclear terrorism lies not with the increased opportunities for proliferation, but rather with the changing nature of political violence and the psychological and organizational characteristics of terrorism itself. To date, there have been few incidents of mass destruction, and no major nuclear terrorism. The question for analysis is, given the conservatism of most terrorist groups, will they make the leap to nuclear, chemical, or biological weapons. Setting the theoretical debate aside, after 11 September, the U.S. Coast Guard set up security zones around at least two nuclear power plants to prohibit ships from approaching the plants. Critics persist, however, in warning that many nuclear-powered plants remain vulnerable.

Modern technology has opened the doors to this new wave of terrorism. Most primitive weapons have been replaced with sophisticated silent and deadlier ones. The emergence of the computer as a technological device associated with terrorism is a rather new phenomenon whereas the use of chemical and biological weapons has been around a while longer, although they have been significantly enhanced. It is recent technological innovations that have made them more viable weapons. The sheer volume of such activities and their destructive potential makes these kinds of terrorism more problematic. One of the most important points about any analysis of terrorism is why the numbers of incidents are down, yet the lethality has reached frightening degrees (Hoffman, 1994). Those responsible for airport security must recognize the threat and prepare accordingly.

After the collapse of the former Soviet Union, the black-market for atomic materials was prevalent and dangerous but thought to be disabled by the Russian authorities. An incident in 2003 and then another in 2006, wherein a Russian uranium dealer was arrested, has renewed security concerns about Russia's nuclear black-market. Corruption continues to be rampant, and the political situation in Russia has resulted in a resurgence of both the gray- and black-markets. Officials have confirmed that the nuclear materials seized originated from Russia. The suspects arrested in each

case corroborated to Georgian investigators that they procured the uranium through a network of Russian contacts and middlemen of various nationalities.

Furthermore, five former U.S. nuclear weapons designers, in cooperation with the Nuclear Control Institute, completed a study that concluded that a sophisticated terrorist group would be capable of designing and building a workable nuclear bomb from stolen plutonium or highly enriched uranium, with potential yields in the kiloton range. The probability of such an event, particularly in light of documented attempts by al'Qaeda to acquire nuclear material and nuclear-weapon design information, must be taken seriously. Despite claims to the contrary from plutonium-fuel advocates in the nuclear power industry, experts agree that effective and devastating weapons could be made using "reactor-grade" plutonium, hundreds of tons of which are processed, stored, and circulated around the world in civilian nuclear commerce (Internet: http://www.nci.org/nci-nt.htm). Several scenarios are possible:

A Dirty Bomb

A radiological dispersion bomb offers the most accessible nuclear device for any terrorist. This so-called dirty bomb would consist of waste by-products from nuclear reactors surrounded by conventional explosives that on detonation would disperse deadly radioactive particles into the environment. This represents a highly practical weapon in that radioactive waste material is much more easily obtained than weapons grade material. As is well known, radioactive waste is widely found throughout the world and is clearly not as well guarded as viable nuclear weapons. In the United States alone, radioactive waste is located at more than 70 commercial nuclear power sites, in 31 states. Enormous quantities also exist overseas. In Russia, security for nuclear waste is especially poor, and the potential for diversion and actual use by Islamic radicals has been shown to be very real. In 1996, Islamic rebels from the break-away province of Chechnya allegedly planted, but did not detonate, such a device in Moscow's Izmaiylova open-air bazaar to demonstrate Russia's vulnerability.

Attack on Nuclear Power Plants

Many people deny the possibility that a terrorist attack on a commercial nuclear power plant would detonate the core of a reactor. However, the feasibility of a meltdown of any reactor core (similar to the Chernobyl disaster), or a dispersal of the spent fuel waste on the site, would still result in extensive casualties. If such an event were to occur, the power plant would be the source of radiological contamination, and the plane or armor would be the explosive mechanism for spreading lethal radiation over extensive areas.

Diversion of Nuclear Material or Weapons

The above-mentioned scenarios, however, pale in comparison to the possibility that terrorists could build or obtain an actual atomic bomb. Potentially, millions of people could be killed by combining the devastation of an original blast and the ensuing death from exposure to radiation. Even a low-yield bomb would kill hundreds of thousands of people and cause enormous fear. For example, a relatively small bomb, say 15 kilotons, detonated in Manhattan could immediately slaughter more than 100,000 inhabitants, followed by a comparable number of deaths in the lingering aftermath. Massive quantities of fissile material exist around the world, and it is questionable how well guarded it is.

BIOLOGICAL AND CHEMICAL WARFARE

Building or stealing a weapon of mass destruction is a difficult, complex, and risky task, but the basic technical requirements for building biological and chemical weapons are well established and

not difficult to acquire. Biological and chemical weapons are actually becoming fairly easy commodities to access. The materials, equipment, and expertise necessary to use them are no longer a significant challenge for today's sophisticated terrorists. The latent ability of terrorists to build or use weapons of this type is also increasing (Burck and Flowerree, 1991). In the aftermath of 11 September, Secretary of Defense Donald Rumsfeld publicly announced that the United States was taking seriously the possibility that terrorists might launch an attack of this sort. The threat has never dissipated and lingers as a serious risk.

For example, the FBI ordered crop-dusting planes to be grounded for 24 hours on 23 September 2001 and urged agricultural pilots to be vigilant of any suspicious activity they observed. Former Secretary Rumsfeld also reiterated that state sponsors of terrorism have very active chemical and biological warfare programs. Biological agents are much deadlier than their chemical counterparts, and the effects are longer lasting. The lethality of biological weapons is such that ten grams of many different kinds of available agents could produce over one million deaths. Biological weapons challenge the conventional modes of thinking about the contemporary terrorist threat and indicate another degree to which technology has transformed terrorism.

The assumption of traditional terrorism was that a small number of casualties would have a dramatic impact on the much larger general audience. Modern terrorists now seek to kill large numbers of innocent victims in a single blow. Among the most readily available biological agents is anthrax. It is extremely lethal, and contact causes an 80 percent mortality rate. Documented cases of criminals attempting to sell the agent have been repeatedly documented (Staten 1998). Fatalities at an airport would be momentous; ranging from thousands to tens of thousands, assuming an effective dissemination of the agent and the absence of timely, effective medical care.

Although the production process for chemical weapons is longer than that of biological weapons, chemical weapons can be designed to kill much faster. Binary weapons constitute one of the most significant developments in the evolution of chemical weapons of terrorism. These devices consist of a chemical for which individual components may be stored separately. When the components are assembled, the elements are combined for an agent of great lethality. These binary weapons ease the storage risks for the terrorists and with proper engineering enable the terrorist to remove themselves from the threat area. Technology has put at the terrorist's disposal a varied array of very lethal and definitely indiscriminate weapons. The sarin toxin gas released in the Tokyo subway was only a sample of what is likely to come.

CONCLUSION

To succeed, terrorist operations require detailed information for planning and executing an attack. If an airport asset is the target, terrorists can often acquire sufficient information to plan the attack by simply visiting the airport and testing its security procedures. Access is generally considered not to be difficult to achieve. In fact, the whole purpose of an airport is to provide an open environment for passengers to travel and move freely from one destination to another.

One private pilot, expressing his views on the Internet, claimed, "I have yet to encounter an airfield I could not enter" (Fries, Internet: http://www.flyer-online.com/Articles/flyer). He believes that fences pose no obstacles to would-be intruders and that airport operators have little interest in constructing good ones. He reasons that a fence provides nothing in financial return to the airport tenant. He repeated the story,

> The closest I came to having a fence stop me was at Duluth International Airport late one winter night. No one was home when I landed. Even the tower had closed. The gates were all locked and welded shut by the ice. However, airport plows had conveniently piled snow mountains on both sides of the fence. I simply climbed up on the snow, stepped across the fence and descended the packed snow of the other side.

Additionally, the events of 11 September seemed to represent the ultimate attack. However, continuing attacks are not a question of if but when, as has now been often repeated. The lesson for Americans is undeniable, and to believe that just because several years have passed translates into safety and security is simply foolish. Usama bin Laden and his organization intend to continue to engage in terrorist acts against Americans in America and elsewhere. For example, not long after 11 September 2001, Richard Reid, a British citizen, attempted to blow up American Airlines Flight 63 from Paris to Miami with a bomb in his shoe. In all likelihood he was not acting alone, and some of the detainees in Guantanamo Bay claimed to recognize him from al'Qaeda training camps in Afghanistan. On 22 December, only 3 months after the tragic events in New York, Washington, D.C., and Pennsylvania, he tried to board the aircraft with 10 ounces of PETN- based material, similar to Semtex. Repeated acts of terrorism have ensued around the globe with no end in sight.

This chapter has really provided only a cursory review of some of the more famous terrorist organizations at play, both in the past and at present. There are numerous others. There are even terrorists who consist of either a party of one or a very small cellular group. Timothy McVeigh, who bombed the federal building in Oklahoma City and was executed in 2001, was just such an individual. He could have easily chosen an airport as his primary target, even though he had mistakenly chosen the Murrah Building as the source of decision-making regarding the Branch Davidian incident at Waco, TX.

REFERENCES

Burck, Gordon M. and Charles C. Flowerree, *International Handbook on Chemical Weapons Proliferation,* New York: Greenwood Press, 1991.

Chen, Hans H, and Eberhardt David, "Web of Terror" Bin Ladin's International Terror Network, http://www.apbonlin.com/newscenter/majorcases /binladen/index.html.

Combating Terrorism Center at West Point, "Letter Exposes New Leader in Al-Qa`ida High Command," 25 September 2006.

Council decision of 21 December 2005 implementing Article 2(3) of Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism and repealing Decision 2005/848/EC(2005/930/EC.

Dillon, Sam "As Peru Votes, Insurgent's Mystique Casts Shadows," *Miami Herald*, 10 June 1998, pp. 1 A, 26 H.

Fries, Ian Blair, http://www.flyer-online.com/Articles/flyer, pg 1.

GAO/RCED-94-38, 27 March 1994.

Gutteridge, William, *Contemporary Terrorism*, 1986, pg. 127.

Hoffman, Bruce, "Responding to Terrorism across the Technological Spectrum," *Terrorism and Political Violence,* Vol. 6, No. 3, Autumn 1994.

http://www.apbonlin.com/newscenter/majorcases /binladen/index.html.

http://www.cfr.org/publication/9362/.

http://www.fas.org/irp/threat/terror.htm.

http://www.front14.org/rac/theorder2.htm.

http://www.hamas.org.uk/.

http://www.ict.org.il/, 1999: pg.1.

http://www.nci.org/nci-nt.htm.

http://www.pals.msus.edu/cgi-bin/pals-cgi…142/te%20%shinrikyo/di%200001/txt.

Israeli Foreign Ministry, "Iran and Hezbolla," 3 March 2000, http://www.israel-mfa.gov.ilgopher://israel-info.gov.il.

Jones, Charisse and Moorem, Martha T., "US v. Bin Ladin Just Beginning," *USA Today*, 30 May 2001, pp. 1A, 3A.

Melman, Yossi. The Master Terrorist: The True Story Behind Abu Nidal, Adama Books, New York, NY, 1986, pg. 190.

Patterns of Global Terrorism–2000, U.S. Department of State, Office of the Coordinator for Counterterrorism, April 2001, pg. 1.

Ranstorp, Magnus, "Hezbollah's Command Leadership," *Terrorism and Political Violence*, Frank Cass, London, 1994, Vol. 6, No.3, pg. 304.

Rosie, George, *The Directory of International Terrorism,* Paragon House, New York, 1987, pg. 39.

Rubin, Rubin, "Islamic Radicalism in the Middle East: A Survey and Balance Sheet," *Middle East Review of International Affairs*, May1998; Internet:http://www.biu.ac.il/besa/meria/journal/1998/issue2/jv2n2a3.html.
Seale, Patrick. *Abu Nidal: A Gun for Hire*. Random House, Canada, UK, 1992, pg. 243.
Staten, C. L., "Two Men Arrested in Las Vegas in WMD Plot," *Emergency New Net*, 19 Feb 1998; www.emergency.com/lv-anthrax.htm.
Taylor, Maxwell and Quay, Ethel, *Terrorist Lives*, Bracey's UK Ltd., 1994, pg. 9.
"Terrorism Threat Assessments", http://www.fas.org/irp/threat/terror.htm.
The Economist, "The Shining Path Comes Back," 17 August 1996, pg. 35.
White, Jonathan, *Terrorism: An Introduction*, Wadsworth Publishers, Belmont, CA, 1998, pg.116.
Ibid. pg. 117.
Ibid., pg. 195.
Ibid., pg. 233.
Yonah, Alexander, "Hezbollah: The Most Dangerous Terrorist Movement," *Intersec,* Three Bridges Publishing Ltd., October 1994, Vol. 4, Issue 10, pg 393.

6 International Major Counter-Terrorism Units, Law Enforcement, and Intelligence Agencies — The Best Defense

NEWS

September 1985: An Egypt Air Flight is hijacked to Malta. The Egyptian government dispatches Force 777 to assist with hostage rescue operations. During the operation snipers outside the aircraft mistake some escaping passengers for terrorists and gun them down.

11 June 1985: Fawaz Yunis, and four others, board Royal Jordanian Airlines Flight 402 armed with grenades and automatic weapons. Eventually, the terrorists blow up the aircraft. "Operation Goldenrod" lures Yunis to a yacht in the Mediterranean under the pretense of a drug deal, and he is arrested and transferred to a U.S. Navy ship.

June 1994: A member of the GSG-9 German counterterrorism unit seeks to apprehend one of the leaders of the Red Army Faction, Wolfgang Grams. Police reports indicate that he is killed in a shootout with the unit. However, there is speculation that he may have been summarily executed after he had been subdued.

May 2002: The FBI is actively engaging in recruiting agents with the critical skills of computer science, engineering, counterintelligence, and foreign language ability; especially Arabic, Farsi, Urdu, and Pashtu.

19 June 2002: The National Security Agency intercepts two messages in Arabic on 10 September 2002, which refer to the next day as "zero hour." The messages are not translated until 12 September.

INTRODUCTION

In light of the fact that modern terrorism has proliferated exponentially during the last half of the 20th Century, counterterrorist and counterinsurgency units have been established around the globe. It is fascinating to investigate the means by which governments have sought to fight the battle against internal terrorism in addition to terror inflicted on citizenry abroad. The efforts by some authorities have become quite controversial, especially in Israel and Northern Ireland. This is in part due to the fact that the civilian population seems to have accepted the loss of certain civil liberties to attempt to win the "war on terrorism." The loss of democratic safeguards on the other hand has disturbed some civil libertarians. They see governments becoming more terroristic in their methodology, with normal democratic procedural safeguards being pushed aside.

However, conventional police forces deployed in large and sometimes cumbersome formations are not capable of combating small, clandestine, mobile, and speedy terrorist units. Furthermore,

using massive force in hostage situations has proved unrealistic. New tactics are needed. The need was amplified after the terrorist attack on the 1972 Olympic Games in Munich where it became woefully apparent that the police forces of Europe were not properly trained or equipped to deal with terrorists.

By legal tradition, this is a slippery slope for democracies. It is deplorable when the terrorist fighters become the terrorists. It is therefore mandatory that nations create counterterrorist forces that are highly trained in responding to terrorism, but also do so on a scale acceptable to the public and compatible with democratic traditions. This chapter will review the development of some of the most well-known units as well as some of their successes and failures. Some governments have incorporated their units into national police forces and others into the military. Generally they all have a flexible command structure, special tactical training, the right people for the job with appropriate personal characteristics, and specific equipment. Most units are designated as either counterterrorist units (CTUs) or hostage rescue units (HRUs). They usually consist of a headquarters unit, several combat units, a training unit, support unit, and a logistics operation.

Cooperation among various law enforcement agencies is crucial to the successful protection of any transportation facility. The protection of airports, because of the unique environment, presents its own specific challenges. Airports and the facilities and equipment that support such a facility are complex, to say the least. They also present a packaged scenario for terrorists to acquire quite a lot of attention with one huge attention-getting gesture. Due to the open and public nature of airport surroundings, access to an airport is easy. However, once people are participants in the busy day-to-day operations of an airport, police and private security are tasked with protecting large numbers of people in an almost "unprotectable" situation. This exclusive and demanding situation has required the imposition of special rules and training on policing units.

The Federal Aviation Administration (FAA) recognized early that an airport, with constantly moving people, aircraft, and ground vehicles, would mandate some special controls. Initially, during the period that terrorist hijackings and assaults seemed all too commonplace, it was thought large numbers of police stationed at the airport would solve the problems. It did not. Other alternatives had to be conceptualized and put into use. The FAA had detailed who is a qualified airport law enforcement officer, what their training should entail, and when an airport operator can ask and receive federal agent assistance.

Many larger airports also have an embedded "Airport Authority Police Department." They are full-service law enforcement agencies with the same responsibility as a county or municipal police agency to enforce state laws. Authority police also enforce federal regulations pertaining to airport operations. Generally, these officers are the first professional law enforcement contact to the traveling public. Travelers transit airports from all over the world, and the challenge is unique. Special training for these units is critical because the work environment of an operational airport is demanding and can be dangerous to the nonaviation professional. Simple issues taken for granted by aviation professionals are misunderstood by nonaviation personnel; especially on the flight line.

One organization, The Airport Law Enforcement Agencies Network, seeks the following:

- To facilitate the rapid exchange of information concerning airport-related crimes between its member agencies
- To achieve a better understanding of the unique problems germane to airport policing
- To provide its unique insight and level of experience to governmental agencies and elected representatives
- To provide a safer more secure environment for the traveling public

It is a not-for-profit organization composed of domestic and foreign airport law enforcement agencies, or port authorities and their associated national law enforcement, regulatory, or intelligence agencies.

In conjunction, the daily, behind-the-scenes operations of many other local, state, federal, and international agencies enhances ongoing security at an airport. All must work in tandem to combat the continuing terrorist threat and to address issues of various criminal operations, including organized crime, drug-trafficking, and most recently the trafficking in human cargo. Jurisdictions overlap, and coordination of the big picture is a difficult job. The success of that job depends on the active intervention and support of the federal government. On top of all this, thousands of positions in law enforcement remain unfilled, and agencies nationwide are seeking to answer the question of where to acquire qualified law enforcement personnel to meet the growing need.

Since the attack at the Munich Olympic Games, many European governments recognized the need for special intervention units. Special operation forces, or in police terminology, special intervention teams, were created to fill the gap in law enforcement capability at the time. The situation has changed dramatically since the 1970s, and the character of global terrorism has evolved from bombings and hijackings to suicide attacks. Regardless, the need for special interventions has not decreased. On the contrary, modern-day terrorists tend to have little risk aversion, meaning that specialized intervention is required more than ever.

In response to the changing environment, the European Union in 1996 pressed for an initiative of cooperation between counterterrorist units. The European Council initiated efforts to create a directory of specialized counterterrorist competences, skills, and expertise to facilitate this concept when special interventions between member states was considered necessary. Although it was envisaged that member states would take turns maintaining the directory, efforts lagged. They were once again vigorously reenergized after 11 September. In fact, the Council, in an extraordinary move following the terrorist attacks, ordered Europol to take responsibility for the directory. At the same Council meeting, the European Police Chiefs were ordered to organize and synchronize collaboration of the special intervention units. This led to the establishment of the "ATLAS network," an informal cooperation structure between special intervention units in the European Union. Its initial goal sought to raise each special intervention unit to the highest possible level of professionalism through intense structural mutual cooperation (Conclusions adopted by the JHA Council, 2001).

COUNTERTERRORIST UNITS

Austrian Special CounterTerrorist Intervention Unit

The "Cobra" unit, or Gendarmerieeinsatzkommando (GEK) was developed in Austria over 30 years ago to combat terrorism and serious crime. The specialized tactical intervention unit was created within the Austrian Federal Gendarmerie. As many other European police forces discovered, they were not equipped to protect their citizens in the 1970s from terrorist assaults. Although not as well known as the British SAS or the German GSG-9, the unit is one of the best-trained and equipped units in Europe.

Two incidents reinforced the need for this type of unit in Austria. A terrorist attack on Jewish immigrants traveling from Russia to Israel, via Vienna, and the assault on OPEC headquarters in 1975, highlighted the problem. The terrorists' expertise at urban warfare also surprised the Austrians. New strategies were needed to combat the tactical realities of the new threat. Brigadier Johannes Pechter, a member of the Austrian Gendarmerie, was instrumental in developing apropos special operations, and his new unit was authorized to have national jurisdiction. Its highest priority is fighting terrorism.

The GEK, however, is specifically tasked with the following (Meyr, "Elite Gendarmes", 2000):

- Intervention in extreme terrorist attacks involving hijackings and hostage taking
- Assisting other security agencies in dealing with violent criminal organizations
- Protection of the president and the prime minister as well as foreign presidents and heads of state visiting Austria

- Protection of Austrian diplomatic missions abroad during periods of crisis or extreme violence

The unit consists of approximately 170 members. Its facilities are located at Weiner Neustadt near the Austrian capital. The command structure runs directly to the Minister of Interior through the General Secretary of Security. Approximately ten senior officers are part of the command staff. The main body of the unit consists of four operational platoons and one training platoon. They train in various mixtures of two-, three-, and five-man tactical units. Training is heavily emphasized, and each member's marksmanship and physical capabilities are tested monthly. Competition remains tough, and members who become "unfit" are returned to their former regular police units, although they are permitted to recompete for a place on the team.*

In December 2006, Austria presented a concrete draft of a legal framework for cooperation between such special intervention units in crisis situations. The envisaged framework recognizes the need for general rules and conditions to allow for special intervention units of one member state to provide assistance or actual operational deployment on the territory of another member state (Official Journal of the European Union, 2006).

Canadian Armed Forces Joint Task Force 2

In 1993, the Special Emergency Response Team (SERT) of the Royal Canadian Mounted Police (RCMP) was disbanded. News reports have described the new Canadian counterterrorism unit as a "…highly skilled counterterrorist force of undetermined size, based somewhere near Ottawa with an anonymous commanding officer." (Mooney, 1995). The task force was created in April 1993 when it became a unit separate and distinct from the RCMP. The unit has a mandate "…to be ready to respond as a force of last resort to terrorist events or major disturbances of the peace affecting national security" (Mooney, 1995). The unit is made up strictly of volunteers drawn from all branches of the armed services and is commanded by a lieutenant colonel. The group's headquarters is actually located at Dwyer Hill Training Center, Ontario, and is believed to include a close-quarter battle (CQB) facility, an eight-story building for hostage-rescue, a DC-10, a bus, a multimillion-dollar shooting range, gymnasium, and Olympic-sized swimming pool. Its membership is estimated to be between 200 and 250 strong, with part of the force on alert at all times. They are organized into two- or four-man teams known as "bricks." Each "brick" has a specialty (communications, sniping, etc.). A 20- to 30-man troop is commanded by a captain. The government of Canada officially provided approximately $20 million to start and equip the unit, and it remains fully funded.

The unit received national attention when it allegedly was sent to Bosnia to free some Canadian hostages from their Serb captors in 1995. Other events at least monitored by the unit were the Commonwealth Games and the G-7 conference during the same year. More, but probably unwanted, media attention was received after an exercise was supposedly conducted in the suburbs of Montreal, much to the surprise of residents. JTF-2 is also reportedly to have contributed 40 operators to the war against Al'Qaeda as part of "Task Force K-Bar." Otherwise, the unit has remained discreet and out of the public eye.

* In 2000, France declined a request from the Austrian government to extradite Illich Ramirez Sanchez, or Carlos the Jackal, to Austria to face charges based on the attack on OPEC (Patterns of Global Terrorism: 2000). The Jackal gained international notoriety as the Cold War-era mastermind of deadly bombings, assassinations, and hostage dramas. He was linked to the 1972 massacre of 11 Israeli athletes at the Munich Olympics and was involved in the 1976 Palestinian hijacking of a French jetliner to Entebbe, Uganda, that ended with an Israeli commando raid. After eluding capture for decades, Ramirez was tried for the Paris killings of two French investigators and a man in the Popular Front for the Liberation of Palestine whom Ramirez suspected as an informer. He was found guilty and sentenced to life imprisonment. In June 2003, Carlos published a collection of writings entitled "*Revolutionary Islam*", seeking to explain and defend violence in terms of class conflict. In the book, he voices support for *Usama bin Laden* and his holy war on the United States. He also supported Saddam Hussein for resisting the United States, calling him the "Last Arabic Knight" (*Follain, 1998).*

Great Britain: SAS

Great Britain formed and trained one of the best-known antiterrorist special forces units in the world. It is quietly headquartered at a Royal Air Force base at Creedenhill. It was formed over 40 years ago and has survived and seen significant success by relying on the basics of secrecy and surprise. Its founding father, Lieutenant David Stirling of the Scots Guard, originated the concept of the standard "stick," which was a small unit of highly trained men to be utilized in volatile terrorist situations. Conventional army theoreticians attacked his theories during World War II, but he was adamant that specially trained units could be especially effective behind enemy lines. An army commando officer, Captain Robert Laycock, and a Welsh Guardsman, Jock Lewis, also envisioned the same concept. Most of the original members of these "special forces" were of Scottish Roman Catholic descent, whose heritage for generations had been to cultivate warriors who were specialists in guerilla warfare wrapped in the traditions of secrecy. The very first unit saw action in North Africa and became known as L Detachment, Special Air Service (SAS) Brigade. All Special Air Service Regiment or SAS members are volunteers, and they are all seasoned dedicated soldiers.

Proof of individual dedication to the unit is evidenced by the fact that when they are accepted into the group, they give up whatever rank they have already received and return to the basic rank of trooper. At the average age of 27, they choose to join the elite unit despite reduction in rank and reduction in pay. The competition and training to remain an SAS member is brutal. Several people have died during training. Members become proficient in explosives, battlefield medicine, use of state-of-the-art communication equipment, and special weapons. They are trained to operate in every sort of environment including the jungle, desert, mountain, and underwater terrain. Training for members is constant, plus one squadron is always on alert to deploy at a moment's notice. A special Operations Research Unit supports all SAS deployments and is particularly accomplished in developing weapons specific to the needs of the unit and the particular mission.

For example, the elite force began testing the Canadian C-7 in 1999. In comparison to the U.S. manufactured M-16, it is a rather expensive weapon. It is a complete weapons system that includes sights, laser targeting, a grenade launcher, and maintenance, all for the price of about 5500 British pounds each; twice that of the M-16. The gun can be adapted to be used as a machinegun or sniper weapon, and according to one member of the SAS, "This weapon is worth its weight in gold" (Harding, 2001).

SAS personnel have accumulated a wealth of information over the years on how to correctly deploy its forces. For example, Operation Nimrod was conducted on 5 May 1980. The SAS, in conjunction with some additional special police units, carried out an assault against the Iranian Embassy in downtown London. With the public watching, the team entered the embassy and methodically moved through the building freeing hostages and throwing stun grenades mixed with gas. This stun grenade is now widely used by similar units around the world.

In addition, after the 11 September 2001 attacks, the SAS immediately entered Afghanistan, many months before the United States ever deployed, accompanied by the Australian SAS. They engaged in numerous secret operations, and some successful exploits were mistakenly credited to U.S. forces. Additionally, when Taliban and al'Qaeda prisoners tried to escape, the SAS was reportedly called in to assist in their capture. The SAS also rescued two Central Intelligence Agency (CIA) men who were trapped behind enemy lines. Operation Trent employed a full squadron of the regiment in a successful attack on an opium storage plant in Helmand province, which doubled as an al'Qaeda local command center. On 30 January 2005, an RAF Hercules C-130 crashed near Baghdad, killing ten British servicemen. The plane had just dropped off 50 members of G Squadron north of Baghdad for an operation to combat the increased insurgency.

On 22 July 2005, the SAS were reported by *The Sunday Times* to have aided in intelligence gathering and surveillance for the Metropolitan Police that resulted in the unfortunate shooting of Jean Charles de Meekness, although the use of SAS forces was later denied by Sir Ian Blair, Commissioner of the Metropolitan Police. Following the 21 July Metro attacks in London, the SAS

assisted in an operation to capture some of the terrorists who were believed to have carried out the attempted attacks. The SAS were seen arriving in unmarked vehicles and wearing balaclavas throughout the operation to conceal identities. The SAS helped with storming the flats in West London and are believed to have fired several shots in the process. However, nothing was truly "seen," and they remain the silent professionals, the world's top special force and the predecessor of all the others.

Regardless, they have sometimes come under a great deal of criticism. Like the Israeli team, Sarayat Mat'kal, the SAS has been called into service more frequently than most. SAS has regularly served as backup forces for the Royal Ulster Constabulary in Northern Ireland who are considered quite unpopular themselves in some Irish circles. On occasion, public indignation has even been rapid and vocal. In fact, the efficiency and brutality of the SAS when they became involved in the urban warfare of Northern Ireland stunned the Irish terrorists and the British public.

Of particular note, was an operation conducted in Gibraltar in 1988. The SAS had followed an Irish Republican Army (IRA) squad to the area. Intelligence information seemed to indicate that they intended to detonate a bomb during a military parade. The SAS launched a preemptive attack on the unit. Military experts would call it a precision maneuver, but civilians labeled it cold-blooded murder. Even though Britons overwhelming support counterterrorist efforts, the outcry against a government authorizing a "shoot first and ask questions later" was too much for such a democratic society. The European Court of Justice also condemned the incident and provided the IRA with three more martyrs.

The British authorities have taken a strong stand against any actions by the SAS that have been considered excessive or have resulted in the needless loss of life. The SAS, locally referred to as Sassmen, have even been prosecuted in criminal courts. Two members were actually tried and convicted criminally for the death of a civilian. Nevertheless, because of the length and breadth of experience of the team, it remains one of the most respected in Europe. It is rumored that they are present at every terrorist incident in Europe to determine what went well and what did not. In fact, the team has frequently trained with the equivalent group in Germany, GSG-9, and provided consulting to hostage situations around the world.

The European Union has both criticized and supported the conduct of the group. The impact of the European Court of Human Rights' ruling in *Ireland versus United Kingdom* reveals some of the distaste with which certain conduct has been scrutinized in the context of the limits of interrogation techniques. The case was remarkable in that it ruled on five specific interrogation techniques that, while "inhuman and degrading," did not rise to the level of torture. Those techniques specifically included wall-standing, hooding, deprivation of sleep, and deprivation of food and drink. The court's ruling underscores the "inherent vagueness" of the language used in the 1984 United Nations Convention Against Torture, and other Cruel, Inhuman, or Other Degrading Treatment or Punishment. This language incentivizes states to push the legal boundaries of the Convention and develop interrogation practices that fall toward the edge of its bounds. The judgment itself is notable for the bounds of law discussed. The Court, commenting on the development of the Diplock Commission — a U.K.-based commission determining detention policy — repeats the U.K. Government's line that "The fear of [terrorist] intimidation is widespread and well-founded. Until it can be removed and the personal safety of witnesses and their families guaranteed, the use by the Executive of some extrajudicial process for the detention of terrorists cannot be dispensed with." The Court then followed that "The European Commission of Human Rights, on the basis of the evidence it had itself obtained, accepted that the findings of the Diplock report as to the level of intimidation were generally warranted."

This shows that the Court, at one stage of the proceeding, was in agreement with the United Kingdom's assessment of the IRA threat. In ruling on the case, too, Judge Sir Gerald Fitzmaurice gives specific insights as to why the techniques employed by the U.K. government do not rise to the torture threshold. He notes the following:

> …. [I]t is the character of the treatment that counts, not its results. It is easy to think of ways in which physical and moral resistance can be broken without any resort to ill-treatment, the use of force, or acts of degradation. Alcohol will do it, and often does. More generally, simple persuasion, or consideration and indulgence, will do it. As has been well said, "There is no defense against kindness." The degradation lies not in what the treatment produces, but in how it does it: it might produce no result at all, but still be degrading because of its intrinsic character.

Fitzmaurice concurs with the Court's finding that the five techniques did not rise to the level of torture, but provides useful analyses of the nuances in language determining torture. *Ireland versus United Kingdom* provides a unique standard for ruling on torture in international law. Although the court did not find the U.K. government's "five techniques" constituted torture, the Court's discussion on the variance in language and understanding regarding torture prove useful for future analyses (Case of Ireland v. The United Kingdom, 1978).

Germany: GSG-9

Grenzschutzgruppe 9 (GSG-9) was a direct outgrowth of the failure of the regular German police to deal with the Munich Olympic attack on Israeli athletes. The German police were woefully unprepared to handle the incident. Consequently, GSG-9 became operational on 17 April 1973, six months after the massacre in Munich. The Federal Border Guard was the parent unit of the team, in part because it reported directly to the central government. As mentioned, the Allies in Europe at the time tolerated the formation of a German national police force for the first time since the end of World War II. The group is headquartered in St. Augustine, Sankt Augustin-Hangelar, near Bonn and was the brainchild of Colonel Ulrich Wegener, who envisioned the small and highly flexible antiterrorist unit.

It is organized into three separate groups, GSG-9/1, GSG 9/2, and GSG 9/3. The group consists of a headquarters unit, a communications unit, and a documentation unit. GSG-1 is the traditional counterterrorist assault group. GSG-9/2 consists of experts in maritime terrorism, and GSG-9/3 is made up of aviation experts. The first two groups have approximately 100 members, and the aviation unit has about 50. Further broken down, each of the three strike forces has a command section and five Special Tactical Sections composed of four men and an officer, known as the five-man stick (Dobson and Payne, 1982).

The German team is not a military organization; it is a civilian police force. Members of the German Armed Forces who wish to join the team must resign from the military first and join the Border police. It is unique, especially in its training in knowledge of the law as it relates to counterterrorism. Members constantly study all active terrorist groups. It is also trained in the usual counterterrorism techniques and possesses one of the most complete arsenals in the world. Each team member is an expert marksman.

GSG-9 is particularly well trained in the rescue assault of aircraft. The training served them well in their most famous rescue effort in Mogadishu, Somalia, in 1977. The team successfully raided a terrorist-held Lufthansa 707 after two men and two women hijacked the plane, demanding the release of Baader-Meinhof prisoners in German jails. Zohair Akache's terrorist team hijacked the aircraft with 82 passengers on board and roamed the Middle East for a place to land, ending up in Mogadishu. The Somalis were more than willing to let the Germans take the lead, especially after the terrorists killed the German pilot. Twenty-eight team members stormed the aircraft and killed the terrorists with no loss of life to the hostages.

The team has been highly successful regardless of the fact that its reputation was slightly soiled in 1993 when an operation directed at the Red Army Faction went bad. The team captured Wolfgang Grams, and after he was in custody, he was shot by one of the team members. An investigation concluded that Grams had shot himself, but the rumor of abusive conduct almost ended in the disbanding of the team. The operation involved an attempt to arrest both Wolfgang Grams and his girlfriend

Birgit Hogefeld at a train station in Bad Kleinen. The original police report indicated that as police had closed in on the terrorists, Grams had pulled a gun and killed an officer. According to the report, the police took down Grams. Eyewitnesses, however, did not support that version of events. In fact, they claimed that Grams was shot while he laid helpless on the tracks of the train station.

One witness claimed, "Two policemen walked up to Grams, who was lying motionless. One bent over and shot him several times from closeup. Then the second officer shot at Grams, but more at his stomach and legs. He was shot several times" (Jackson, 1993). The coroner's report authenticated the eyewitness accounts and concluded that Grams had been shot at close range. In addition, the incident had disrupted efforts to negotiate a peace settlement with the Red Army Faction. As a result of the alleged murder and coverup, Interior Minister Rudolph Seiters resigned, followed soon after by a chief federal prosecutor.

Later, exhibiting incredible restraint, the team captured a hijacker who had commandeered a KLM flight from Tunis to Amsterdam. The hijacker demanded that Sheikh Omar Abdel Rahman, on trial for the World Trade Center bombing in New York in 1993, be immediately released. GSG-9 was able to capture the hijacker without firing a single shot. From 1972 to 2003 they reportedly completed over 1500 missions (http://www.bundespolizei.de/nn_249932/ DE/Home/06Presse/ Infobroschuere__down,templateId=raw,property=publicationFile.pdf/Infobroschuere_down.pdf, pg. 17), with shots being fired on only 5 occasions. (official count, prior to the 2003 Iraq War). These occasions were Mogadishu in 1977, Bad Kleinen in 1993, Aachen in 1999, and two more missions where firearms were used to shoot the dogs of the persons being arrested. At the SWAT championship in 2005, GSG 9 won seven out of seven events, beating 17 other teams. In March 2006, in the same competition, GSG 9 defended its championship.

Most recently in 2007, GSG-9 participated in the arrest of three terrorists with links to al'Qaeda, suspected of preparing a massive bomb attack on U.S. facilities in Germany. The terrorists had collected 730 kg (1500 pounds) of hydrogen peroxide, which would have enabled them to construct bombs with more explosive power than those utilized in the Madrid and London attacks. In an ingenious move, a few days before the arrest, "police experts secretly swapped the 35-percent solution of hydrogen peroxide contained in 12 barrels for a diluted liquid that only contained 3 percent of the chemical." GSG-9, in part due to its success, may not survive for very much longer. With the decrease in terrorist incidents in Germany and costs constraints coming into play, the team may be replaced with new SWAT-type units. Hopefully, its expertise and legacy will remain within the German antiterrorism effort.

Israel: Sarayat Mat'Kal

The Israelis have been combating terrorism for longer than almost any other country. Because of the abundance of terrorist attacks, the state of Israel swiftly developed the technological means, military doctrines, and general policy for counterterrorism efforts. Golda Meir, Prime Minister for many years, whole-heartedly supported the concept of secret strike teams after the attack on the Israeli team at the Munich Olympics. The whole country was seeking revenge, and the leadership of the country settled on a policy of "seek out and destroy" terrorists. They have perfected the concept of strike teams and have been actively involved in activities labeled both excessive and possibly illegal. The team's purpose was redefined in 1989 when Itzhak Rabin, then Minister of Defense, stated that "The goal we set ourselves in the campaign against terror is not one of elimination, but to minimize our vulnerability and delivery of the strongest possible blows against terrorists" (Israeli Counter-Terrorists Activity, Internet: http://www.ict.org.il/counter_ter/is_ct.htm. pg. 1).

The team, officially known as the Sarayat Mat'kal, but also known as the General Staff Reconnaissance Unit 269, has embraced the Talmudic concept that if someone arrives to kill you, you should rise up and kill them first. Officially, the team was established in 1957 as Unit 269 by veterans of the Paratroopers Brigade, Unit 101, and the Intelligence Branch (*Aman*) of the Israeli Defense Force (IDF). It was given both a peacetime mission relating to counterterrorism and a

wartime mission dealing with deep reconnaissance intelligence gathering, but the unit is first and foremost a field intelligence-gathering unit, used to obtain strategically important intelligence far behind enemy lines. It is *the* elite special forces unit of the IDF. The team is also in charge of hostage rescue missions outside of Israel's borders. Their overall approach is three-pronged. It involves operative measures designed to combat terrorist targets in the area directly and defensive measures meant to foil any attempts. Lastly, the strategy of punitive measures involves the legal, and some would say not so legal, concepts to punish the members and supporters of terrorist organizations. The three approaches are similar but can be distinguished. The offensive activities seek to prevent the implementation of any terrorist attack by intervening during the planning and organizational stages of the attack. The defensive activities aim to disrupt an attack immediately after it is initiated. The punitive measures apply at all stages of the attack.

The strike team has been particularly successful and was especially effective during the raid on Entebbe in 1972 and in executing raids against Palestinian terrorists in neighboring Arab countries. Initially, forerunners of today's team embraced the rage sweeping Israel after the Olympic Games attack and sought to kill those responsible at all costs. Unfortunately, in their zeal, one of the hit teams, which had been unleashed, assassinated an innocent waiter in front of his pregnant wife. The Israelis were hunting for Ali Hassan Salameh, the architect of the Munich massacre. However, one of the intelligence team members mistakenly identified a Moroccan man married to a Norwegian woman as him. The Israelis were embarrassed after the man was gunned down, and international pressure forced Israel to restrain their exuberance for killing alleged Palestinian terrorists.

Regardless of the international indignation, the team eventually found Salameh and killed him with a radiocontrolled car bomb in Beirut. The incident precipitated another outcry from the international community because the bomb killed four bodyguards and five innocent bystanders. The team also claimed to have been responsible for the assassination of Khalil al-Wazir, one the leading Palestinian Liberation Organization strategists in Tunis in September 1985.

Despite some initial "media" setbacks, the Sarayat Mat'kal, is one of the best-trained and best-equipped special forces units in the world. The Irgun, a terrorist organization in its own right in the Israeli dispute with the British, was the predecessor to the team. The Irgun is best known for the bombing of the King David Hotel on 22 July 1946. The bomb killed 91 people; Arab, British, and Jewish alike. Some of the initial efforts of the team focused on efforts to prevent Palestinian terrorists from mounting attacks from Lebanon into Israel. The Israelis were retaliating for a Palestinian hijacking of an El Al airliner enroute from Rome to Tel Aviv and a second incident at the Athens airport.

In retaliation, the Sarayat Mat'kal launched a commando raid directly against the Beirut International Airport in hopes of stopping intrusive Palestinian raids. The team completely destroyed 13 empty aircraft. No one was injured. However, international reaction was still negative. Specifically, the French condemned the attack and used the raid as a reason for suspending arms shipments to Israel. The United States expressed its displeasure over the raid into another nation's sovereign territory, but did not cut off arms sales. In another unwanted twist of events, the Palestinians seemed to gain a bit of global sympathy, and the aircraft were replaced and upgraded as a result of claimed insurance money.

Regardless, strikes on Entebbe and elsewhere have made the team famous. In 1972, they successfully ended the hijacking of a Sabena Boeing 707 on a flight from Brussels to Tel Aviv. The hijackers, members of the Black September group, forced the plane to land in Tel Aviv and threatened to blow it up with all souls on board. The team stormed the aircraft with minimal loss of life. Many other counterterrorist squads quickly adopted their procedures in the years to come as the textbook way to conduct an aircraft rescue operation. Overall, the team has been very effective, and generally their efforts have been applauded, especially when viewed in humanitarian terms.

The Israeli government historically has maintained an official policy of denying existence of the "unit." Operations were generally accredited to "elite paratroopers." However, due to the unit's successes in bold operations, it quickly became a very publicly known secret in Israeli society.

The following list is from *The Illustrated Directory of Special Forces.*

1968 – Operation Shock – Sabotage of power plant and Nile bridges in Egypt (jointly with Israeli Air Force)
1968 – Operation Gift – Sabotage of 14 Arab airliners in Beirut International Airport, Lebanon
1969 – Operations Orchard 22, Orchard 37 - Assaults on high-voltage wires and a control antenna in Egypt
1969 – Operation Bulmus 6 - Assault on fortified Green Island, Egypt (jointly with Shayetet 13)
1969 – Operation Rooster 53 - Seizing an entire Egyptian radar installation (jointly with Israeli Air Force)
1970 – Operation Rhodes - Assault on fortified Shadwan Island, Egypt (jointly with Shayetet 13)
1972 – Operation Isotope – Foiling a Sabena aircraft hijacking in Tel Aviv, Israel (hostages rescued)
1972 – Operation Crate 3 - Kidnapping 5 Syrian intelligence officers
1973 – Operation Spring of Youth - Killing Black September terrorist leaders in Beirut, Lebanon (jointly with Shayetet 13)
1973 – Recapture of Mount Hermon from Syrian commandos in the Yom Kippur War (jointly with Golani Brigade)
1973 – Deep interdiction ambushes in Egypt and Syria during the Yom Kippur War
1974 – Ma'alot massacre (school hostages rescued)
1975 – Savoy Operation (hotel hostages rescued)
1976 – Operation Thunderolt- Foiling an Air France aircraft hijacking in Entebbe, Uganda (hostages rescued)
1978 – Coastal Road Massacre (bus hostages rescued)
1980 – Misgav Am (Kibbutz hostages rescued)
1984 – Kav 300 affair (bus hostages rescued, see The Shabak's years of crisis)
1988 – Tunis Raid - assassination of Abu Jihad, in Tunis, Tunisia
1989 – Sheik Abdul-Karim Obeid kidnapping, Lebanon (see Ron Arad)
1994 – Mustafa Dirani kidnapping, Lebanon (see Ron Arad)
1994 – Nachshon Waxman (foiled hostage rescue)
2006 – Attack near Hezbollah stronghold Baalbek (to disrupt weapons smuggling)

Civil Guard

Less known and not as flamboyant as the Sarayat Mat'kal is Israel's Civil Guard (INP). With increasing criminal and terrorist activity, the Guard has become very essential in the fight against terrorism. It was founded on 9 June 1974 and has grown into a significant force. The 50,000-strong force consists totally of volunteers. They participate in maintaining roadblocks, conducting security searches of public transportation, and operating emergency teams on a 24-hour basis. After terrorists murdered 22 school children at a school in Ma'alot in 1974, the response from the public to assist the police in internal security matters was immediate and has remained constant. The volunteer units have become fully incorporated into the national police force at all levels. They are activated in two main operational forms. First by means of local units deployed from neighborhood operational bases, and second by special units assisting the police in specific law enforcement and security operations.

This second form includes specially trained sharpshooter units and bomb disposal support units. The national police confirm that, "Sharpshooters are primarily deployed in the assistance to INP units engaged in counterterrorist activities, ambushes, and preventive operations" (Meyr, 2001).

The bomb disposal unit also assists the INP in surveillance of likely terrorist targets, evacuation of bomb victims, and driving bomb disposal vehicles, as well as providing aid in the disposal of bombs. The integration of the Civil Guard into the INP has greatly facilitated their efforts in controlling the aftermath of terrorist attacks as well as aiding the prevention of them. The volunteer human resources potential is immense, and other governments could benefit from such a program in the counterterrorist arena.

Border Guard Force

The Israeli Border Guard Force is a semimilitary force that possesses police powers and is worthy of mention in this context. They are referred to as the Green police because of their easily recognizable green uniforms. It is a part of the national police and is answerable to the Israeli Police Commissioner. Its primary mission, since its inception in 1953, is to protect the borders of Israel. However, because terrorists have repeatedly attempted to infiltrate the border, the border guard force's importance and amount of responsibility has increased.

Immediately after the Six-Day War, units of the organization were sent into the newly occupied territories. The Guard is now formally tasked with guarding airports and seaports, in addition to other vital installations. They are approximately 8000 members strong and, uniquely, 12 percent come from minorities such as Bedouin, Circasians, Christians, Druze, and Moslems. (Meyr, "Protector if Internal Security", 2000). The Guard is also tasked with protecting the green line between Israel and the West Bank, a highly volatile area. In addition, the border guard also operates a number of special units like the Counterterrorism Hostage Rescue Unit or YAMAM, which was set up in 1974. In conjunction, the YAMAS or Mista'arvim unit conducts special undercover operations against terrorists in Judea and Sumaria.

Ireland: Army Ranger Wing

The Army Ranger Wing (ARW), or "Sciathán Fianóglach an Airm," has the principal task of leading the tactical fight against terrorism in Ireland. Its headquarters is located at Camp Curraugh in County Kildare. The organization is directly subordinate to the Army's chief of staff. The organization includes a command group, two assault platoons, and a support platoon composed of explosive experts, medical officers, and other specialists. As the primary counterterrorist force in Ireland, it is tasked with intervening in any extreme terrorist attack to include hijackings. For intervention purposes, each of the assault platoons can be subdivided into smaller tactical teams depending on the operational need.

Members from the ARW unit were deployed to Iraq alongside Arabic-speaking members of G2 (the military intelligence branch of the Irish military), after Irish journalist Rory Carroll was abducted in 2005. The Rangers were charged with liaison with U.S. Special Operations Forces in regard to a possible rescue operation, and to provide security to the Irish Government representatives who were attempting to negotiate his release.

France: Groupment d'intervention de la Gendarmerie Nationale (GIGN)

The Groupe d'Intervention de la Gendarmerie Nationale, GIGN, has become one of the world's busiest counterterrorism units. The organization was founded as early as 1974 and consisted of a relatively small number of members. It was created following the attack at the Munich Olympic Games and the takeover of the Saudi Embassy in Paris. After so much experience, they have significantly honed their skills in combating the activities of terrorists. Between the years 1974 and 1985, "…they have participated in over 650 operations that freed over 500 hostages and eliminated dozens of terrorists" (France's GIGN, Internet: http://www.specwarnet.com/europe/gign.htm., pg. 2). Different from the British SAS, the unit is a police unit, not a military one. Consequently, they are called on to handle not only terrorist incidents, but nonpolitical criminal circumstances as well.

The original organizers realized that the small number of officers assigned to the group was one of its advantages. Since its creation, therefore, it generally has had about 90 to 100 members. Additionally, the team has been noted for its creativity. Like American police departments that have sent lottery award notifications to individuals with outstanding warrants against them to have them claim the prize in person only to be arrested, the French have also pulled off some exceptional ruses of their own. In 1976, for example, in a hostage situation involving children, the GIGN sent drugged sandwiches to the terrorists. They fed the sandwiches to the hostages, having them immediately fall asleep. After the hostages lay down, the police had an open field of view for the GIGN snipers.

Because the French have former colonies all over the world, the GIGN has been known to effectively operate everywhere from Djibouti to the Sudan. However, one of their most famous deployments involved the storming of an Air France Airbus in Marseilles, wherein all 13 hijackers were fatally shot. They are a particularly heavily armed unit, preferring as many other counterterrorism units, the Heckler and Koch MP5 submachine gun, plus an assortment of handguns.

They are correspondingly well trained in all sorts of environments from alpine to ocean diving. The members of the group are recruited from the national police, the Gendarmerie. All officers have had at least five years of regular police experience. Once accepted, they receive an additional ten months of training to master the weapons of their adversaries. They also become experts in evasive driving, parachuting, mountain operations, marksmanship, and marine operations. The organization is broken down into four 15-man units and is supplemented by a command and support unit, including specialists in hostage negotiation. The commanding officer is a major, and the command staff consists of a total of five officers. The staff consists of a deputy commander, three captains, and lieutenants. Their headquarters are located at Maison Airport outside Paris.

Overall the French have continued to conduct an all-out effort against terrorists. They have a nationwide "Vigi-Pirate" plan that combines military forces and the police as reinforcements for each other, in part to specifically counter attacks by Algerian terrorists in the Paris Metro and other major cities. The combined teams are highly successfully in increasing security at metro and train stations, bolstering security at borders, and expanding identity checks throughout the country. Additionally, in a cooperative effort with the Spanish, they launched an aggressive cross-border operation to shut down operations and supply lines of the ETA.

GIGN has engaged in hundreds of operations since its inception in 1973 and has gathered a great deal of practical experience. As a result, they are frequent hosts to members of other counterterrorist units such as the United States' Delta Force and Germany's GSG-9. In one well-publicized case, GIGN members advised the Saudi National Guard prior to their assault on the terrorist-held Grand Mosque in Mecca. Prior to 1994, GIGN had made its name in Djibouti when, in 1976, its commandos rescued 29 schoolchildren from Somali terrorists. In 1995, France sent some ten members of GIGN to a forward-deployment base in the Indian Ocean for possible intervention in a coup by white mercenaries. Since its inception, GIGN has actively participated in almost 700 operations, which have resulted in more than 500 rescued hostages. Criminal arrest statistics are reportedly even more impressive.

Spain: Grupo Especial de Operaciones (GEO)

In light of the fact that Spain has recently been inundated by significant acts of domestic terrorism, the government has not regretted its decision to establish a counterterrorism unit. The unit, assembled in 1978, initially suffered from a lack of political support and minimal fiscal resources. Spain has suffered from attacks from both left-wing and right-wing terrorist groups, but most notably the Basque Fatherland and Liberty (ETA). The ETA has historically targeted police, military personnel, and politicians. The initial unit received some meaningful advice and assistance from German's GSG-9 unit after their repeated successes and has since become an elite unit proven to be effective. One incident involved a terrorist takeover of the Central Bank of Barcelona, which involved over 200 innocent hostages. The 24-member terrorist team had occupied the bank and threatened to kill

the hostages. The GEO stormed the bank. One hostage was injured, ten terrorists were captured and one killed. The remaining terrorists blended into the hostages fleeing the building and escaped.

The GEO unit was first utilized in Bilbao, on 7 February 1981, when five persons were freed from two armed criminals in a branch office of the Banco Bilbao Vizcaya. GEO also experienced success after it was responsible for rescuing Dr. Iglesias Puga, father of singer Julio Iglesias, as well as foiling an attempt by ETA to attack the 1992 Summer Olympics in Barcelona. The unit had been repeatedly called on as Spain was wrenched by terrorism in the years 2000 and 2001, after a ceasefire with the ETA fell apart. Additionally, a group quiet for many years reappeared. The First of October Anti-Fascist Resistance Group (GRAPO) murdered a Spanish policeman following the arrest of seven of their members in Paris. The group also killed two security guards during an armed robbery and detonated seven bombs. The GEO was consequently busy during the years 2000 and 2001, assisting in quite a few antiterrorist deployments justifying their continued existence.

The GEO has unarmed several organized crime groups, arrested 41 armed members of different terrorist groups, freed 424 persons who had been kidnapped or taken as hostages, and boarded 20 ships used to carry narcotics. Despite this, as of 2005, the GEO was undermanned, and riot control units were deployed to Iraq instead of GEO members, as originally intended (Ryan et al., 2004).

United States: Special Forces Teams

The home bases of American military counterterrorist forces were located back in the United States, away from most previous international terrorist attacks. The Joint Operations Command, located at Fort Bragg, NC was generally believed to be tasked with the mission of repelling terrorist attacks or launching rescue operations of American citizens held as hostages. The command brought together units from all of the branches of the armed forces, most publicly well known being Delta Force and Task Force 100. The Navy and Air Force have their own respective teams, namely, Seal Team Six (now the Naval Special Warfare Development Group, NSWDG) and AF Special Operations Command. They all have some unique expertise to bring to the mix such as the MC-130s at Hurlbert Air Force Base. The Navy's team is specifically tasked to deal with any terrorist activity in a maritime environment. Many critics of the teams, as well as many military officers, recognize the lack of cohesion of any effort that is "joint." On top of that, the founding father of Seal Team Six, Commander Richard Marcinko, was criminally tried for fraud and bribery, hence the name change of the unit.

Surprisingly, the teams are best known for the failed attempt to rescue the U.S. hostages being held in Teheran, Iran, also known as Operation Eagle's Claw. It failed miserably. Shrouded in so much "classified material," some of the military officers involved did not know what the mission they were preparing for was to accomplish. The effort proved the point that what can go wrong will go wrong. First, too many people held command authority, and their lack of ability to work together effectively contributed to the failed effort. The supposed overall commander, Army Major General James Vaught, was theoretically in command of Air Force Colonel James Kyle, Marine Colonel Charles Pitman and Delta Force Commander, Colonel Charles Beckwith. Personalities coupled with interservice rivalry contributed to mixed signals and ultimate disaster. A huge dust storm and the fact that one of the helicopters on the mission crashed into a C-130 loaded with munitions resulted in the death of eight Marines and has been touted as the tangible reason for the mission being aborted mideffort.

Partly, as a result of the "debacle in desert," the United States originally lacked the political will and senior military support to create a truly single unit to combat terrorism. Despite this, U.S. Special Forces later went through a series of major changes and "special forces" from all services are now combined under U.S. Special Operations Command (SOCOM).

SOCOM Command Components consist of the following (see Figure 6.2):

- U.S. Army Special Operations Command
- Naval Special Warfare Command

- Air Force Special Operations Command
- Marine Corps Forces Special Command
- Joint Special Operations University

The U.S. experience reinforces the point that it is not sufficient just to possess a force. There must also be a commitment to train, equip, and, most importantly, command them properly. They need to be equipped with high tech, real-time information and refined weaponry to meet the ever-increasing sophistication of the terrorists.

Seal Team Six Engagements are listed as follows:

- 1985 – Six were deployed to the site of the Achille Lauro hijacking in anticipation of a possible assault on the vessel.
- 1985 – SEAL Team Six members were also responsible for the rescue and evacuation of Governor Sir Paul Scoon from Grenada during Operation Urgent Fury. Four SEALs were lost to drowning during helicopter insertion offshore. Another aspect of the operation included the securing of a radio transmitter that resulted in heavy contact with Grenadian forces.
- 1989 – The unit took part in Operation Just Cause as part of Task Force White, which included SEAL Team Two. Their primary task, along with Delta Force, was the location and securing of Panamanian strongman Manuel Noriega.
- 1990 – They again operated in Panama as part of a secret operation code-named "Pokeweed," which had as its goal the apprehension of Colombian drug lord Pablo Escobar. Although Six was deployed from the U.S. aircraft carrier U.S.S. Forrestal offshore, the mission was unsuccessful due to poor preassault intelligence.
- 1991 – SEAL Team Six reportedly recovered Haitian President Jean Bertrand Aristide under cover of darkness following the coup that deposed him.
- 1991 – Six was also part of contingency planning for shooting down Saddam Hussein's personal helicopter with Stinger missiles, although this operation never got beyond the planning stage.
- 1996 – The unit reportedly deployed to Atlanta, GA as part of a large U.S. counterterrorist contingency plan for the 1996 Summer Olympics.*

Operation Ice Eagle

In the aftermath of 11 September, airline travel in the United States and abroad dropped dramatically. Although long-term plans to heighten airport security were underway, an interim solution was needed to restore public confidence in air travel. A visible increase in security was recommended. As a result, President Bush offered federal funds to state governors if they would use those funds to place National Guard troops at security checkpoints.

Although public reaction was mixed, National Guard troops in Minnesota and many other States were activated and ready for duty by 6 October 2001. The mission was the subset of Operation Noble Eagle with a Minnesota twist, Operation Ice Eagle. Operational orders were cut, and the state adjutant general, 1st Brigade of the 34th ID (MECH) was assigned the task of placing troops at the Duluth, Minneapolis-St. Paul, and Rochester airports. Normally, the 34th military police company would cover civilian law enforcement-related missions, but there were insufficient personnel. Consequently, combat arms units were used to fill the gap. On 30th September, the 2nd Battalion

* *NOTE*: The Hostage Rescue Team (HRT) of the Federal Bureau of Investigation (FBI) is responsible for domestic counterterrorism and was the primary response unit (Internet: *http://www.sealchallenge.navy.mil/*). Local, state, and national law enforcement officers generally handle incidents of domestic terrorism. At least, they are frequently, if not always, the first to be called to the scene of an incident. The FBI is also the lead agency tasked to collect intelligence on domestic terrorists, not the Central Intelligence Agency which has an overseas mandate.

135th Infantry Air Assault and 1st Battalion 194th Armor Regiment were given the duties of securing the airports in Minnesota.

Because the Posse Comitatus Act forbids the use of the U.S. military from engaging in law enforcement duties against U.S. citizens, the activation of the troops remained at the state level. Authorization came from 32 U.S. Code Section 502, which authorizes the use of National Guard troops by the governor of a state for whatever purposes he deems fit. The authorization was not based on Title 10 of the U.S. Code which would have given the troops federal jurisdiction, placing them in federal service. Guard units from many states remained at U.S. airports, with little training, under very unusual conditions, sometimes without normal federal benefits but serving with distinction until 17 May 2002.

Local Law Enforcement

Exactly who is a law enforcement officer, as it relates to aviation, was expressly defined in FAR 107. Section 107.15: Law Enforcement Support states that (a) each airport operator shall provide law enforcement officers in the number and in a manner adequate to support (1) its security program, and (2) each passenger screening system required by Part 108 (Internet: http://www.faa.gov/avr/AFS/FARS/far-107.txt., 2001).

What this means is often debated. How many officers are needed and their precise function will vary from airport to airport. First, of course, law enforcement officers are appointed by a government entity and have statutory authority to engage in certain conduct. As already discussed, they possess the authority to arrest and detain under circumstances completely different from those of a private security guard or a private citizen. For example, a police officer has the authority to arrest an individual without a warrant for a crime committed in his or her presence or for a felony on which they have probable cause to arrest. That standard duty is applicable on and off an airport complex. Airport police are also tasked with assisting security personnel in the prevention and investigation of any terrorist threat. This special duty requires them to meet special criteria and to have special training. Private security and law enforcement must have a seamless working relationship. In fulfilling both their duties, there are, of course, many differences and some similarities between airport security personnel and a governmental police force.

Private and public police officers may both wear uniforms and badges and carry weapons. Both seek to compel obedience, prevent crime, and apprehend criminals. They are both apt to be sued as well. Therefore, it is absolutely mandatory that both groups understand what acceptable behavior is under the law and what is not. Because public officers and airport security guards should receive respect and cooperation does not make it so. In reality, they may face hostility and aggression that they need to be trained to handle.

Under the Federal Aviation Act of 1958, it is illegal to attempt to board an aircraft while having concealed a deadly or dangerous weapon on or about one's person. Private security officers routinely conduct the required regulatory searches. More and more federal employees will be assuming these duties. Furthermore, the regulations require that passengers or visitors discovered to be carrying an undeclared weapon, whether on their person or inside carry-on baggage, must be referred to a duly appointed law enforcement officer. Hence, the combined efforts of security and law enforcement are essential to the overall endeavor.

TSA 49 CFR Chapter XII, Part 1542.217 (a) Law Enforcement Personnel (formerly, Section 107.17 of the FARs) defines an airport qualified law enforcement officer as follows:

- Has the authority to arrest
- Is readily identifiable by uniform and displays or carries a badge or other indicia of authority
- Is armed with a firearm and is authorized to use it
- Has completed a training program that meets the requirements

The law enforcement officer must, while on duty at the airport, have the authority to arrest, with or without a warrant, for the following violations of the criminal laws of the state and local jurisdictions in which the airport is located: (a) a crime committed in the officer's presence and (b) a felony, when the officer has reason to believe that the suspect has committed it (Internet: http://www.faa.gov/avr/AFS/FARS/far-107.txt, 2001).

Under the Federal Aviation Act of 1958, the law enforcement officer was originally supposed to be immediately available at the screening point. This concept was eventually discarded. The flexible response concept permitted the law enforcement officer to be available but not necessarily present. Historically and depending on the size of the airport, the response time varied considerably. Previously, "at Category I airports the response time may not exceed five minutes, and at selected Category IA airports may not exceed one minute. At Category II airports the response time was 10 minutes; at Category III the response time was 15 minutes. At Category IV airports the response time could have been as much as 20 minutes" (Gesell, 1981). For security reasons, response times are no longer so readily available, although a common sense approach recognizes that a qualified law enforcement officer is probably only a few minutes away if needed. Not all airports are large enough to justify an entire "airport police" contingent directly at the airport. Others, when necessary, have to call local police to the scene.

Training

When the airport and airline security rules were implemented in the early 1970s, the FAA also established a special training program for local law enforcement officers. FAR 107.17 specifically required and TSA 49 CFR Chapter XII, Part 1542.217 (c) requires that each officer complete an appropriate training program. The training program must include training in:

- The use of firearms
- The courteous and efficient treatment of persons subject to inspection, detention, search, arrest, and other aviation security activities
- The responsibilities of a law enforcement officer under the airport operator's approved security program
- Any other subject the administrator determines is necessary (Internet: http://www.faa.gov/avr/AFS/FARS/far-107.txt., pg.11, 22 August 2001)

Airport police officer training is conducted at the FAA facilities in Oklahoma City. The first class of officers was graduated as early as 26 January 1973, but since that time, thousands of law enforcement officers, private security professions, FAA employees, and international students have been graduated. The school, known as the Transportation Safety Institute, is still in existence and continuously provides officers with classes directly related to airport security techniques. Funded by the FAA to meet the expanded need to provide highly trained people at airports, the school's availability was extended to include FAA inspectors and special agents and not just local law enforcement. The school is internationally recognized and also provides training to aviation and security professionals from around the world.

Over the years, the curriculum offered by the school has also been greatly expanded. They now conduct courses not only in basic civil aviation security, but also more explicit and detailed seminars. Training now also includes courses in hijacking, terrorism, explosive detection, K-9 units, investigations, rule compliance, and inspections.

Training is also available at the FBI Academy in Quantico, VA. It is one of the world's most respected law enforcement training centers. Police training programs include the FBI National Academy, an 11-week multidisciplinary program for seasoned law enforcement managers; the Executive Training Program; and the Operational Assistance Program, which specifically trains law enforcement personnel in how to respond in certain emergency situations, including terrorist acts. Many agencies engage in cooperative efforts to maintain security at airports. They incorporate but

are not limited to the U.S. Customs Service, the Drug Enforcement Agency (DEA) the FBI, the U.S. Marshals, the Immigration and Naturalization Service (INS), Interpol, and the U.S. Postal Inspection Service (USPIS.) All make distinct and unique contributions to the fight against terrorism.

One of the greatest detriments to the ongoing battle against the scourge of hijacking and airport assaults is when these organizations become proprietary and do not cooperate. Secrecy between agencies only assists the terrorist. If one agency does not wish to share its knowledge with another, critical information often fails to reach the person or officers who may need it most. In the future, the government has to ensure better interagency communication at all levels of government. All data accumulated must be shared so that it can be correlated and used as a source of predictive information.

The FAA also maintains its own staff of exceptionally trained security officers to supplement the policing of airports. FAR Section 107.19: Use of Federal Law Enforcement Officers (TSA 49 CFR 1542.219: Supplementing law enforcement personnel) states that (a) whenever TSA decides, after being notified by an airport operator prescribed in this section, that not enough qualified state, local, and private law enforcement personnel are available to carry out the requirements of Sec. 1542.215, the TSA may authorize the airport operator to use, on a reimbursable basis, personnel employed by the TSA.

Consequently, the FAA, the TSA, and many other agencies are considered necessary to provide overall security for airports in what is hopefully a cooperative team effort. Jurisdictional disputes and personalities must not interfere with the protection of the public. Providing a safe working environment for airline employees, airport employees, and the traveling public is a very high priority and requires constant vigilance. A short description of some of these agencies follows.

The U.S. Customs Service

The original U.S. Customs Service was one of the oldest agencies of the U.S. government. It was established in 1789 and constituted an integral part of the Department of the Treasury. It was the primary enforcement agency charged with the protection of U.S. borders at 300 ports of entry. Specifically, the U.S. Customs Service had a mission to assess and collect customs duties on imported merchandise, prevent fraud and smuggling, and control carriers, people, and articles entering and departing the United States. The department was broken down into the offices of Assistant Commissioner for Enforcement, Inspection and Control, Commercial Operations, International Affairs, and Internal Affairs.

The commissioner was in charge of over 19,000 employees and responsible for protecting U.S. citizens from everything such as mad cow disease to explosives. Customs boosts a gigantic source of revenue for the government. In 2000, Customs returned $22.1 billion to the U.S. Treasury in confiscated goods and currency, and $23.8 in 2001. In a typical day officers examine approximately 1.3 million passengers, 2661 aircraft, 60,196 trucks, 348,205 vehicles, and 522 vessels. Approximately, 472 million pedestrians and passengers were examined in 2001 alone. The number of individual transactions increased from 23.5 in Fiscal Year 2000 to 23.7 in Fiscal Year 2001 (U.S. Customs Annual Report 2001).

The U.S. Customs Service was the federal agency responsible for preventing the smuggling of contraband across U.S. borders. It was well known as the primary enforcement agency protecting U.S. borders from the particular threat of drugs, illegal immigration, and more recently of bondaged humans. The agency was equipped with extensive air, land, and marine interdiction forces. The assets conduct continual surveillance over water and all types of terrain. Customs agents have widespread authority to investigate and search all international passengers, including those arriving at airports. In a cooperative effort to stop or at least minimize the international flow of illegal drugs through the nation's borders, customs agents often work in tandem with the Drug Enforcement Agency (DEA).

The challenges facing the U.S. Customs Service continued to evolve with the times. They were also deeply involved in targeting the illegal export of weapons and weapons technology to countries that support terrorism. They were also focusing on the transfer of money used in drug trafficking to

offshore banks. Such scrutiny, however, requires time, and most passengers are focused on arriving at their aircraft before it takes off, continuing with their trip, or simply getting home. In recognition of the desires of most of the law-abiding traveling public, the agency had publicly announced they hoped to process most international air passengers through inspection in 30 minutes or less, while improving enforcement and regulatory processes. In addition, they had pledged, in partnership with the airlines, to obtain advance biographical information on 80 percent of all international air travelers through the use of the Advance Passenger Information System (APIS), expediting the processing of passengers (see Figure 6.1).

Customs officials had also developed the Target Flight Connector System (TFCS), which provides analysis of data elements relating to flights that have the most potential for an enforcement threat. They also used the Interagency Border Inspection System (IBIS) that encompasses more than 24,000 computer terminals located at air, land, and sea ports of entry. The service also uses a sophisticated air surveillance system developed by Decision Science Applications. It is designed to quickly identify legal fliers versus smugglers. The system is operated by radar controllers and is supposed to detect any suspicious flight. Controllers can immediately acquire the plane's identification number, altitude, direction of flight, and airspeed. Appropriate law enforcement officers can then be contacted and their pursuit efforts coordinated. In keeping with many of the changes made after 11 September and the creation of the Department of Homeland Security, the U.S. Customs office was combined with the U.S. Border patrol and is now known as the Customs and Border Protection Bureau.

Customs and Border Protection Bureau

On 28 March 2005, the current Commissioner said, "The priority mission of CBP, specifically including all Border Patrol Agents, is homeland security, nothing less than preventing terrorists and terrorist weapons — including potential weapons of mass destruction —- from entering the United States" (Internet: http://www.customs.ustreas. gov/xp/cgov/border_security/). The U.S. Customs and Border Protection priority mission is to keep terrorist weapons from entering the United States.

FIGURE 6.1 A customs officer checks declaration and packages for a passenger arriving at U.S. international airport. U.S. Customs continues to play a critical role in the overall environment and quality of airport security. (Source: U.S. Customs and Border Protection. www.cbp.gov)

FIGURE 6.2 Command mission: Provide full capable Special Operations Forces to defend the United States and its interests. Plan and synchronize operations against terrorist networks. (Source: U.S. Special Operations Command. www.socom.mil)

As the nation's unified border agency, CBP is strategically positioned at and between ports of entry. This includes carrying out traditional border-related responsibilities, such as stemming the tide of illegal drugs and illegal aliens, securing and facilitating legitimate global trade and travel, and protecting the food supply and agriculture industry from pests and disease (Internet: http://www.cbp.gov/).

Drug Enforcement Agency

Former Director of the DEA, Asa Hutchinson, had acknowledged the challenge regarding the needed reorganization of the agency and the establishment of a cabinet position for Homeland Security. At the time, the DEA had 4763 support employees and 4625 special agents. The agency is assigned the explicit task of enforcing the provisions of the Controlled Substance Act, which monitors the manufacture, distribution, and dispensing of prescription drugs. The Federal Bureau of Narcotics preceded the FBI, which had been established by President Herbert Hoover in 1930 to supervise the proliferation of cocaine and heroin. The level of illegal drug usage had expanded exponentially since that era. Therefore, President Nixon formed the DEA in 1973 as a "super agency" to combat the rapidly proliferating problem. Overall, it is the primary agency for domestic enforcement of federal drug laws and also coordinates and participates in drug investigations overseas.

On 31 July 2003, Karen P. Tandy was confirmed by unanimous consent in the U.S. Senate as Administrator following her nomination by President George W. Bush. Due to a continuing concern about the growing problem of illegal drug infiltration into the United States, the DEA continues to be one of the fastest-growing law enforcement agencies in the United States. It is an ever-present force at both domestic and international airports. Its mission is to enforce domestic drug laws and regulations and to assist other federal and foreign agencies in combating illegal drug production, sale, and transfer.

The DEA aviation program represents a process started in early 1971 when the Bureau of Narcotics and Dangerous Drugs acquired its first aircraft. Over the next few years, additional aircraft were acquired from the U.S. military, and the aviation program was made part of the Special Projects Division. Management of the aviation resources came under the direction of a chief pilot who utilized experienced special agents as pilots, which gave the program the expertise necessary to perform a wide range of enforcement missions that would be impossible with the use of civilian pilots. On creation of the DEA in 1973, the aviation program consisted of 24 aircraft and 41 special

agents or pilots. The program continued to expand, and in 1994, the Aviation Section was granted field division status and renamed the Office of Aviation Operations (OA). The OA makes use of over 100 aircraft and approximately 125 special agents.

In one particular aviation-related case, creatively called "Operation Green Air," the DEA completed an important marijuana trafficking investigation in April 2000. This case was especially unique because it successfully terminated the illegal drug transportation of an organization that used Fedex, a commercial air shipment company, as its exclusive transportation source. The DEA reported that it is, of course, common for drug traffickers to use air transport in their logistics schemes to move quantities of drugs; however, to solely use one company had not been detected prior to this particular operation. The DEA uncovered evidence that a Los Angeles-based criminal group had bribed a number of Fedex employees, mostly drivers but some customer service representatives as well, to facilitate in the delivery of marijuana. The employees were paid to make sure that marijuana shipments were appropriately loaded on aircraft traveling between several major distribution areas. The bribed employees also provided security for the shipments while they were under Fedex control. Other employees manipulated corporate billing and accounting to provide for free shipping services. The DEA estimates that over 4000 packages were successfully airlifted in this manner, accompanied by the Fedex guarantee of pick up by 4 p.m. and next day delivery by 10 a.m.

The DEA conducted an extensive 18-month investigation to unravel the scheme. According to DEA officials, "…over 100 individuals, including 25 Fedex employees, and the seizure of 34,000 pounds of marijuana and $4.2 million in currency and assets" were involved. In addition, the DEA effectively dismantled the target organizations, which had shipped at least 121 tons of marijuana valued at $145 million over the past two years" (Internet: http: //www.usdoj.gov/ dea/major/greenair. htm., 4 July 2001).

Federal Bureau of Investigation

The FBI was originally known as the Bureau of Investigation (BOI). Attorney General Charles J. Bonaparte, at the request of President Theodore Roosevelt, ordered the creation of an investigative arm of the Department of Justice in 1908. The BOI began operations with nine special agents. By 1924, the time J. Edgar Hoover was named Director, the BOI had approximately 650 employees, including 441 special agents. Shortly thereafter, Director Hoover fired special agents he considered unqualified and began to professionalize the organization. He abolished the seniority rule of promotion and introduced uniform performance appraisals. The Bureau doubled in size in the 1930s.

It was renamed in 1935 and became one of the primary investigative agencies in the U.S. government. It too plays an important role in airport security. The FBI in recent times has jurisdiction over nearly 200 federal crimes. The agency is especially well known for its professionalism, which is perpetuated by the extensive training of its agents and thousands of local law enforcement officers who receive supplemental training at the FBI National Academy. As of the year 2000, the agency had over 11,000 active agents and a budget of over 3 billion U.S. dollars. The agency has five priorities including terrorism, organized crime, foreign intelligence operations in the United States, federal drug offenses and white-collar crime.

In 1976, the "Levi Guidelines" severely restricted the ability of the FBI to investigate domestic terrorist groups and their support structures. Levi had established a criminal standard "for domestic security investigations." The FBI was required to have some reason to believe that a group was actually involved in or was about to be involved in criminal activity before it could begin investigating an extremist group. Under these guidelines The *Wall Street Journal* (1984) reported that domestic security investigations declined from 4868 just prior to the Levi Guidelines to 38 in mid-1980s. The FBI even terminated investigations of such terrorist groups as the Weather Underground Organization and the Black Liberation Army (BLA).

On the other hand, in March 1983, Attorney General William French Smith, in the aftermath of the Iranian hostage crisis, relaxed some of the restrictions on collection of domestic intelligence. He amended the former Levi rules that had been established after Congressional hearings in 1975 and

1976, whose heavy criticism of the FBI had exposed alleged abuses. The Smith Guidelines required only a criminal nexus for investigation. In effect, the FBI was permitted to investigate a group if it was part of an ongoing criminal enterprise rather than if it had committed or was about to commit a specific criminal act. Thus, the Smith Guidelines retained a criminal standard, but in looser form. They also relaxed several Levi restrictions regarding the use of informants and other investigative techniques. Other legal impediments to effective counterterrorism intelligence collection existed in provisions of the Freedom of Information Act (FOIA) and in the Federal Tort Claims Act. By granting wide public access to federal government information, the FOIA had inhibited recruitment of effective informants in terrorism and organized crime cases. Informants understandably were reluctant to divulge information to federal authorities if they believed their identities could be revealed to their terrorist or organized crime colleagues by an FOIA request.

On 2 November 1979, Joanne Chesimard, a leader of the BLA serving a life term for the murder of a New Jersey state police officer escaped from prison with the aid of her terrorist comrades. After authorities examined her cell, they found 327 documents, all of which were FBI reports, and were obtained by her through the FOIA. Not only was this particular individual able to conclude the identification of informers who provided information that made it easy to detect her activities, the results of her efforts went to the very heart of the operations of the Bureau and other enforcement agencies. She had learned insider techniques and how to anticipate what the FBI would do in any given situation.

The Federal Tort Claim Act also has deterred effective domestic security investigations by holding individual law enforcement officers personally liable for alleged violations of constitutional rights committed in the course of authorized investigations. FBI agents, for example, may feel reluctant to open or to pursue vigorously an investigation if they fear a lawsuit brought by the subject of the investigation or by groups such as the American Civil Liberties Union (ACLU).

International terrorism came directly to the shores of the United States in the 1990s, and the Anti-Terrorism and Effective Death Penalty Act of 1996 gave the Bureau additional resources to meet the increased demands. Several Presidential Decision Directives issued during the latter part of the decade delineated the FBI's leadership role in countering terrorism. The federal structure had come under considerable criticism for failing to coordinate antiterrorism activity, assess and analyze accurate intelligence, and act quickly to prevent incidents. Acts of international terrorism at the World Trade Center in 1993 and the Atlanta Olympics as well as several poorly handled hostage situations had forced the FBI to bolster its mission in this area. At the time, the FBI had assigned approximately 500 agents to contend with the heightened domestic threat (Internet: http://www.fbi.gov). The predictive deficiencies of the program at the FBI were once again self-evident on 11 September 2001 and may have contributed to the tragedy.

As a result, Director Mueller announced plans to further reorganize the agency. The agency's new strategic focus is to be to protect the United States from terrorist attacks. He plans to restructure the counterterrorism division to "redefine the relationship between headquarters and the field" and to "shift from reactive to preventive orientation." The proposed shift in manpower will move 400 agents from narcotics, 59 agents from white-collar crime, and 59 agents from violent crime units to 480 counterterrorism field agents and another 38 agents to a security and training divisions (Internet: http://www.fbi.gov/terrorinfo/terrorism.htm, pg. 1, 11 June 2002). The FBI's mandate is established in Title 28 of the United States Code (U.S. Code), Section 533, which authorizes the Attorney General to "appoint officials to detect...crimes against the United States." Other federal statutes give the FBI the authority and responsibility to investigate specific crimes.

In the past 10 years, the FBI has already had its budget relating to terrorism tripled. In fiscal year 2006, the FBI's total budget was approximately $8.7 billion, including $495 million in program increases to enhance counterterrorism, counterintelligence, cyber-crime, information technology, security, forensics, training, and criminal programs. The number of agents has also significantly increased as well as efforts to improve cross-communication between agencies to exchange information on terrorists. The CIA passed the names of over 100 suspected associates of Usama bin

Laden just in the last several years. Two of them, Khalid Al-Midhar and Nawaq Alhazmi, later crashed an airplane into the Pentagon in September 2001. As has long been the case at the FBI, the agency is at its best in collecting evidence against known criminals. They have not been as successful in gathering intelligence and anticipating criminal activity before it happens. As discussed in a previous chapter, there is no universally accepted single definition of terrorism. The FBI defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." The FBI further describes terrorism as either domestic or international, depending on the origin, base, and objectives of the terrorist organization.

Domestic terrorism involves groups or individuals who are based and operate entirely within the United States and Puerto Rico without foreign direction and whose acts are directed at elements of the U.S. Government or population.

International terrorism is the unlawful use of force or violence committed by a group or individual who has some connection to a foreign power or whose activities transcend national boundaries, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives (Internet:http://www.fbi.gov).

The agency assists airport operations in several unique ways. For example, the FBI's identification division is often called in to identify victims of major airline crashes. The FBI laboratory is one of the largest crime laboratories in the world. These services are provided free of charge to all law enforcement agencies in the United States. The ability to quickly identify passengers who are victims of a terrorist attack is particularly useful to aviation security personnel. The Automated Fingerprint Identification System (AFIS) converts fingerprints into algorithms; that is, it uses the converted algorithms, or sets of mathematical equations and compares them to fingerprints of individuals that need to be identified. Using the automated program, law enforcement agencies can search and compare millions of samples in minutes. When combined with another new tool, Live Scan™, which electronically scans fingerprints instead of using printer's ink, combinations can be made quickly and easily. Of course, the system is of no assistance in identifying victims unless they have a fingerprint on file. Millions of Americans do, however, as a result of job applications, military service, and the like.

The FBI is also an integral part of the National Domestic Preparedness Office, which is the clearinghouse for state, local, and federal weapons of mass destruction information and assistance. Other members include the Federal Emergency Management Agency (FEMA), the Environmental Protection Agency (EPA), the Department of Energy, the Department of Defense, and Health and Human Resources. Contact can be made with this organization at FBI, National Domestic Preparedness Office, RM 5214, 935 Pennsylvania Ave., Washington, D.C., 202 324-9026 (Internet: http://www.ndpo@leo.gov).

The FBI remains the primary law enforcement agency in the battle to protect the United States from terrorists domestically, even though the demarcation between what is domestic and what is international is blurring. In February 2008, for example, the FBI participated in an operation involving the very deadly chemical agent ricin found in a Las Vegas hotel room and possibly linked to a connection in Utah. Ricin can be a powder, a mist, pellets, or dissolved in water. Depending on the form of the poison, as little as 500 micrograms, the size of a pinhead, can kill an adult. The poison gets inside cells and stops them from making the proteins they need. Without proteins, cells die sometimes causing fatality. The FBI used sealed search warrants after taking advantage of powers granted them under the Patriot Act to gain access to a home and some storage units. The FBI's expertise in dealing with these situations was critical to public safety. The only legal use for ricin is cancer research, according to the Centers for Disease Control and Prevention.

As previously stated, the Patriot Act increased the powers allocated to the FBI, especially in wiretapping and monitoring of Internet activity. The extension of this authority is undergoing increased debate. One of the most controversial provisions of the act is also the so-called *sneak and peek* provision, permitting the FBI power to search a house in secret, and not requiring them to notify the residents for several weeks afterward. Under the Patriot Act's original provisions, the

FBI also resumed accessing the library records of those who are suspected of terrorism, something it had not sought to do since the 1970s.

The U.S. Marshals

The U.S. Marshals Service is the oldest federal law enforcement agency in existence. Congress created the service over 200 years ago by means of the Judiciary Act of 1789 (28 USC § 561). As part of the federal judicial system, the agency is charged with carrying out all lawful orders issued by federal judges, Congress, or the President. Their primary mission is to protect the federal courts and ensure effective operation of the judicial system. As an interesting footnote, during the Cold War, they were also responsible for swapping spies with the former Soviet Union. Today the service supports the needs of 94 districts spanning the continent as well as Guam, the Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands. Headquartered in Arlington, VA, the agency employs more than 4000 deputy marshals.

They also provide a particularly unique service with regard to aviation and the transportation of prisoners. "The U.S. Marshals Service assumes custody of individuals arrested by all federal agencies and is responsible for the housing and transportation of prisoners from the time they are brought into federal custody until they are either acquitted or incarcerated (Internet: http://www.usdoj.gov/marshals/prisoner.html). Once a prisoner is convicted, the U.S. Marshals retain the responsibility of delivering the prisoner to a specific institution for service of sentence. Carriage of passengers under the control of armed law enforcement escorts was provided for in FAR Section 108.21 and now TSA 49 CFR Chapter XII, Part 1544.221.

In 1995, the Immigration and Naturalization Service and the U.S. Marshals combined air fleet assets to create the Justice Prisoner and Alien Transportation System (JPATS). Costs and the consolidation of federal resources necessitated the move and have established a very effective and coordinated system for transporting both prisoners and criminal aliens. Most of the prisoners are transported aboard service-owned aircraft, but not all. Some are still transported by commercial aircraft even though JPATS provides the more economical and secure means for transportation. When JPATS is not utilized, the TSA regulations apply to the transportation of prisoners aboard commercial aircraft.

JPATS acquired many agency airplanes at no cost from the Government Surplus Property Program and the Asset Seizure and Forfeiture Program. It is, aside from the military, the only government-owned, scheduled prisoner transport system in the world. The system serves over 40 cities and has some unique aspects. Deputy Marshals, Aviation Enforcement Officers, and Aviation Safety Officers are all involved. They are strategically positioned throughout the aircraft during flight. In addition, the prisoners all wear handcuffs and leg irons. Local law enforcement assists in ground security and is stationed at each airport transfer point (Internet: http://www.usdoj.gov/marshals/usmshist.html).

As stated, the airlines, however, are often tasked with transporting alleged nonviolent prisoners and illegal aliens. Problems arise if the individual being transferred does not turn out to be nonviolent after all. The airlines, and supporting ground security and law enforcement officers, simply are not equipped to handle an unruly prisoner or illegal alien if they really want to escape. Additionally, once the aircraft becomes airborne the problems are even more acute. Other passengers and air crew become readily available hostages. Plus firing a weapon inside a pressurized aircraft is an extremely dangerous maneuver, limiting the options available to the escort officer.

Recently, on 24 January 2002, John Walker Lindh, the alleged American Taliban, appeared in U.S. Magistrates Court in Alexandria, VA. U.S. Marshals accompanied him. Currently, the Marshals are responsible for the detention and transportation of both John Walker Lindh and Zakarious Moussaoui, the first defendant charged in the 11 September attack (Internet: http://www.usdoj.gov/marshals. pg. 1, 11 June 2002). Representative of the amount of work they contribute to the criminal justice system, in 2003, U.S. Marshals captured over 34,000 federal fugitives and assisted in the capture of over 27,000 state or local fugitives.

Department of Homeland Security

The Bush Administration announced on 6 June 2002 an attempt to revolutionize the method by which the government seeks to protect the United States from internal and external forces. The agency consolidated many existing agencies, including the entire Immigration and Naturalization Service, into one department. The new department was divided into separate divisions to include: border transportation and security, emergency preparedness, information analysis and infrastructure protection, and chemical, biological, and nuclear countermeasures.

Border transportation and security enveloped the entire Immigration and Naturalization Service from within the Department of Justice, the Customs Services from the Department of the Treasury, the Coast Guard from the Department of Transportation, Animal and Plant Health Inspection Service from the Department of Agriculture, the Federal Protective Service from the General Services Administration, and the new Transportation Security Administration.

Emergency preparedness consolidated FEMA; chemical, biological, nuclear response services from Health and Human Services; the emergency support team from the Department of Justice; the Office of Domestic Preparedness from the Department of Justice; the nuclear incident response section from the Department of Energy; and the national domestic preparedness office from the FBI. The Office for Domestic Preparedness (ODP) is the principal component of the Department of Homeland Security responsible for preparing the United States for acts of terrorism. In carrying out its mission, ODP is the primary office responsible for providing training, funds for the purchase of equipment, support for the planning and execution of exercises, technical assistance, and other support to assist states and local jurisdictions to prevent, plan for, and respond to acts of terrorism. ODP launched its Fiscal Year 2003 State Homeland Security Assessment and Strategy (SHSAS) process on 1 July 2003. As part of this effort, ODP had refined the SHSAS process that was originally established in Fiscal Year 1999.

The new process allows states and local jurisdictions to update their needs assessment data to reflect post-September 11, 2001 realities, as well as identify progress on the priorities outlined in their initial homeland security strategies. Furthermore, the refined process will serve as a planning tool for state and local jurisdictions, and will assist ODP and its partners in better allocating federal resources for homeland security. Concurrent with the launch of the SHSAS process, ODP has also activated a revised Online Data Collection Tool. The tool allows states and local jurisdictions to input data from the assessment section of the SHSAS online, without the need to develop complex systems to support the required data collection. The tool also serves as the medium for each State Administrative Agency (SAA) to develop and submit a revised state homeland security strategy. The Online Data Collection Tool may be accessed through the following link: https://www.dct.odp.dhs.gov/dct/.

Directorate of Information Analysis and Infrastructure Protection: IAIP consolidates intelligence from both the FBI and CIA, and combined the Critical Infrastructure Assurance Office from the Department of Commerce, the Federal Computer Incident Response Center from the General Services Administration, the National Communications Systems division from the Department of Defense as well as the National Infrastructure Protection Center from the FBI. It has the capability to identify and assess current and future threats to the Nation, map those threats against vulnerabilities, issue timely warnings, and take preventive and protective action. The directorate analyzes information from multiple sources pertaining to terrorist threats.

The Department's threat analysis and warning functions support the President and other national decision-makers responsible for securing the homeland from terrorism. It coordinates and, as appropriate, consolidates the federal government's lines of communication with state and local public safety agencies and with the private sector, creating a hopefully more coherent and efficient system for conveying actionable intelligence and other threat information.

The IAIP Directorate also administers the Homeland Security Advisory System.

Indications and Warning Advisories. In advance of real-time crisis or attack, IAIP provides the following:

- Threat warnings and advisories against the homeland including physical and cyber events.
- Processes to develop and issue national and sector-specific threat advisories through the Homeland Security Advisory System.
- Terrorist threat information for release to the public, private industry, or state and local governments.

Partnerships. The IAIP team will establish the following:

- Partnerships with key government, public, private and international stakeholders to create an environment that enables them to better protect their infrastructures.
- Awareness programs, development of information sharing mechanisms, and sector focused best practices and guidelines.

National Communications System. The IAIP team provides the following:

- Coordination of planning and provision of National Security and Emergency Preparedness (NS/EP) communications for the Federal government (Internet: http://www.dhs.gov/)

Chemical, biological, nuclear countermeasures includes the Lawrence Livermore National Laboratory, civilian biodefense research programs from Health and Human Services, and the Plum Island Animal Disease Center from the Department of Agriculture.

Transportation Security Administration

In November 2001, President George W. Bush signed into law the Aviation and Transportation Act (P.L. 107-71) creating the Transportation Security Administration within the Department of Transportation. The act specifically tasked the TSA with responsibility for security "in all modes of transportation that are exercised by the Department of Transportation." The TSA interpretation of the law, in conjunction with Presidential Directive (PDD) 63 also placed pipeline security within TSA jurisdiction, along with the other modes of transportation. Overall, the range of duties included general transportation security, intelligence coordination, threat and vulnerability assessment, oversight and enforcement, and mitigation efforts. However, due to the obvious threat to aviation, the TSA primarily focused on the aviation aspect during its first year of operation.

Soon thereafter, on 25 November 2002, President Bush also signed the Homeland Security Act of 2002 (P.L. 107-296), formally establishing the Department of Homeland Security (DHS). The Act transferred the TSA to the DHS. During the following two years the TSA has expanded its efforts in the direction of the other modes of transportation. On 17 December 2003, Presidential Directive (PDD) 7 clarified the agencies responsibilities for identifying, prioritizing, and protecting critical infrastructure. It also instructs the DOT to collaborate in regulating the transportation of hazardous materials by all modes of transportation, as well as requiring DHS to collaborate with "appropriate private entities" (P.L. 107- 296, Para. 25.).

The TSA was specifically created after 11 September to screen passengers and baggage at 429 of the nation's airports. The law bans private companies from airports but allows their return by 2005 if they are approved by the government. TSA was given a budget of $4.8 billion and initially hired 65,000 employees, 54,000 of which were screeners. Screeners, who are not compensated particularly well considering the responsibility they have, are actually paid $23,600 to $35,400 per year plus federal benefits; depending on their experience level. In March 2003, the agency announced it intended to cut 6000 airport screening jobs. The first 3000 lost their jobs in September 2003 and the second by September 2004. Employees attribute the cutbacks to mismanagement.

Three private companies are already operating security checkpoints at the San Francisco, Kansas City, and Rochester, NY airports under a $127 million pilot program. Department of Homeland

Security estimates that as many as 25% of the nation's airports will eventually return to private screeners. Key dates in the TSA's opt out program are as follows:

- 19 November to 10 December 2004: Airports could apply with TSA to opt out of the federal screening program. In late 2004, TSA began prequalifying private security firms that seek to provide passenger and baggage screening services.
- December 2004 to February 2005: Selection of airports for participation in the Screening Partnership Program started.
- Spring 2005: TSA will select the private screening firms that have qualified. Airports will have input into the selection process.
- Late 2005: Screening operations will be transferred to qualified airports.

Some large firms such as Argenbright (now Cognisa), Wachenhu, and Huntleigh were actually forbidden to engage in screening activities in the United States after September 11. Wachenhut is lobbying to return and is doing a profitable business overseas, including having provided screening at the Athens Airport during the Olympics in Greece in August 2004. Advocates of federal screening believe the government raised the standards and recruited better-trained employees, but critics would strongly disagree.

The Immigration and Naturalization Service, U.S. Citizen and Immigration Service

The Immigration and Naturalization Service, now the U.S. Citizen and Immigration Service (USCIS), is charged with the task of monitoring and policing the flow of immigrants into the United States. They have the almost Herculean task of patrolling the borders of the continental United States and American territories to ensure that illegal immigrants do not enter the country. Their jurisdiction encompasses approximately 8000 miles of border. Consecutively, they apprehend and deport illegal aliens who have not complied with U.S. naturalization laws. Border management units consist of Border Patrol and Inspections, as well as Interior Enforcement units. 1 March 2003, saw the U.S. Immigration and Naturalization Service (INS) transition into the Department of Homeland Security (DHS) as the U.S. Citizenship and Immigration Services (USCIS), and the INS ceased to exist. More specifically, the Homeland Security Act of 2002 officially transferred the INS functions to the DHS, and immigration enforcement functions were placed within the separate USCIS.

The President nominated and the Senate confirmed Eduardo Aguirre to lead the USCIS. Robert Divine followed him, and as of December 2005, Dr. Emilio T. Gonzalez was appointed the current Director. The organization is responsible for the administration of immigration and naturalization adjudication functions and establishing immigration services policies and priorities. These functions include (internet: http://www.uscis.gov/aboutus.):

- Adjudication of immigrant visa petitions
- Adjudication of naturalization petitions
- Adjudication of asylum and refugee applications
- Adjudications performed at the service centers
- All other adjudications performed by the INS

Fifteen thousand (15,000) federal employees and contractors working in approximately 250 headquarters and field offices around the world comprise the agency. Every day, USCIS completes more than 135,000 security checks on individuals seeking benefits, and in Fiscal Year 2004, a total of 35 million background checks were conducted (Internet: http://uscis.gov/graphics/publicaffairs/USCIS TodayAugust05.pdf). On 13 July 2005, DHS Secretary Michael Chertoff announced a six-point agenda for the department designed to improve how the organization addresses the present threat level. The agency is particularly unique in that, unlike most other federal agencies, USCIS is funded almost entirely by user fees. Under the Fiscal Year 2008 budget proposal, direct congressional

appropriations will make about 1 percent of the USCIS budget, and about 99 percent of the budget will be funded through fees. The total USCIS Fiscal Year 2008 budget is projected to be 2.6 billion U.S. Dollars (Internet: http://www.uscis.gov/files/ pressrelease/ FY08 Budget 020507FS.pdf).

Inspection units are assigned the task of enforcing and administering U.S. immigration laws by inspecting all persons seeking admission to or transiting the United States at air, land, and sea port facilities. Inspectors make determinations regarding the eligibility of applicants seeking admission to the United States on a daily basis. Each inspector is charged with intercepting terrorists, smugglers, criminals, and undocumented aliens. Inspectors are authorized to search the applicant and their possessions without a warrant. The program also provides for the preinspection of passengers overseas prior to flights destined for the United States. In detail, USCIS personnel work directly with foreign governments and air carriers to assist them in identifying passengers without the proper paperwork and preventing them from boarding aircraft destined for the United States. The inspectors are also involved in the training of domestic and international air carrier personnel.

The USCIS, as does other law enforcement agencies, possesses the tool of prosecutorial discretion. This discretion authorizes the agency to decide when to exercise its enforcement authority. The agency exercises this discretion every day in one form or another. However, attention was focused on the former INS after passage of the Illegal Immigration Reformation Immigrant Responsibility Act in 1996 due to allegations of discriminatory abuse (Internet: http://www.ins. usdoj.gov/graphics/lawenfor/index.htm). It was alleged that INS personnel were using their discretion arbitrarily, singling out minorities for detention, and performing intrusive searches. The INS, now USCIS, has since gone to great lengths to train personnel to restrict their activities to be in conformance with all applicable laws.

It has been reported that the agency deports more than 23,000 illegal immigrants a year on commercial air carriers. The Detention and Deportation Branch is responsible for safely and humanely detaining and deporting illegal aliens or aliens who have violated U.S. laws and are being deported. Most of the individuals deported have been indicted for criminal misconduct. Some high-risk deportees are considered such a risk that armed agents escort them. All other deportees travel on board the aircraft unescorted to the dismay of the airlines. Agency policy is to escort deportees when they consist of a group larger than 12, groups of 11 or fewer travel unescorted, again placing a burden on the airlines.

It is not surprising that the transport of these people often presents security problems. Even if the deportees are not violent offenders, they are being sent somewhere against their will, automatically placing them in the category of a potential escape risk. It is not entirely unimaginable that a group or an individual could take over an aircraft or attempt to do so. The Air Line Pilots Association (ALPA) has in the past expressed profound concerns over the practice of deporting individuals on commercial flights without an escort. In testimony before Congress, an ALPA representative made the following statement, which glowingly describes the irony of current policy:

> "Ironically, the INS's own deportee escorts refuse to operate their deportee transport vehicles unless there are at least two of them in each vehicle, even though the deportees are handcuffed and often in leg irons. There is an obvious problem when these vehicles are allowed to pull up along side of our aircraft and unload deportees, who moments before were in handcuffs, to ride unescorted in the seat next to Grandma." (Internet: http://www.alpa.org/internet/tm/tm061198.htm. pg. 5, 14 July 2001)

Prior to 11 September, the system was completely geared toward easing the way for commerce, in the form of tourism, business, or education. The manual still requires customs to exclude immigrants who incite or direct terrorist activity. Statements by immigrants of a general nature who do not directly advance specific acts of terrorism are not automatically a basis for exclusion, however offensive the statements might be. Therefore, Hani Hanjour, identified as the pilot who flew the jet that slammed into the Pentagon, began blending into the American landscape with a $110 application for a 4-week English course. He only had to prove that he had paid for the lessons. He never

turned up for class. Two other hijackers, who had crashed planes into the World Trade Center, Mohammed Atta and Marwan al-Shehhi, entered the United States on tourist visas. While their applications for student visas were pending, they had already completed flight training at school in Florida. Much to the embarrassment of the INS, those visas were in fact granted 6 months after the 11 September tragedy. Clearly change was required.

Unfortunately, there is currently an exceptionally high employee turnover rate at the INS. The agency has about 16,000 officers, about 500 fewer than authorized. Admittedly, it hired 1499 agents during fiscal year 2002, but also lost 1459 veterans to the TSA. Employee's morale is not at an all-time high, and care needs to be taken to maintain the proficiency of the institution. The agency processes about 90,000 asylum applicants, interviews about 70,000 refugee applicants, while naturalizing another half million new citizens. Each day, USCIS employees process more than 135,000 national security background checks, issue 7000 permanent resident cards, and record more than 8000 sets of fingerprints at 130 Application Support Centers (Internet: http://www.uscis.gov/files/pressrelease/FY08Budget020507FS.pdf).

The Border Fence and The Real ID Card Program

Many Americans have called for increased security along the U.S.'s southern border by building a wall. The response from Mexico has been quick and harsh. Luis Ernesto Derbez, foreign secretary to Mexican President Vincente Fox commented in 2005, "Mexico is not going to bear, it is not going to permit, and it will not allow a stupid thing like this wall." The border between Mexico and the United States extends some 2000 miles, and the barrier systems along the border vary greatly. The proposal for the barrier came the day after U.S. Homeland Security Secretary Michael Chertoff outlined plans to increase security along U.S. borders. Chertoff's strategy includes the construction of a 14-mile wall near San Diego and the hiring of more federal agents.

The House bill, passed on a 239 to 182 vote, included a proposal to build 700 miles of additional fence through parts of California, Arizona, New Mexico, and Texas. It would have also enlisted military and local law enforcement to help stop illegal entrants and require employers to verify the legal status of their workers. The first installment, the True Enforcement and Border Security Act called for thousands of new border patrol officers, immigration investigators, immigration judges, and attorneys. Later, on 17 May 2006, the U.S. Senate proposed a similar bill (S. 2611) that would have authorized 370 miles of triple-layered fencing and a vehicle fence. Although that bill died in committee, eventually the 109th Congress passed the Secure Fence Act of 2006 that was signed by President Bush on 26 October 2006. The version authorizes and partially funds the "possible" construction of 700 miles (1125 km) of physical fence or barriers along the border. Currently, there is an allocation of 1.2 billion U.S. dollars to the Department of Homeland Security marked for border security, but not specifically for the border fence. A 2007 Rasmussen Report survey reported that polled Americans favored building a fence along the U.S. border with Mexico, by a margin of 56 percent in favor and 31 percent against (Murray, 2007). Construction of the fence has lagged and there have even been accusations that in places a part of the fence has been built on Mexican territory. Any further construction will likely depend on the results of the 2008 election.

At the end of 2007, Secretary Michael Chertoff, DHS, outlined four priorities for USCIS in 2008. In a major speech he reiterated the need for continued priorities related to the improvement of immigration control and border security. The Secretary called for a program that would reform the immigration process and recognize some rights for the approximately 12 million illegal immigrants currently in the United States. However, to prevent further illegal immigration, he reiterated plans concerning the building of an additional 380 miles of fencing along the U.S.-Mexico border and building up the total number of 18,000 Border Patrol agents. Chertoff also defended the e-Verify system, a controversial new initiative that can match employee social security numbers to identification records to identify illegal immigrants. He also commented on the further development of a standardized secure identification card, the Western Hemisphere Travel Initiative, which will mandate that all U.S. citizens show an approved type of identification, such as a new Enhanced Driver's License, before returning to the United States by land. The DHS is expected to issue the

final regulations for the Real ID program in 2008. Other priorities include expanding the Einstein Program to further improve national cybersecurity.

The federal government and businesses across the United States are at an impasse as to how to effectively enforce the Real ID Act. The bill was established in 2005 by the DHS and makes it difficult for individuals to obtain illegitimate forms of identification such as drivers' licenses. Few disagree with the DHS's goal of keeping terrorists out of the country; however, many businesses have difficulty enforcing the act due to lack of funding and flaws in the department's e-Verify system. The e-Verify system checks workers' names and Social Security numbers against government databases to make sure the information is credible, but flaws in the system account for a high number of mistakenly flagged names — one in ten — among foreign-born U.S. citizens. Secretary Chertoff acknowledged some of the funding flaws and says new regulations will soon be issued to "satisfy some of these concerns about cost," but has cautioned states and businesses to avoid not complying with the act.

9-11 Commission

The National Commission on Terrorist Attacks Upon the United States (also known as the 9-11 Commission) was an independent, bipartisan commission created by congressional legislation and the signature of President George W. Bush in late 2002. It was chartered to prepare a full and complete account of the circumstances surrounding the 11 September 2001 terrorist attacks, including preparedness for and the immediate response to the attacks. The Commission was also tasked with providing recommendations designed to guard against future attacks. On 22 July 2004, the Commission released its public report, which is available for download from http://www.9-11commission.gov/. Certainly one of the first government publications to become a best seller, the report is also available in bookstores nationwide and from the Government Printing Office. The Commission consisted of ten members and completed its work on 21 August 2004. Chaired by former New Jersey Governor Thomas Kean, the Commission was composed of five Democrats and five Republicans.

The Commission's final report comprises a very lengthy book, based on extensive interviews and testimony, but its primary conclusion was that the failures of the U.S. Central Intelligence Agency and Federal Bureau of Investigation permitted the terrorist attacks to occur and that had these agencies acted more wisely and more aggressively, the attacks could potentially have been prevented. Because the investigation was controversial and politically sensitive, many participants had been criticized during the process. The report concludes that the U.S. government was simply not active enough in combating the terrorist threat before 11 September. It also offers evidence of more ties between bin Laden's network and Iran than al'Qaeda's connections with Iraq and Saddam Hussein's regime. For example, Iran had apparently ordered its border guards not to stamp the passports of al'Qaeda members from Saudi Arabia who were traveling through Iran after training in Afghanistan. Allegedly, as many as ten of the 11 September hijackers had benefited from Iran's cooperation in that when they entered the United States, there had been no indication they had ever been to Afghanistan or Iran in their passport record. The report also contains a copy of a 1998 CIA briefing paper to President Clinton warning of a possible hijacking plot as well as a 2001 White House briefing paper to President Bush warning that Usama bin Laden planned an attack within U.S. borders. The full report details a rather lengthy history of intelligence failures leading up to the 11 September attack. For example, the summary of the report specifically lists the following:

- There were several unexploited opportunities.
- Our government did not watchlist future hijackers Hazmi and Mihdhar before they arrived in the United States, or take adequate steps to find them once they were here.
- Our government did not link the arrest of Zacarias Moussaoui, described as interested in flight training for the purpose of using an airplane in a terrorist act, to the heightened indications of attack.

- Our government did not discover false statements on visa applications, or recognize passports manipulated in a fraudulent manner.
- Our government did not expand no-fly lists to include names from terrorist watchlists or require airline passengers to be more thoroughly screened.

Many disagreements and difficulties plagued the commission's efforts. For example, the independent commission in October 2003 accused the FAA of withholding documents. They eventually subpoenaed the records and questioned why the FAA took 29 minutes to notify NORAD of the hijackings. The report specifically made some recommendations. The creation of the following:

- A National Counterterrorism Center. We need unity of effort on counterterrorism. We should create a National Counterterrorism Center (NCTC) to unify all counterterrorism intelligence and operations across the foreign-domestic divide in one organization. Right now, these efforts are too diffuse across the government. They need to be unified.
- A National Intelligence Director. We need unity of effort in the Intelligence Community. We need a much stronger head of the intelligence community, and an intelligence community that organizes itself to do joint work in national mission centers. We need reforms of the kind the military had two decades ago. We need a "Goldwater-Nichols" reform for the intelligence community. The intelligence community needs a shift in mindset and organization, so that intelligence agencies operate under the principle of joint command, with information-sharing as the norm.
- Reform in the Congress. We need unity of effort in the Congress. Right now, authority and responsibility are too diffuse. The Intelligence Committees do not have enough power to perform their oversight work effectively. Oversight for Homeland Security is splintered among too many committees. We need much stronger committees performing oversight of intelligence. We need a single committee in each chamber providing oversight of the Department of Homeland Security.
- Reform in the FBI. We need a stronger national security workforce within the FBI. We do not support the creation of a new domestic intelligence agency. What the FBI needs is a specialized and integrated national security workforce, consisting of agents, analysts, linguists, and surveillance specialists. These specialists need to be recruited, trained, rewarded, and retained to ensure the development of an institutional culture with deep expertise in intelligence and national security.
- Changes in Information Sharing. We need unity of effort in information sharing. The U.S. government has access to a vast amount of information, but it has a weak system for processing and using that information. "Need to share" must replace "need to know."
- Transitions. We need a better process for transitions involving national security officials, so that this nation does not lower its guard every four or eight years.

(The complete report is available at http://www.9-11commission.gov/report/911Report_Statement.pdf.)

The *Implementing Recommendations of the 9/11 Commission Act of 2007* (Public Law No: 110-53) puts into operation, as of 3 August 2007, some of the recommendations of the 9/11 Commission; including mandating 100 percent inspection of all air and sea cargo entering the United States, and a new method of redistributing antiterrorism funding (GovTrack.us. H.R. 1--110th Congress (2007): Implementing Recommendations of the 9/11 Commission Act of 2007, Internet: http://www.govtrack.us/congress/ bill.xpd?bill=h110-1. accessed Mar 3, 2008). According to a review made by Project Vote Smart, the highlights of the bill are summarized as follows (Internet: *http://www.govtrack.us/congress/bill.xpd?bill=h110-1&tab=summary*):

- Provides that the Secretary of the Department of Homeland Security will supply grants to states, urban areas, regions, or directly eligible tribes to be used to improve the ability for first responders to react to and prevent terrorist attacks
- Appropriates funds to the Department of Defense Cooperative Threat Reduction Program and the Department of Energy National Nuclear Security Administration for the purpose of opposing terrorism
- States that all cargo transported on passenger aircraft must be inspected
- Establishes the Privacy and Civil Liberties Oversight Board
- Establishes the State, Local, and Regional Fusion Center Initiative and the Homeland Security Information Sharing Fellows Program
- Requires reports on the implementation of the 9/11 Commission's recommendations with regard to the detention and treatment of captured terrorists

Director of National Intelligence

On 17 February 2005, President George W. Bush named John Negroponte as the first Director of National Intelligence (DNI), a position created due to recommendations made by the 9/11 Commission completed late in 2004. On 21 April 2005, Negroponte was confirmed by a vote of 98 to 2 in the Senate, and subsequently sworn in. The next director, Michael McConnell, holds the U.S. cabinet-level position coordinating all 15 components of the Intelligence Community, and is the principal intelligence adviser to the President and the statutory intelligence advisor to the National Security Council. Creating the post of DNI was one of the recommendations in the report by the House-Senate Intelligence Committee investigating the September 11 attacks. Previously, the Director of Central Intelligence (DCI) oversaw the intelligence community and served as the principal intelligence adviser to the president, in addition to serving as head of the CIA. The DCI's title is now Director of the Central Intelligence Agency (DCIA), and the director serves only as head of the CIA.

Congress has tasked the DNI with a number of authorities and duties, as outlined in the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. They include:

- Ensure that timely and objective national intelligence is provided to the President, the heads of departments, and agencies of the executive branch; the Chairman of the Joint Chiefs of Staff and senior military commanders; and the Congress
- Establish objectives and priorities for collection, analysis, production, and dissemination of national intelligence
- Ensure maximum availability of and access to intelligence information within the intelligence community
- Develop and ensure the execution of an annual budget for the National Intelligence Program (NIP) based on budget proposals provided by intelligence community component organizations
- Oversee coordination of relationships with the intelligence or security services of foreign governments and international organizations
- Ensure the most accurate analysis of intelligence is derived from all sources to support national security needs
- Develop personnel policies and programs to enhance the capacity for joint operations and to facilitate staffing of community management functions
- Oversee the development and implementation of a program management plan for acquisition of major systems, doing so jointly with the Secretary of Defense for the Department of Defense programs, that include cost, schedule, and performance goals and program milestone criteria (Internet: http://www.dni.gov/who_what/061222_DNIHandbook_Final.pdf)

The Intelligence Community

The Director of CIA is the manager of the CIA, the Defense Intelligence Agency (DIA), and the National Security Agency (NSA). The CIA was established in 1947 when President Truman signed the National Security Act into law. The Act tasked the Director of the Central Intelligence Agency (DCI) with coordinating the nation's intelligence activities and evaluating and disseminating intelligence that affects the security of the United States. The CIA is an independent agency. It is responsible to the President, in coordination with the new DNI, and accountable to all Americans, generally through the intelligence oversight committees of the U.S. Congress. Specifically, the CIA's mission is to "… provide accurate, comprehensive, and timely intelligence on national security topics and to conduct counterintelligence activities, special activities, and other functions related to intelligence and national security, as directed by the President (Internet: http://www.cia.gov/cia/information /info.html).

NSA, known as the eavesdropping and code-breaking agency, collects an incredible amount of traffic everyday. Unfortunately, on 10 September 2001, the agency intercepted some messages from Afghanistan in Arabic referring to 11 September as "the big match" and "zero hour." They were not translated until 12 September 2001. The NSA is equipped with an amazing amount of computer power. It intercepts millions of conversations and transmissions every single day. It coordinates traffic from everything from satellites to simple listening devices. The challenge is to identify which intercepted message is of value and which can be ignored. Translation is a huge problem. Nuances, dialects, and simple familiarity among the terrorists and criminals make it difficult to correctly and appropriately understand the exact meaning of a particular conversation. It takes years of training and specialization to accomplish this and a massive artificial intelligence network on top.

All three agencies are facing intense public scrutiny for apparently missing potential signals of a gigantic attack on American soil. The debate sparked a discussion about revamping the intelligence community and improving coordination and information sharing inside the government. This would constitute a Herculean task, especially in light of the classified nature of the information. The critical problem facing all these agencies is the sheer volume of information that they collect. It is virtually impossible to analyze it all in a timely manner, let alone effectuate policy based on it.

The DIA was created in 1961 as the nation's primary military intelligence organization and designated a combat support agency. The genesis of the DIA generally is attributed to the political environment of the 1950s; however, the requirement for a unified military intelligence organization can be traced back to World War II. One of the earliest indications of formal military intelligence cooperation was the Joint Intelligence Committee (JIC) created in 1941 as a coordinating mechanism of the Joint Chiefs of Staff organization The JIC consists of the directors and representatives of the intelligence organs of the Army, the Navy, the State Department, the Board of Economic Warfare, and the Coordinator of Information (COI). Its mission is to "provide timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers" (Internet: http://www.dia.mil/thisisdia/mission.htm). A workforce of approximately 11,000 people provide foreign military intelligence for the Department of Defense.

During the 1970s, the United States was often dependent on other intelligence agencies for information regarding the Middle East. Israel, Jordan, and Lebanon provided some data, but it frequently lacked the detail required to produce qualified analyzed intelligence. HUMINT activities targeted at terrorist organizations were weak to nonexistent. Eventually, the Reagan Administration improved the intelligence community's counterterrorism capabilities. This included increased funding and personnel, the development of small strike forces to respond to terrorist attacks, and a center for evaluating intelligence on terrorism.

At the time, Iran, Syria, Libya, and North Korea were considered supporters of terrorism. If the terrorist threat is seen as simply criminal and primarily a law enforcement problem, the danger could be met by passive measures carried out by law enforcement agencies alone. If, however, terrorism is a form of war or unconventional warfare as the Administration now views it, terrorism is a problem of national security. Consequently, not only law enforcement, but also military and

national security agencies should be used within an overall national counterterrorism policy, both overtly and covertly.

The term covert act has in recent years acquired a sinister connotation, suggesting assassinations, the overthrow of governments, and other extralegal activities. Some covert action, admittedly, includes such measures; however, it also includes propaganda, agents of influence, and nonviolent political, economic, or psychological warfare used to distinguish activities intended to influence other states or parties from intelligence collection. Its principal purpose would be the disruption of terrorist organizations by striking at their internal unity and ability to carry out acts of violence.

Varying forms of low-risk, low-level covert action against terrorists and their organizations could be crafted by intelligence services. For such measures to be effective, however, it is necessary for the United States to have reliable and detailed intelligence on targeted terrorist groups to anticipate accurately the results of such measures, to assure the security of covert operations, and to be able to deny credibly U.S. involvement in the action. Although the use of such techniques against domestic terrorists and their supporters today might be too controversial, they should be employed by counterintelligence and covert action institutions on an international level.

Since 11 September, considerable effort has been expended in an effort to catch and "bring to justice" Usama bin Laden and the members of his organization. Whether the United States continues to be as dedicated to this effort in the current political environment is debatable. Additionally, the cost may outweigh the need to martyr him. According to Michael Scheuer, a 22 year CIA veteran, the effort has been partially suspended. He claims in his book *Imperial Hunts*" that the headquarters unit assigned to bin Laden has fewer experienced case officers now than on 11 September 2001. He also makes the assertion that the CIA is rotating inexperienced officers into the bin Laden unit for short stints of 60 to 90 days. The CIA has denied these allegations. Scheuer has further commented that the CIA has avoided serious efforts to capture bin Laden for many reasons; including insufficiency of evidence should he ever be brought to trial. He has specifically stated,

> The pattern of decision making I have witnessed seems to indicate a want of moral courage, an overwhelming concern for career advancement, or an abject inability to distinguish right from wrong. Questions about the CIA's capabilities are part of a larger debate over reforming U.S. intelligence. Even the CIA's former director, George Tenet, told the Sept. 11 commission that it would take five years to have in place the kind of clandestine service needed to deal with international terrorism and other threats.

There is little argument to the contention that the intelligence community needed some sort of reform. Everyone agrees that on improvement involves developing better human intelligence and analytic capabilities, expanding intelligence sharing with state and local law enforcement agencies, and enhancing foreign language capabilities at the CIA.

Terrorist Screening Center (TSC)

Former Attorney General John Ashcroft in coordination with former Secretary of Homeland Security, Tom Ridge, as well as former Secretary of State, Colin Powell, former FBI Director Robert Mueller, and former CIA Director George Tenet announced the establishment of the Terrorist Screening Center (TSC). The group consolidates terrorist watch lists and provides information around the clock for federal airport screeners and others. The organization allows government investigators, screeners, and agents access to complete accurate and timely information. As previously discussed, the DHS's new Information Analysis and Infrastructure Protection (IA/IP) system allows the department to analyze information and take specific action to protect critical infrastructure. It is unclear if the organization will undergo significant changes in light of the 9/11 Commission's recommendation to reorganize the entire intelligence community.

The Terrorist Threat Integration Center (TTIC) was established to ensure that all members of the federal government's intelligence community have access to the same information. This effort

was meant to enhance intelligence "fusion." The fusion will allow analysts from many agencies to coordinate and not have to view only part of the picture as opposed to the whole. For example, all government employees involved in the war on terrorism will be able to run name checks against the same government watch lists, from the most accurate information databases available. The State Department's TIPOFF program, containing the names of approximately 100,000 suspected terrorists, will provide the initial bases of the database.

Additional efforts have resulted in the FBI making information on subjects of their terrorism investigation available to local and state law enforcement officials through the National Crime Information Center. Over 650,000 law enforcement officers have access to the information. The TSC represents a significant effort on the part of the TSA to integrate counterterrorism efforts by all components of the government. As mentioned it represents at least a first step, as was recommended by the 9/11 Congressional Joint Inquiry, but more changes are likely forthcoming.

In summary, the TSC is a multiagency center. Participants include the Department of Justice, Homeland Security, State Department, and the intelligence community. The FBI administers the program that became operational in December 2003. The general mission is to develop the technical capability for watch list integration at the FBI's Foreign Terrorist Tracking Task Force, where the TSC operations will be absorbed. The TSC was formally established by Homeland Security Presidential Directive and a Memorandum of Agreement between the participating agencies. They will need a variety of tools to be successful.

There has been much scrutiny of the CIA since the terrorist attacks of 11 September 2001, with the majority of discussion centered on the competencies of personnel, working relationships with other agencies, and collection philosophy in general. One controversy has focused on the means of collection. Since the end of the Cold War, supporters of technical intelligence versus human intelligence resources have been at odds within the intelligence community. They will both need to reconcile their differences and optimally utilize both means.

The United States has carried on foreign intelligence activities since the days of the Revolutionary War, but it has only been since World War II that efforts have been formally coordinated. President Franklin D. Roosevelt was concerned about intelligence well before the start of World War II and had requested that a plan for an intelligence service be drafted. He asked that a unique and comprehensive service be created and the Central Intelligence Agency was born. During the war and especially leading up to D-Day, the OSS played a critical role in collection of military intelligence. After the war, the military services protected their areas of responsibility, and the DIA has remained the agency tasked primarily with the collection of military intelligence.

The need for a postwar centralized intelligence system of collection had become self evident. In response, President Harry S. Truman established the Centralized Intelligence Group in January 1946. The group was put under the direction of a National Intelligence Authority composed of a Presidential representative and the Secretaries of State, War, and Navy. Rear Admiral Sidney W. Souers, who had been the Deputy Chief of Naval Intelligence, was appointed the first director of the CIA. George W. Tenet, the director during the events of 11 September 2001 submitted his resignation in June 2004. Publicly, the President reluctantly accepted his resignation, but there was clear evidence that a change was necessary. The Deputy Director assumed his responsibilities until the Senate affirmed General Michael Hayden. His methods, especially the conduct of his carryover Congressional staff, have caused what can only be labeled as "insurrection" within the agency.

About two years after formation, the National Intelligence Authority and the Central Intelligence Group were disbanded. Under the provisions of the National Security Act of 1947, the National Security Council and the CIA came into being. The Act tasked the Agency with coordinating the nation's intelligence activities and correlating, evaluating and disseminating intelligence which affects national security. In 1949, the original Act was supplemented by the Central Intelligence Act of 1949, which permitted the Agency to use confidential fiscal and administrative procedures and exempted the CIA from the usual limitations on the expenditure of federal monies. The Act further

exempted the CIA from being forced to disclose its, "organization, functions, names, officials, titles, salaries, or numbers of personnel employed."

Currently, the director serves as the principal adviser to the President and the National Security Council on all matters of foreign intelligence related to national security. The agency reports regularly to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, as mandated by the Intelligence Oversight Act of 1980 and a number of Executive Orders. Recently, the organization has come under heavy fire for failing to detect and prevent the activities and successes of various terrorist groups around the globe. Additionally, as stated, the special 9/11 Commission has been particularly critical.

United States Postal Inspection Service

The mission of the U.S. Postal Inspection Service (USPIS) is to "protect the U.S. Postal Service, its employees, and its customers from criminal attack, and protect the nation's mail system from criminal misuse" (Internet: http://www.usps.gov/websites/depart/inspect). The USPIS is particularly interested in mail bombs. Even though the postal service processes over 170 billion pieces of mail annually, less than one in a billion will contain a bomb. In light of the fact that the mail is frequently carried on commercial aircraft, that one piece of mail is still significant. The USPIS has disseminated a list of characteristics of mail bombs that have repeatedly been observed. They include the following (Internet: http://www.usps.gov/websites/depart/inspect/bombs.htm):

- Mail bombs may have excessive postage. Normally a bomber does not want to mail a parcel over the counter and have to deal face to face with a postal clerk.
- The return address may be fictitious or nonexistent.
- The postmark may show a different location than the return address.
- Mail bombs may bear restricted endorsements, such as "Personal" or "Private." This is particularly important when the addressee does not usually receive personal mail at the office.
- Mail bombs may display distorted handwriting, or the name and address may be prepared with homemade labels or cut and paste lettering.
- Parcel bombs may be professionally wrapped with several combinations of tape used to secure the package, and may be endorsed "Fragile-Handle with Care" or "Rush-Do Not Delay."
- Letter bombs may feel rigid or appear uneven or lopsided.
- Package bombs may have an irregular shape, soft spots, or bulges.
- Mail bombs may have protruding wires, aluminum foil, or oil stains, and may emit a peculiar odor.

The advice that the postal inspectors give to postal employees applies just as well to security officers who may encounter a suspicious package. First, do not open the package. Second, isolate the suspect package and evacuate the immediate area. Employees are further instructed not to put the package in water or a confined space. If possible, all windows in the immediate area should be opened to assist in venting the potential explosion. Last, do not hesitate to check any suspicious package further, and never be embarrassed about a false alarm. It is always better to inspect harmless packages instead of ignoring a dangerous one.

Congress empowered postal inspectors to "…investigate postal offenses and civil matters relating to the Postal Service." Approximately, 2000 postal inspectors work closely with other law enforcement agencies and local prosecutors to investigate cases. They are federal officers who carry firearms, make arrests, and serve warrants. They operate five forensic crime laboratories that have been put to significant use during the years 2001 and 2002. A coordinated and intensive criminal investigation focused on the anthrax-tainted letters processed through the postal service in late 2001, which resulted in the death of five persons. By the end of June 2002, the FBI and the U.S. Postal Service (USPS) were offering a $2.5 million dollar reward for information leading to the arrest and conviction of the perpetrator. The recent suicide of the primary suspect in the case has

effectively ended further investigative efforts. The investigation combines a criminal investigation with public health concerns. Additionally, pipe bombs discovered in Iowa and Illinois in rural mailboxes, injuring five persons, occupied many agents during April 2002 until the bomber was apprehended on 7 May.

Aviation Mail Security and Hazardous Materials

The safety and security of the mail is the U.S. Postal Service's top priority. The Aviation Mail Security and Hazardous Materials Programs are supposed to provide a safe environment for customers, employees, and the traveling public.

What is hazardous material? Hazardous materials come in a wide variety of forms and can be chemical, biological, radioactive, or a combination thereof. If a material or substance can cause harm to someone or something, it can be considered a hazardous material.

The Postal Service's definition of a hazardous material includes many common household and consumer products. These items may not be hazardous during normal use or storage in your home, but can present a significant hazard when placed in the mail due to vibration, temperature changes, and variations in atmospheric pressure. Some examples of commonly used items restricted or considered hazardous under USPS regulations include perfumes, nail polish, flea collars, flea sprays, aerosols, bleach, pool chemicals, paints, matches, batteries, fuels or gasoline, airbags, dry ice, mercury thermometer, cleaning supplies, items previously containing fuels, glues, and fireworks.

Other items, such as alcoholic beverages (beer, wine, liquor), are not considered hazardous but are prohibited, and boxes displaying such markings are also prohibited.

Resources to Help Determine Mailability

1. Poster of the most relevant information on hazardous materials: Poster 138 – *(PDF)* | *(HTML).*
2. The mailing standards of the USPS: *Domestic Mail Manual 601.8.*
3. Information on what may be mailed and how items must be packaged and labeled: Publication 52, Hazardous, Restricted, and Perishable Mail - *(PDF)* | *(HTML).*
4. Notice on hazardous materials found in all USPS retail locations: Notice 107, Let's Keep the Mail Safe – *(PDF)* | *(HTML).*
5. Notice on hazardous materials available from USPS letter carriers: Notice 128, The Safety of the Mail is Everyone's Responsibility – *(PDF)* | *(HTML).*
6. Post Office lobby poster: Poster 37, Some Things Were Never Meant to Be Mailed – *(PDF)* | *(HTML).*
7. USPS workplace poster: Poster 298, Department of Transportation Hazardous Materials Warning Labels and Markings – *(PDF)* | *(HTML).*

Hazardous Materials' Program

Mailers are responsible for the following:

- Ensuring no hazardous material is mailed unless it is permitted under USPS mailing standards described in the Domestic Mail Manual 601.10.
- Knowing the physical characteristics of the hazardous materials they wish to mail.
- Making sure all USPS regulations are followed regarding the packaging, markings, labeling, and declaration of hazardous materials placed in the mail.

Reused packaging and boxes are only acceptable when all markings and labels are removed or completely marked out so they cannot be read. Regardless of what is actually inside the package, markings or labels for hazardous or restricted materials may prevent the package from being deliv-

ered. For more information, see Domestic Mail Manual 601.5.1.b. Failure to comply with any USPS requirements may result in the delay or nondelivery of an item.

Aviation

Mail Security Program Because of heightened security, all mail pieces weighing over 13 ounces bearing only postage stamps as postage must be presented to an employee at a retail service counter at a post office. (http://www.usps.com/aviationsecurity/welcome.htm.)

Interpol

International police cooperation has been in use since the creation of the International Criminal Police Organization (Interpol). Interpol exists to facilitate the maintenance of a safer world community, especially within the 178 member countries. The organization plays a critical role in tracking terrorists and relating the information to the appropriate law enforcement agency. It has a fundamental objective of overcoming national boundaries to coordinate international efforts to combat crime in whatever form. The development of rapid travel has made it far easier for criminals to move around the planet. Additionally, the complex structures of modern societies and the constant growth of international exchanges provide more and more opportunities for international criminal activity. Their mission specifically challenges the organization to be the world's preeminent organization dedicated to preventing and detecting international crime, including terrorism. It aims to "ensure and promote the widest mutual assistance between all criminal police authorities, within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights and to establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes" (Fooner, 1989).

As early as April 1914, during the First International Criminal Police Congress held in Monaco, legal experts and police officers from 14 different countries and territories studied the possibility of establishing an international criminal records office and harmonizing extradition procedures. The outbreak of World War I prevented any further progress until 1923. The second International Criminal Police Congress met in Vienna, Austria, and established the International Criminal Police Commission. The agency, still essentially a European organization, was created after World War I, at which time counterfeit money was posing a big threat to the economic welfare of European countries. U.S. participation began when J. Edgar Hoover was appointed director of the FBI. He began receiving reports from Interpol in 1925 and increased the FBI's involvement by the late 1930s.

After World War II, another conference, held in Brussels, Belgium, revived the International Criminal Police Commission, and the name Interpol was officially recognized. However, as stated, during the first 15 years it remained mainly a central European organization. The agency consists of a General Assembly, Executive Committee, and the Secretary General. The General Assembly elected current Secretary General Ronald K. Noble beginning a five year term in the year 2000, and he was unanimously reelected to a second five-year term by the 74th Interpol General Assembly in Berlin, Germany, in 2005.

Interpol investigates crimes including trafficking in human beings, crimes against minors, theft of art work, organized crime, counterfeiting, illicit drug trafficking, technology-related crime, environmental crime, and, of course, terrorism. They define terrorism as "a crime, characterized by violence or intimidation, usually against innocent victims in order to obtain a political or social objective." They became extensively involved in the fight against terrorism as a result of a resolution passed at the 54th Interpol General Assembly in Washington, D.C., in 1985. The resolution, AGN/54/RES/1, created a specialized group within the then police division to "…coordinate and enhance cooperation in combating international terrorism" (Internet: http://interpol.int/Public/ Terrorism/default.asp).

The Anti-Terrorism Branch began operations in 1987 and is tasked with matters related to terrorism, firearms and explosives, attacks and threats against civil aviation, maritime piracy, and weapons of mass destruction. The unit seeks to disseminate information on terrorists and terrorist groups

by responding to inquiries from member countries and coordinates sophisticated analysis. They attempt to keep the lines of communication between national police forces, military units involved in battling terrorism, and governments open. Interpol possesses a database called Interpol Weapons and Explosives Tracking System (IWETS) that maintains information on firearms and explosives. It provides current data on firearms manufacturers, identification of firearms, and information on stolen and recovered weapons. It must be remembered that Interpol has no arrest power or the authority to search and seize. It is purely an organization that facilitates cooperation between other police organizations. Interpol has recognized that the effort to combat terrorism must include coordinated efforts to disrupt funding to the terrorists. It has supported the concept that the frequency and seriousness of international terrorist acts are often "…proportionate to the funding the terrorists might get" (Internet: http://www.interpol. com./public/Terror/finance.asp, pp. 1,2; 11 June 2002).

The U.S. National Central Bureau (USNCB) was established to promote a seamless working relationship between the United States and Interpol. The USNCB is the point of contact for international law enforcement within the United States and acts as the U.S. representative to Interpol on behalf of the U.S. Attorney General. It was authorized by 22 U.S.C. 263(a) and is officially part of the Department of Justice, as well as being closely affiliated with Department of Treasury. The published functions of the USNCB are to transmit information of a criminal justice, humanitarian, or other law enforcement-related nature between the National Central Bureaus and Interpol member countries. It also coordinates cooperation between law enforcement agencies of the United States and responds to requests by law enforcement agencies and other legitimate requests by appropriate organizations, institutions, and individuals to and from Interpol.

It should be pointed out that for more than a decade, the National Institute for Standards and Technology has advocated the development of data exchange within the law enforcement community. In the year 2000, the Institute adopted ANSI/NIST-ITL 1-2000, which uses a database format for the interchange of fingerprint, facial, and scar and tattoo mark information. The standard defines a structured framework for representing and exchanging rap sheets, photos, and arrest records into virtually all commercial fingerprint identification systems. Its impact, in conjunction with agencies such as Interpol, and the accessibility, connectivity, and mobility afforded by the World Wide Web will prove to be dynamic.

As evidence of Interpol's success, in March 2008, a man believed to be the world's largest arms dealer, suspected of supplying weapons to al'Qaeda and the Taliban, was arrested in Thailand following a multicountry operation with Interpol's cooperation. U.S. authorities have accused Viktor Bout of conspiracy to provide material support or resources to a designated foreign terrorist organization. He was arrested by the Royal Thai Police at a hotel in Bangkok. Interpol continues to assist in the war on terrorism and to facilitate international police cooperation, even where diplomatic relations do not exist between particular countries.

CONCLUSION

The coordination of all law enforcement efforts at an airport is something like choreographing an intricate dance. The same can be said of law enforcement agencies nationwide. All the players need to be working in tandem, but they might not know who each other are or even if they are present in an airport at any particular time. On top of that, they might not know exactly what kind of case each other is currently working on at any particular time. Airport security officers must be worked into the mix. For example, if a DEA agent is following drug traffickers and the officer is carrying a weapon, it is highly detrimental to the operation for airport security to discover the weapon, thereby exposing the agent as law enforcement. Precise synchronization is essential, regardless of the territorial proclivities of some law enforcement officials.

A significant second problem relates to the lack of communication between agencies. There is a serious laxity disseminating information that may not relate to an immediate threat. When the agencies fail to share information, the big picture is eluded. Worse yet, when they have the information,

they often do not know what to make of it. The series of events and information acquired prior to 11 September 2001 is an unfortunate example. The FBI had been collecting information on international terrorists who were attending U.S. flight schools to learn to fly large aircraft. However, when a Minnesota flight school alerted the FBI of a suspicious student, no bells went off. Based on the events of 11 September, it is safe to surmise that the biggest problem the United States faces is not the simple number of law enforcement personnel on the job, by what organization they are employed, or where they are deployed. The greatest difficulty is communication. They must learn to overcome the bureaucratic tendency to protect territory and not share databases, in short, to integrate agencies that really are not working together.

Additionally, this chapter does not begin to detail all the counterterrorist units deployed around the world. However, it is meant to at least recognize the most famous and to reemphasize some of their successes. Some have been exceptionally productive. Budget restraints have the power to erode the overall effectiveness of these units. Airport security and local airport police cannot really begin to match the expertise of these units of the type discussed. Efforts to make sure they remain a mechanism in the antiterrorism toolbox will be essential in the future. Complacency is the terrorist's friend.

Not enough commitment to the concept can result in flawed missions, and too much zeal can result in the loss of innocent lives. Too little training and inappropriate equipment for the task is also a recipe for disaster. Last but not least, the philosophy of the use of force in retaliation is a slippery slope. The protection of the average citizen's civil liberties must be preserved. Whenever the police or the military become judge and jury, the foundations of a democratic state could be in jeopardy. Much care should be given to the idea that the terrorist hunters not become the terrorists.

REFERENCES

Case of Ireland v. The United Kingdom, Application No. 5310/71. European Court of Human Rights, 1978. Retrieved February 19, 2008 from the European Court of Human Rights web portal.

Conclusions adopted by the JHA Council (12156/01), Brussels, September 20, 2001.

Dobson, Christopher and Payne, Ronald, *Counterattack*: *The West's Battle Against Terrorists,* New York: Facts on File, 1982, pg. 96.

Follain, John Jackal: *The Complete Story of the Legendary Terrorist, Carlos the Jackal*. Arcade Publishing, 1998.

Fooner, Michael, *Interpol Issues in World Crime and International Criminal Justice*, New York: Plenum Press, 1989.

France's GIGN, http://www.specwarnet.com/europe/gign.htm., pg. 2.

Gesell, Laurence E., *The Administration of Public Airports*, Coast Aire Publications, 1981 Pg. IX-15.

GovTrack.us. H.R. 1--110th Congress (2007): Implementing Recommendations of the 9/11 Commission Act of 2007, http://www.govtrack.us/congress/ bill.xpd?bill=h110-1. accessed Mar 3, 2008.

Harding, John, "SAS carries 'ultimate' weapon," *The Daily Telegraph*, 27 October 2001, pg. 4.

http://interpol.int/Public/ Terrorism/default.asp.

http://www.interpol. com./public/Terror/finance.asp, pp. 1,2; 11 June 2002.

http://uscis.gov/graphics/publicaffairs/USCIS TodayAugust05.pdf.

Interrnet: http://www.9-11commission.gov/.

Internet:http://www.alpa.org/internet/tm/tm061198.htm. pg. 5, 14 July 2001.

http://www.bundespolizei.de/nn_249932/DE/Home/06Presse/Infobroschuere__down,templateId=raw,property=publicationFile.pdf/Infobroschuere_down.pdf, pg. 17.

http://www.cbp.gov/.

http://www.cia.gov/cia/information /info.html.

http://www.customs.ustreas. gov/xp/cgov/border_security/.

https://www.dct.odp.dhs.gov/dct/.

http://www.dhs.gov/.

http://www.dia.mil/thisisdia/mission.htm.

http://www.dni.gov/who_what/061222_DNIHandbook_Final.pdf.

http://www.faa.gov/avr/AFS/FARS/far-107.txt., Pg. 9, 22 April 2001.

http://www.faa.gov/avr/AFS/FARS/far-107.txt., pg.11, 22 August 2001.

http://www.fbi.gov.
http://www.fbi.gov/terrorinfo/terrorism.htm, pg. 1, 11 June 2002.
http: //www.ins.usdoj.gov/graphics/lawenfor/index.htm.
http://www.ndpo@leo.gov.
http://www.sealchallenge.navy.mil/.
http://www.uscis.gov/aboutus.
http://www.uscis.gov/files/ pressrelease/ FY08 Budget 020507FS.pdf.
http: //www.usdoj.gov/ dea/major/greenair.htm., 4 July 2001.
http://www.usdoj.gov/marshals/prisoner.html.
http://www.usdoj.gov/marshals/usmshist.html.
http://www.usdoj.gov/marshals. pg. 1, 11 June 2002.
http://www.usps.gov/websites/depart/inspect.
http://www.usps.gov/websites/depart/inspect/bombs.htm.
http://www.usps.com/aviationsecurity/welcome.htm.
Israeli Counter-Terrorists Activity, http://www.ict.org.il/counter_ter/is_ct.htm. pg. 1.
Jackson, James, O., "Death on Track 4," *Time,* 23 August 1993.
Meyr, Eitan, "Elite Gendarmes", *S.W.A.T*, May 2000.
Meyr, Eitan, "Protector if Internal Security," *S.W.A.T,* May 2000.
Meyr, Eitan, "The Israeli Civil Guard," *S.W.A.T*, January 2001, pg. 27.
Miller, David, *The Illustrated Directory of Special Forces*, London, Salamander Books, Ltd., 2002.
Mooney, Paul, "Anti-Terrorism Unit Efficient, But Low Profile," *The Chronicle-Herald/the Mail Star*, 4 May 1995, Pg. A10.
Murray, Joe, "Poll: Americans Frustrated With Immigration Crisis," *Philadelphia Evening Bulletin*, August 21, 2007.
Official Journal of the European Union, C321, December 29, 2006.
Patterns of Global Terrorism: 2000, European Overview, pg. 2.
Ryan, Mike, Mann, Chris, and Stilwell Alexander (2004). *Fuerzas Especiales del Mundo* (in Spanish). Alcobendas, Madrid, pp. 110, 226.
The Wall Street Journal, January 31, 1984, p. 4.
US Customs Annual Report 2001, http://www.customs.ustreasury.gove/reports 2001.

7 Screening — The Last Line of Defense

NEWS

02 November 2001: In Miami a federal investigator sneaks three knives past airport screeners; in Fort Lauderdale undercover sheriff's deputies take a pocketknife and a box cutter through the airport metal detectors and x-ray machines.

22 November 2001: Baggage screening firm at Boston's Logan Airport is reinstated after being fired for hiring criminals and allowing security breaches. Argenbright argues it did not get a hearing before losing its license.

14 June 2002: Government officials insist they can meet Congressional deadlines to put security screeners into all airports by 19 November 2002 and to subject all baggage to the security of bomb-detection devices by 31 December 2002. They declare success in November.

18 May 2005: Union representatives and federal airport screeners call on Congress to pass legislation that would strengthen the Transportation Security Administration and prohibit the privatization of passenger and baggage screening services.

28 August 2005: San Francisco International Airport is one of five airports in a pilot program designed to test whether private companies are a better option than federal screeners.

INTRODUCTION

An airport is a unique transportation center used for the landing and takeoff of aircraft. Its primary purpose is to provide transportation for passengers, freight, and the U.S. mail. Generally, an airport consists of numerous structures designed to facilitate the needs of both aircraft and passengers. Runways provide the means for aircraft to take off and land. Taxiways are paths the aircraft use to reach the terminal building where passengers are boarded and off-loaded. The aircraft parking area at the gates of the terminal is known as the loading apron. The terminal also contains ticket and baggage counters, vendor operations, and security operations. A control tower is usually located near the terminal where air traffic controllers coordinate the movement of aircraft, maintenance, and refueling personnel. Hangers, maintenance facilities, refueling facilities, and navigational equipment complete the basic layout of an airport. Of course, airports also need to offer passenger parking. All of these areas and people must be patrolled and protected by adequate security forces.

Because airports are among the busiest transportation centers in the world, the unhindered continuation of operations is vital to the world economy. In the United States alone, over 500 airports provide services to over 500 million passengers every year. These airports also move over 9 million metric tons of air cargo. Some economists estimate the total annual economic impact on the nation to be approximately 600 billion U.S. dollars annually. Ensuring the safety of all these passengers, freight, and personnel is a crucial part of airport operations. The Transportation Security Administration (TSA) requires that airports provide security measures to ensure the safety of everyone and everything involved. Most passengers are generally aware that security personnel operate metal detectors

and x-ray machines that screen baggage for possible weapons or, inadvertently, illegal substances. Air carriers now also require that each passenger show photo identification before entering an aircraft. However, the job of providing overall security to an airport entails a great deal more.

As stated previously, air carriers, in conjunction with the TSA, routinely exercise 100 percent screening of all passengers and carry-on baggage and will be required to screen all passenger cargo by December 2002. The main terminal is one of the primary security challenges of security officials. Initially, there were three general security concepts for the physical arrangements of the main terminal facility. First, the sterile concourse, second, the sterile boarding area, and last departure gate screening.

As discussed, the courts have consistently upheld the reasonableness of subjecting anyone who travels on an airplane to a search by metal detector and their baggage to x-rays before the person is allowed to board the airplane. The rationale is simply explained in one legal case and provides that (*United States versus Biswell,* 406 US 311 [1972]*)*:

1. It is necessary to prevent hijackings and bombings.
2. The passenger "consents" to the search.
3. The intrusion is administratively limited only to a search for weapons and explosives.

The issues related to the best way to conduct the searches, by what method, where, and for how long were to be determined by trial and error by airlines and airport operators alike. Recently, even the luggage manufacturers have gotten into the mix. Samsonite's engineers, immediately after 11 September, were working on a bag that doubles as a seat for those caught in airport security lines. After being notified that passengers would only be allowed one carry-on item and a personal item, the company came up with an overnight bag with a sturdy pouch that can carry a laptop.

TSA 49 CFR Chapter XII, Part 1540.107, formerly Section 107.20, relates to submission by travelers to the screening process. It specifically states that "No person may enter a sterile area without submitting to the screening and inspection of his or her person and property in accordance with the procedures being applied to control access to that area" (Internet: http://ccfr.access.gpo.gov/otcgi/cgr. pg.1, 19 June 2002). The process of screening is subject to many restrictions, and security personnel have perfected the more expeditious methods of processing passengers and accompanying vendors and airline employees through the procedures. The TSA monitors the screening on a regular basis. Even though it has been criticized heavily, the process is currently serving a basic public need. Any process can always be improved, and the TSA will continue to make adjustments to policies and procedures as needed.

As a result of 11 September, a 19 November 2002 deadline was established for the federal government to assume the responsibilities for screening at airports. In April 2002, the U.S. TSA announced that three companies were selected to develop plans for the takeover. Fluor Enterprises, Inc., Hensel Phelps Construction Co., and Lockheed Martin Corporation received $8.9 million for the plans. Each company was tasked to design plans for replacing the private screener at checkpoints with an all-federal work force. The TSA reviewed the plans and selected Lockheed Martin Systems to implement it. The company and the TSA were all working under a congressionally mandated 19 November 2002 deadline for the complete replacement of employees. Unfortunately, the security of airports may still be at risk for many reasons.

STERILE CONCOURSE

The sterile concourse establishes an area to which access is controlled by the inspection of persons and property in accordance with an approved security program. Passengers have come to accept them as the normal course of business in an airport. At most U.S. airports, security operations are located at a central screening point at the central access point to a concourse that serves several

gates. This negates the need for airport authorities to bear the costs of maintaining security personnel at each gate or to station a law enforcement officer at each gate. This simple change of location from the gate to the choke-point before the concourse entrance eventually made the practicality of x-ray machines to search baggage practical. Previously, the cost of an x-ray machine at each gate was a severely costly proposition. x-ray screening only became practical with the improvement of technology and the increase in number of businesses manufacturing them.

Now all sorts of x-ray machines and walk-through or hand-held metal detectors have resulted in a tremendous economy of equipment and personnel (see Figure 7.1). Fewer pieces of equipment and, more importantly, the need to employ fewer people to operate them, has arguably furnished the greatest savings. Cost-related problems resurfaced with the high cost of explosion detection systems and the requirement to screen all checked baggage by the end of 2002. It had become clear that airport baggage areas, not the ticket counters, provide a better venue for the location of the newly mandated explosive detection equipment. This required extensive renovations to some airports. However, placing the explosive detection equipment in the baggage area makes the screening invisible to the passenger and eliminates unnecessary congestion at the check-in and passenger-screening points. This sequence becomes part of the normal process of transferring the baggage from the ticket counter to the airplane.

Improvements made during the initial years of implementation of the rules also greatly increased the distance between the screening checkpoint and the boarding gate. Should an individual attempt to smuggle weapons or explosives, their physical presence is a good distance from the gate. This clearly provides a benefit to security personnel and law enforcement agents, who are afforded the advantage of time and distance. The potential hijacker is deterred from attempting to storm the aircraft directly, and the arrangement gives authorities some precious time and geography to prevent it.

Sometimes the checkpoint screening procedures fail to work. Despite years of perfecting the screening of all passengers, people who are in possession of dangerous contraband are able to slip by undetected. Some of those people sidestepping security are in a hurry, some are evading the security, and some are inspectors testing the procedures. For example, outgoing flights at the Minneapolis/St. Paul Airport in July 2001 were grounded for about an hour while the airport police conducted a search for a man who bypassed a checkpoint after ticketing and before reaching the sterile concourse and gates. The police failed to locate the man and a regular flight schedule was resumed after airlines pressured for the continuation of operations. Had he been a terrorist, a catastrophe could have occurred.

A number of breakdowns to the system contributed to the incident. It was reported that a security officer failed to follow the man who walked past the metal detectors and also failed to

FIGURE 7.1 A female screener checks a traveler with a hand-held metal detector at a security checkpoint. The quality and capabilities of all metal detectors have continued to improve since their incorporation into standard airport security practice. (Source: Transportation Security Administration. www.tsa.gov.)

report it to the airport police to seek assistance for a full 20 minutes. Additionally, the surveillance camera installed at this particular checkpoint, which could have given a pictorial image of the man, did not have any film in it. Even though nothing seems to have come of the incident, the threat could have been consequential (Internet: "Security Breach at Airport," 2001). Problems such as this remain.

The simple movement of passenger and baggage screening to a central point has contributed other advantages, some directly to the airlines. Predeparture screening is accomplished gradually as passengers arrive at the terminal, rather than delayed until the aircraft is prepared to depart. This hugely cuts back on the annoyance factor to passengers. The quantities of passengers and visitors that must be processed each day are spread out. They are permitted to arrive at the airport gauging in advance the time they will need to process security and arrive at the gate. The flow of passengers and accompanying public is markedly quicker, avoiding long lines just at boarding time. Once at the gate, passengers are permitted to board the aircraft directly, giving them a sense of rapidity to the process, whether it is a true perception or not. Processing at the main terminal entrance to the concourse also prevents crowding in the concourses and around gate areas, denying a terrorist or gunman a less prepackaged crowd. This concept is even truer today because only ticketed passengers may enter the sterile concourse.

When the security screening was first initiated, airport managers considered the main disadvantage to this arrangement as being the floor space needed to accommodate the equipment and personnel. However, the other advantages mentioned above soon became self-evident. Thereafter, make-shift screening facilities were turned into permanent, better-arranged security operations. The only unhappy people at the time were vendors and concessionaires who thought that the choke-point screening would somehow adversely affect sales. Their worries proved unfounded, and screening at the entrance to the concourse has become a bedrock element of airport planners. In addition, vendors have flourished on both sides of the screening checkpoints. Airport terminals, on both sides of the security checkpoint, now have everything from restaurants to retail outlets to spas. All of them need to be staffed, and all of them require the delivery of merchandise and supplies, providing an opportunity to smuggle dangerous instruments into the sterile area.

Of continuing concern is the need to keep the concourse sterile. If the airport is not large enough to maintain a 24-hour operation, a thorough search must be made for any weapons or dangerous objects that may have been secretly deposited during closed periods. Security personnel must voraciously search the entire sterile area for any objects that should not be present. A cursory search is unacceptable. All restroom facilities, airport lounges, gate areas, and concessionaire operations need to be checked. This can be tedious work but is an absolute necessity. Vast amounts of money invested in sophisticated screening equipment is useless if a weapon or dangerous device is already in the concourse readily accessible to potential terrorists who have cleared security. Bomb-sniffing dogs are an increasingly useful tool in this capacity (see Figure 7.2). All airport employees should receive some minimal security training no matter how unrelated their job function within the airport complex may appear.

To assist in securing the sterile concourse, consideration must be given to the adequacy of physical barriers at the perimeters. Nonscreened individuals must not have easy access to the concourse. Nor should it be easy to pass dangerous items from someone outside the area to someone inside the area. Except for authorized personnel, access to the concourse must be restricted to passage through the security checkpoint. Additionally, passengers must not be permitted to have access to baggage or anything else that has not been screened. Even if someone clears security but seeks to return to the sterile concourse, they must be screened again, regardless of any protestations from the passenger, vendor, or airline employee.

Also of concern is the sometimes flagrant abuse by airline employees of the door from the field to the jetway. Airline employees believe it a major imposition to use security procedures at these entry points and other access points to the concourse. Any efforts by security personnel to protect

FIGURE 7.2 Law enforcement officers watch as their bomb-detecting dogs sniff baggage and cargo. Dogs are a critical component of any airport security management plan and offer a mobile and reliable means of explosive detection. (Source: Transportation Security Administration. www.tsa.gov).

the aircraft and aircrew from inadvertent incursion by potential hijackers or terrorists are nullified if the attackers can bypass all the screening requirements. If they can gain access at a weak airfield perimeter point and walk into the jetway or other access door with hostile intentions, security has failed. Airline personnel are also notoriously guilty of opening a door to a restricted area and permitting someone else to piggyback, so to speak, onto their entrance credentials.

This brings up another bone of contention with airline employees who believe they should be exempt from screening procedures. Because many believe that they would never engage in nefarious conduct, they also believe that none of their fellow employees would do so either. This is naïve thinking. When airlines weigh the minor inconvenience imposed on the regular screening of employees with the potential for disaster, the inconvenience is rightfully seen as minimal. The corporate culture of airlines needs to reinforce the importance of security at all times. Previously, when Federal Aviation Administration (FAA) personnel observed security violations and attempted to warn airline personnel of the potential fines involved, airline personnel generally remained unmotivated. The current rules mandate that the airlines will receive the fine and not the individual employee. Consequently, because of labor issues or corporate culture or whatever, the present rules have proved ineffective in motivating regular compliance.

STERILE BOARDING AREAS

A second option available to airport planners and security was the sterile boarding area or sterile holding area at the gate. Once passengers completed checking into the flight and were screened, they would be isolated from physical contact with persons outside the area. Constructing these isolated sanctuaries presented challenges. Often the areas were relatively small, and if the waiting period was extended, they became confining and were difficult to make attractive and keep well ventilated. Passengers were not enamored with the arrangements, and the costs could be prohibitive. Admittedly, timing was critical for the advantage of screening passengers arriving at the boarding gate, rather than after an aircraft was available for loading. Regardless, many European and non-Western airports have determined this method of screening suitable for their purposes. Some high-threat airports even have instituted double-screening procedures. The passenger is screened before entering the concourse and again before being permitted into a sterile waiting area. This prohibits passengers from acquiring a weapon or dangerous materials from someone already in the sterile concourse but outside the gate-boarding area.

DEPARTURE-GATE SCREENING

Many security professionals consider departure-gate screening the least desirable of the available alternatives. This option requires personnel to be available for screening at each individual gate, and the operating authority originally had to also provide a law enforcement officer at each gate. Consequently, personnel costs are significantly higher than under the other choices. In addition, passenger screening does not usually begin until the aircraft is actually available for loading. Because of the costs involved and the timing restrictions, this method is only practical for small airports. Making restroom facilities readily available at each gate was also a cost consideration.

This method is enhanced if storage areas can be built to prescreen carry-on baggage. Passengers can then pick up their prescreened carry-on items after they pass through the walk-through weapons detectors. However, women's purses should never be prescreened. The potential for excessive complaints of theft are likely to abound. The same precaution applies to any carry-on baggage that a passenger claims holds valuables. Furthermore, the presence of valuables should never be revealed to other passengers. Due to potential lawsuits and extensive costs, the prescreening method is often found to be impractical. Another drawback is that the protection of time and distance evaporates. Any potential hostile terrorists are already at the gate and very close to the aircraft. "The TSA seldom conducts predeparture gate screening now that most of the commercial airports have integrated screening checkpoints" (http://www.tsa.gov).

Unfortunately, complaints related to missing personal items continue to plague the TSA.

SCREENING CHECKPOINT AUGMENTATION

Since the first prescreening procedures came into effect, many improvements have been made. Not only have technological enhancements to the equipment been accomplished, but also procedural controls have been developed that have improved the process. For example, some screening checkpoints have control booths constructed behind the checkpoints that are raised above the floor for better visibility. The control booth usually has a duplicate set of monitors so that whatever the primary screener is viewing can be double-checked by a supervisor. A two-way communication system provides constant dialogue between the control booth and the screening operation. This second set of eyes increases the effectiveness of the screening.

Many of the control booths also have the capability of videotaping the activities taking place at the checkpoint. At the first sign of trouble, taping can document and protect the professional conduct of the operator. Any accusations by a passenger or visitors of inappropriate conduct on the part of security can be easily disproved. The supervisor in the booth should also have the capability of viewing the screening procedures at other gates and other x-ray machines by use of closed circuit TV (CCTV). Any attempt by someone seeking to distract security at one checkpoint while accomplices rush a second checkpoint can be more easily thwarted. Additionally, because supervisors can view screening at other gates and other x-ray machines, supervisors are better capable of monitoring the effectiveness of their employees while also engaging in security prevention themselves.

The addition of CCTV monitors at checkpoints is another effective enhancement tool. These monitors should televise the view from the cameras monitoring the line rather than the x-ray images. Placing two large-screen color monitors directly adjacent to screening points and allowing passengers in line to view themselves and each other, deters misconduct. As discussed, should a difficult incident occur, the entire activity can be taped for later review or be used in any appropriate criminal or civil prosecution. The monitors also permit law enforcement personnel the ability to assess an ongoing situation prior to entering the scene. Improvements in the quality of the picture have also improved the overall usefulness of this tool. A security professional in a central control booth can literally monitor the entire airport.

Law Enforcement Officers at the Gate

When Part 107.4 (former FAR's which have now been superseded by the TSA regulations) was originally drafted, it required the presence of at least one law enforcement officer at each gate because the screening was taking place at the gate. Specifically, the regulations stated that a law enforcement officer must be present:

> "…at the point, and prior to and throughout, the final passenger screening process prior to boarding, for each flight conducted by a certificate holder… continuously until all doors on the aircraft being boarded are closed and the aircraft has taxied away from the boarding area; and in the event that the aircraft returns to the boarding area before take-off."

On 1 April 1981, the FARs were amended as Sec 107.15 to state:

Each airport operator shall provide law enforcement officers in the numbers and in a manner adequate to support

1. Its security program
2. Each passenger screening system required by Part 108 or Sec 129.25 of this chapter.

49 CFR Chapter XII Part 1544.217 now requires each airport operator to arrange for law enforcement personnel meeting the qualifications and standards specified in Section 1544.21 and provide its employees current information regarding procedures for obtaining law enforcement assistance at that airport.

The first Rule FAR 107.4 was originally interpreted to require a law enforcement officer's presence during the entire process of prescreening. The responsibility for overseeing the presence of the law enforcement officer rested with the airport operator. The carriers would often suspend screening of passengers until an officer was on the scene even though nothing in the regulation prevented the airline from continuing the processing of passengers. Problems arose when a passenger could not be cleared for unaccountable metal on their person. Airlines did not want nonsecurity-trained personnel to conduct a pat down search of passengers. The only alternative was to deny the passenger access to the aircraft. This did not endear the airline to the paying passenger.

Another area of conflict revolved around who was responsible for the added costs of such a law enforcement presence. The debate is still ongoing especially with law enforcement officers now assuming some of the duties temporarily conducted by the National Guard to give the appearance of beefed up security. Previously, some small communities even attempted to present the airlines with a bill. Today, they can apply to the federal government for reimbursement. Everyone was in favor of a safer airport environment, but no one wanted to bear the burden of the additional costs. Compromises had to be made and eventually the Airport Operators Council International (AOIC) contributed to ironing much of these issues out. One of the successes of the later Air Carrier Standard Security Program (ACSSP) covered the negotiations regarding legitimate expenses attributable to the airlines and subsequent assessments as to the need for implementation of new concepts with corresponding new costs. The debate still rages.

Eventually, it became obvious that the presence of law enforcement officers at each gate was not only not cost effective, but did not contribute to better security. After a trial and error period, it was soon discovered that the armed officer could even prove to be a liability being stationed so close to the actual aircraft. Two incidents proved the point. A law enforcement officer assigned to the Baltimore Airport on 22 February 1974 was positioned at a gate-screening point for Delta Flight 523. Samuel Joseph Byck was armed and approached the gate. He drew his weapon and without any warning shot the police officer and entered the cockpit whereupon he shot and killed the copilot and wounded the pilot in command. After announcing his plan to fly the aircraft into the White House, he was eventually shot but succeeded in committing suicide while still on the aircraft. The law

enforcement presence at the gate failed to stop the attacker and after the death and incapacitation of the officer, gave the attacker free and quick access to the aircraft.

Another example of the wisdom of not having an officer at the gate took place in Nebraska a few years later. In October of 1977, a lone gunman casually approached the law enforcement officer at the gate of a Frontier Airlines flight. He removed a shotgun from his carry-on luggage and rapidly disarmed the police officer. After boarding the flight he ultimately shot himself. The incident contributed to the discussion regarding the proper placement of officers within the airport complex. It was finally determined that the millions of dollars being spent to station these officers could be better spent elsewhere.

Flexible Law Enforcement Response Program

The solution was named after the post-Vietnam military concept of flexible response as opposed to conventional response. Under this system, an officer was not required to be at the screening checkpoint at all. Officers were tasked with having to be able to arrive at the checkpoint within a given response time. The airlines were thereby somewhat assured that an officer would arrive, and the police were relieved of the burden of stationing an officer at each gate. In a realistic move, the FAA was not requiring a "guaranteed" response time. The police needed some flexibility in case of multiple requests for assistance and other emergency situations. This greatly reduced the number of officers that communities had to assign to an airport. At Washington's Reagan Airport, authorities initiated the first flexible response program ironically on 11 September 1981, and the number of law enforcement officers was immediately reduced from 51 to 17. The exact response times for each airport were part of the ACSSP and are still not available to the public for obvious reasons.

Catering to the all-important public perception, the program was originally named the Strengthened Screening Point Security Program (SSPS). Few airlines or security professionals wanted to send the signal to the traveling public that it was based primarily on cost reductions. In reality, it was cost effective, but that was only the positive by-product of a legitimate security need to give the police the advantage of time and distance to the gate.*

Airport Categories

Category X – Any number of passengers. The designation is based on the need for special attention due to the perceived threat.
Category I – More than 2 million travelers
Category II – 500,000 to 2 million travelers
Category III – Less than 500,000
Category IV – Any number
Category V – No screening (Note there are no longer any Category V airports.)

The Flexible Response Program also created the position of a Checkpoint Security Supervisor (CSS) who is now referred to as the TSA checkpoint supervisor. This individual was to take over many of the functions of the law enforcement officers previously stationed at each gate. The individual was to receive special training and was to have a more extensive security background than the average contract security officer. At a minimum they were to have at least three years of prior law enforcement or private security experience. It is important to note that while it was the responsibility

* *Note*: The categories of airports are generally broken down based on the number of passengers that transit the airport annually.

of the airport to provide the law enforcement officer, it was the airline carrier's duty to hire and train this "screener in charge." Many former checkpoint supervisors employed by contractors like Argenbright and Globe Aviation hired or promoted employees with little or no law enforcement background. The CSS, or the new equivalent substitute to the position, should use the acronym VETO, for the following:

1. Verify the credentials of any law enforcement officers who claim the need to board an aircraft with a weapon.
2. Evaluate the need to assemble law enforcement officers or station management if required.
3. Conduct timely patdowns and searches as required.
4. Organize responses to false statements by passengers, faulty communications equipment, and general supervisory duties.

Similarly, the 49 CFR Chapter XII, Section 1544.215 requires a designated Aircraft Operator Security Coordinator (AOSC). The AOSC must be designated in the airport security program. The individual appointed AOSC, or an alternate, must be available 24 hours a day and is supposed to serve as the airport's primary contact for security-related activities and communications with the TSA. This position was eventually done away with in light of the new Security Manager Program.

PUBLIC AND PRIVATE SECURITY INTERFACE

The general purpose of any private security is to protect assets and people. Airport security personnel are present to create nonthreatening environments in which passengers, accompanying family and friends, employees, and airline personnel are able to conduct their business in a nonthreatening environment. All security people that work within the airport environment should be able to recognize the differences between the private "policing" function and that of the public police. In the airport those differences are becoming more blurred, making it difficult to distinguish between those boundaries that have traditionally defined the roles of the public sector versus airport security personnel. The same overlapping parameters relate to individual versus institutional responsibilities. The most important difference relies on the fact the police can use force whereas private security, whether contract or federal, possesses power that really relies mostly on persuasion.

Security personnel usually wear some distinctive clothing so they can be easily identified even from a distance. They are distinctly different from police uniforms. However, a police officer is generally armed, in uniform, and wears an insignia of his or her profession. All are easily recognizable, but their responsibilities and authority are quite different. Various situations compel the expertise of both, and both need to be appreciated for the value they bring to the overall security picture.

Airport security and local law enforcement must work in conjunction with each other in an assortment of situations. Most notable are situations when an individual threatens or attempts to board an aircraft with a dangerous weapon. The Federal Aviation Act, implemented again by Section 1540.111, makes it illegal to attempt to board an aircraft while having a concealed weapon on or about one's person or a deadly or dangerous weapon in any carry-on baggage. The regulations require that passengers discovered to be carrying an undeclared weapon must be referred to a police officer. However, before that officer is ever summoned to the scene, an airport security officer makes independent decisions every day about what exactly constitutes a dangerous weapon.

Almost anything can be used as a weapon. Swiss Army knives, knitting needles, and scissors are all dangerous in the wrong hands. The original emergency order requiring 100 percent screening of all passengers and carry-on luggage provided in part, "The certificate holder shall not permit any passenger to board its aircraft unless the carry-on baggage items are inspected to detect weapons, explosives, or other dangerous objects." What the term "dangerous weapon" encompasses is open to much dispute. Generally, the term should encompass any device or object that if its possession alone supports a reasonable presumption that it could be used as a weapon.

Each decision is a matter of judgment, especially because most airlines previously provided first-class passengers with a metal knife during meals. An incident in December 1996 proves the point. A 32-year old Algerian with an expired visa boarded a DC-10 from Detroit to Frankfurt, Germany, and about four hours from arrival attacked a flight attendant by choking her and screaming "to Africa." The stewardess escaped, and the passenger attacked a female passenger yelling "whore" repeatedly. He had concealed his dinner knife in a blanket and was extremely intoxicated after consuming another passenger's bottle of duty free liquor. Military police on board subdued the subject who grappled with them for several hours after getting restraints on him. The meal service had to be canceled in the back of the aircraft due to the passengers' excrement, which contaminated the aft food service area. Several crew members sustained minor injuries, and some military police uniforms were ruined. The subject became extremely violent, appeared insane and out of control during the entire incident. He was apparently trying to hijack the aircraft, but was too intoxicated to consummate the act of taking the hostage and getting control of the flight. On arrival in Frankfurt, the captain was denied the courtesy of discussing the matter with the police, and the subject was released without prosecution by the German authorities after about three hours (Internet: http://www.alpa.org/internet/tm/ tm061198.htm. 22 April 01, pg. 2). Even though current policy requires "plastic knives" in all passenger cabins, all the passenger needs to do is grab a wine bottle, break it, and use it as a weapon.

In 1986, FAR 107.21 was amended to substitute the words "deadly or dangerous weapon" for the word "firearm." The previous regulation had stated, "No person may have a firearm, an explosive, or an incendiary device on or about the individual's person or accessible property when presenting himself or herself for screening or when entering or in a sterile area." The broadened definition permits security officials to make a determination as to what could be considered dangerous on board an aircraft. They can evaluate the article itself and the demeanor of the individual possessing it. The regulation was amended to state that no person may have explosive, incendiary, or a *deadly or dangerous* weapon on or about the individual's person or accessible property. As stated, what exactly constitutes a dangerous weapon was often difficult to surmise. However, horror stories abound of taking nail clippers from airline pilots and knitting needles from grandmothers. Section 1540.11 now simply provides "…an individual may not have a weapon, explosive, or incendiary on or about the individual's person or accessible property.[*] Difficulty in determining who exactly is a police officer persists.

According to Harbor Police Dispatch records, approximately 6687 armed peace officers entered the passenger boarding areas of San Diego Lindbergh Field in 2001. Their purpose was assumed official. Before entering the passenger areas, armed officers are required to present their documents and departmental identification to the airline and later to security. However, prior to 11 September, using false identification, FAA officials succeeded in breaching security around the nation on repeated occasions. Security had received no special training in the recognition of valid credentials. Department ID cards often vary in style and appearance, and improvements in technology make

[*] *Note*: The provisions of this section with respect to firearms do not apply to the following: (1) Law enforcement personnel required to carry a firearm or other weapons while in the performance of law enforcement duties at the airport; (2) an individual authorized to carry a weapon in accordance with 1544.219, 1544.231, 1544.223 or 1544.211; (3) an individual authorized to carry a weapon in a sterile area under a security program.

the duplication of documents much easier than before. This issue has been addressed when devising training materials for new screeners.

CRIMINAL CASE LAW EXAMPLES

U.S. v. James Edward Ware, U. S. District Court, Western District of Oklahoma, August 1970

This early case discusses whether the weapon in question was deadly or dangerous. The case ultimately determined that an unloaded .25 caliber automatic pistol in a passenger's pocket did constitute a dangerous weapon under 49 USC Section 1472 (1). Once again the court confirmed that the primary purpose of this section is to prevent the hijacking of commercial aircraft, and it has been demonstrated many times that an aircraft can be hijacked with an unloaded gun.

The court held that the unloaded gun in question was indeed dangerous and prohibited by statute. The case set the stage for countless cases involving such "dangerous weapons" as toy guns, knitting needles, and large scissors. Generally, a dangerous weapon definition should include any firearm, whether loaded or unloaded, or any device designed as a weapon capable of producing death or great bodily harm. Additional thought should be given to adding language pertaining to combustible material or flammable liquid and any other device or instrumentality that, in the manner it is used or intended to be used, is calculated or likely to produce death or bodily harm.

U.S. v. Feldman, U.S. District Court, Eastern District of New York, 1 May 1969

This case deals with the constitutionality of a law that imposed only a civil penalty as opposed to a criminal penalty for falsely reporting a bomb at an air navigation facility. The court held that the statute was constitutional under the commerce clause of the U.S. Constitution. The government argued that the elimination of all false bomb reports at airports was crucial to the safety of all air navigation. The legislative history of the law specifically cited its purpose is to eliminate the disruption of interstate commerce arising from the conduct of pranksters and jokesters.

The defendant moved to dismiss the complaint for failure to state a cause of action, and the government sought summary judgment. The defense considered this section to be unconstitutionally vague. The defendant was charged under 18 USCA Section 35 (a). The purpose of the new law, HR 6848, was to reduce the existing penalty against pranksters who falsely report the presence of bombs and the like aboard aircraft and who have no real evil intent or malice in mind. However, the court supported the contention that such comments, no matter how innocuous, must be prohibited. Their holding in the case concluded that 18 USC Section 35 (a) is clearly constitutional, and the court order denied the defendant's motion for summary judgment.

U.S. v. Benrus Eugene Brown, United States District Court, Western District of Texas, October 1969

In this unusual case, the court tackled the concept of what actually constitutes a dangerous weapon and the threshold of what constitutes an attempt to board an aircraft with a dangerous weapon. Generally, the court held that an unlawful attempt to board an aircraft while carrying a concealed weapon was made when the air passenger surrendered his ticket at the customer service agent's desk and entered the departure lounge for the flight covered by the ticket. The court also determined that statements elicited from the passenger by the arresting airport security guard were inadmissible as evidence. However, the portions of the ticket held by the passenger and the customer service representative, as well as the weapon removed from the person of the passenger were admissible.

The defendant pled not guilty to knowingly, willfully, and unlawfully attempting to board an aircraft being operated by an air carrier involved in air transportation at the San Antonio International Airport, while having on or about his person a concealed, deadly, and dangerous weapon, to wit a .22 caliber weapon. The defendant was charged under Title 49 USC Sec 1472. The court determined there were three main issues at trial:

1. Did the acts of the defendant constitute an attempt to board an aircraft?
2. Were statements made by the defendant at the time of his arrest admissible in view of the fact that he was not given any warnings under the rule in *Miranda versus Arizona*?
3. Was the evidence, which was seized illegally, obtained from him as the result of an unlawful search and seizure?

There is no question that the guard fully intended to take him into custody to determine the presence of a gun. The defendant was under arrest when the security guard began to question him in the departure lounge and that arrest was lawful. When a person is lawfully arrested, the officer has the right, without a search warrant, to make a contemporaneous search of the person of the accused for the fruits of or the instrumentalities used to commit the crime. Consequently, the gun and the ticket components were admissible at trial (*Agnello versus United States*, 269 U.S. 20, [1925]). The court also reasoned that he had in fact attempted to board the aircraft.

Lawrence Havelock v. the U.S. Court of Appeals, Tenth Circuit June 1970

This particular case provides a case study on circumstantial evidence as well as illustrating an arson attempt on board an aircraft. The circumstances supported a passenger's conviction for willfully setting fire to an aircraft while in flight. The circumstantial evidence consisted of a variety of nondirect evidence. The prosecution introduced documentation concerning his demeanor during the entire flight and particularly prior to and subsequent to a fire in the restroom. They also offered his statements to other passengers, his bizarre behavior in wearing yellow gloves, and the attempt to secret them, and the fact that he was the last visitor to the restroom prior to the ignition of the incendiary fire. The court also saw fit to permit the admission into evidence of similar acts, which evidenced intent or scheme, while they determined that these statements were not unnecessarily prejudicial. Mr. Havelock was convicted of setting fire to an aircraft in flight while the aircraft was being operated in interstate commerce.

Even evidence that is slightly prejudicial does not necessarily require a reversal. Courts have repeatedly held that not every error occurring during a trial requires reversal, only errors that affect substantial rights are prejudicial and worthy of reversal. To prove the defendant willfully set fire to the aircraft, the definition is well settled. Willful conduct consists of acts that are intentional and accomplished with an awareness of what one is doing. The prior acts must be similar in results, and there must be such a concurrence of common features that the various acts are naturally to be explained as caused by a general plan of which they are the individual manifestations. The sum of the hotel evidence illustrates sufficient fundamental features of a scheme, which culminated in the fire aboard the aircraft, to be admissible at the trial. Consequently, the conviction was affirmed on appeal.

U.S. v. Reid 2003 (Shoe Bomber)

Richard Reid, or Abdul Raheem, was convicted on charges of terrorism and is currently serving a life sentence in a maximum security prison in Colorado. Reid had pled guilty to all eight counts against him, including attempted use of a weapon of mass destruction, attempted homicide, and placing an explosive device on an aircraft. More specifically, in January 2003 he was sentenced on each of the three charges, 20 years imprisonment on four other charges, and 30 years on four other counts, to be served consecutively, followed by five years of supervised release. Reid tried to blow

up American Airlines Flight 63 from Paris to Miami in 2001 with explosives in his shoes. The attempt was foiled when flight attendants tackled the avowed al'Qaeda operative before he could light the fuse. Even though it was originally thought that he acted alone, it appears he had the support of an Islamist terror network in Paris. Reid, 28, who trained in al'Qaeda camps, repeatedly contacted fellow extremists while in Paris in the weeks before his planned attack. Reid told authorities he bought the explosives in the Netherlands and hid them in his shoes himself, but one French official says he is virtually certain Reid obtained his explosives while in Paris. Authorities have also found Reid's e-mails, including one from Pakistan urging Reid to try again after a failed attempt to board the same flight one day earlier.

U.S. v. John Walker Lindh

John Walker Lindh, aka Suleiman Ferris, aka Abdul Hamid, aka The American Taliban, was captured by U.S. forces in Afghanistan with a group of Taliban and al'Qaeda fighters who survived the bloody Mazar-e-Sharif revolt. He was charged with conspiring to kill U.S. nationals and aiding Usama bin Laden's al'Qaeda network. Initially facing 11 criminal counts, the only charge that John Lindh was found guilty of was violating economic sanctions by supporting the Taliban government, for which the 20-year-old was sentenced to 20 years in prison. He was sentenced in September 2002.

In 1998, while his parents were divorcing, John Walker asked them to finance a trip to Yemen to learn Arabic. He came back to the United States for a short while, but later returned to Yemen. The next time his parents saw him he was on the news as the American Taliban. In an affidavit by a federal agent the following information was disclosed:

> From my review of reports and other statements prepared by law enforcement officers, U.S. military personnel, and other government officials, I have learned that on or about November 25, 2001, Johnny Michael Spann who was, at the time an employee of the Central Intelligence Agency, and an individual identified herein as "confidential source 1" ("CS-1"), an employee of the United States Government, were conducting interviews at the Qala-i Janghi ("QIJ") compound near Mazar-e Sharif, Afghanistan, of al'Qaeda, and Taliban forces who had been captured by, or who had surrendered to, Northern Alliance forces in the course of the ongoing conflict in Afghanistan. Among those interviewees was an individual later identified as the defendant, Walker. Shortly after Walker's interview, prisoners —- who numbered several hundred — staged an uprising that took several days to suppress and which resulted in Spann's violent death. During the course of the uprising, Walker retreated with other detainees to a basement area of the QIJ compound, where he remained for several days before being identified by military and medical personnel as a United States citizen. Walker has remained in the custody of U.S. military forces since that time (Affidavit in Support of a Criminal Complaint and an Arrest Warrant, Anne E. Asbury, Special Agent with the Federal Bureau of Investigation [FBI], United States Department of Justice, assigned to the Washington Field Office).

Defense attorneys had filed documents alleging their client was tortured while the FBI coerced statements from him in violation of his Fifth Amendment rights. The pleadings were filed for a hearing held on 15 July 2002 to determine whether statements made by Lindh after his capture with an Afghan Army unit would be suppressed or allowed into evidence at trial (Internet: http://www.lindhdefense. info/ 20020613FactsSuppSuppress.pdf). Prosecutors acknowledged early on that they had little evidence outside of Lindh's own statements to support their charges that he conspired to murder U.S. citizens and illegally supported terrorist organizations. A plea bargain was eventually struck, and no decision was made by the court on the admissibility of Lindh's original confession in Afghanistan.

Case Law Summary

All these cases illustrate some aspect of criminal misconduct within the airline industry or in Lindh's case violating sanctions against a hostile nation. It should be noted that any crime that can be committed on the ground can be committed in an airport or on an aircraft. The law literally is exactly the same. The same constitutional protections apply, and the same evidentiary issues come into play. The same safeguards imposed on police officers and private security guards are also applicable.

However, legislators have passed additional laws making it a crime to intervene with the air crew, board an aircraft with a weapon or dangerous instrumentality, board an aircraft intoxicated, and, of course, it is a crime to hijack the aircraft. Screening of people and baggage is the only way to determine whether individuals are attempting to commit some of these prohibited acts or possess the means to do so. Much litigation has been generated regarding what is a "dangerous weapon," what constitutes an "attempt to board an aircraft," even what can constitute a criminal act versus a civil tort, and what specific evidence can be used to convict someone of a crime. Even though it is not possible or desirable to turn security professionals into mini-constitutional or criminal lawyers, it is important that they possess a basic understanding of the rules so that they can appropriately apply them.

INITIAL SCREENING

Everyone who has ever flown is familiar with the first safety question asked the traveler by the airlines for security reasons. Did you pack your bag yourself? Many security directors questioned the utility of the practice, and most travelers do not take it seriously anymore. Homer Boynton, the former director of security of American Airlines, claims the question had become perfunctory and was no longer worthwhile (Tierney, 2001). Admittedly, most travelers have learned to casually lie and basically ignore the question. When John Tierney, a reporter for the New York Times, tested the question, his bags were subjected to increased security. The official position of the TSA was better safe than sorry.

Unfortunately, there is some credibility to the concept that the question serves no real security purpose. The TSA continued to justify the policy for awhile because bombs are still discovered in baggage. However, the only domestic incident occurred in 1955 when a son packed his mother's bag, including a highly lethal incendiary device, to murder her and collect some insurance money. Consequently, the regulation has survived for all these years long after the original justification has faded. The TSA finally removed the requirement in August 2002.

SCREENING PROCEDURES

Screening procedures, at the entrance to the sterile concourse have repeatedly come under close scrutiny. The FAA, and its parent agency, the Department of Transportation, had been internally reviewed by the Inspector General's (IG) on the status of airport security numerous times. The results had not always been very favorable regarding the conduct of contract security personnel at airport concourse checkpoints. The IG conducted a survey in 1993 in which it discovered numerous security flaws at several U.S. airports, especially at four major airports. According to one report, "…in the 1993 investigation, agents were able to pass the screening points at all four airports, and in 75 percent of the attempts, were able to actually board planes with the 'bombs' in their carry-on luggage, as well as accessing ramp-side areas, where the planes parked" (Fay, 2001). A follow-up survey three years later indicated that FAA agents still had access to sterile areas 40 percent of the time. Consequently, four of every ten passengers could be carrying some sort of contraband. Security procedures are very good at intercepting most contraband; however, 100 percent complete and totally accurate security has yet to be obtained and likely never will. Currently, security is better than previously, but far from without flaws. There remains room for improvement despite recent changes.

Of course, there is no good substitute for simple good judgment. No matter how many times employees are taught proper procedures, what appears to be an exception to every rule is frequently going to happen. Unfortunately, common sense is difficult, if not impossible to teach. Therefore, extensive, continuous, and repetitive training is an absolute necessity. Effective November 2001, all airport screeners were supposed to be required to minimally have a high school diploma and undergo government-approved training under a new federal aviation administration. The rule has proved more difficult to totally implement than originally hoped.

Generally, the airport security officer will handle thousands of routine situations on a daily basis. Consequently, certain scenarios will repeat themselves, and all security personnel should be thoroughly trained on exactly how to handle them. When questions do arise, a supervisor should be called and consulted. Everyone should be encouraged to exercise caution and to think through each situation and not to simply react to it. Under no circumstances should a passenger be allowed beyond the screening point unless screening personnel are assured that the passenger is not carrying any dangerous objects. Such negligence can have serious consequences.

On July 2000, an x-ray screener at the San Francisco International Airport actually spotted a handgun, yet still allowed the passenger to proceed. He later notified the police and the several gate areas had to be literally shut down while 800 people and their baggage were searched. Both a Delta and a Northwest flight were delayed for quite a long period of time (ASI, 2001). In the alternative, random selection of individuals is giving the appearance that security is blatantly ineffective. For example, Al Gore, former Vice President, in June 2002 was randomly selected for screening while other maybe more likely individuals were not. Such high-profile "apparently unnecessary" screening only deters from the real job at hand and sends the wrong signal to the public and the terrorists.

Of course, arrest situations based on probable cause should be left to the appropriate law enforcement personnel. It is neither desirable nor effective to have security personnel attempt to engage in law enforcement duties, especially when life-threatening conduct is involved. Police officers are part of a governmental enterprise better equipped to combat crime and enforce laws as well as apprehend offenders. Most importantly, they possess the statutory authority to do so. Ultimately, however, it is always wise to remember that, assuming the passenger poses no threat to the aircraft or other passengers; the final decision for boarding an aircraft still rests with the airline, not the security officer or law enforcement official. Unless, as mentioned, a dangerous situation exists where the individual involved is being arrested, all authority must indeed shift to law enforcement.*

In the past there were rare situations in which local law enforcement had cleared a passenger for boarding, but the airline still did not want to board them. For example, situations arose when a passenger may have had too much to drink or even just smelled offensive. They may not have broken any laws, and yet the airline may not consider them appropriate passengers. The government may fine the airline for boarding an intoxicated passenger even though not all intoxicated passengers are hostile or noisy and consequently obvious to identify. Therefore, airlines have different procedures in dealing with the intoxicated, offensive passenger or pregnant passengers near full term. The final decision actually rests with the pilot. Federal Aviation Regulation 91.3a states that "…the pilot in command of an aircraft is directly responsible for and is the final authority as to the operation of the aircraft." The pilot can refuse to board anyone considered detrimental to flight.

As mentioned, the actual policies regarding specific types of passengers will vary from airline to airline. One rule was put to the test when an American Airlines pilot refused to board an armed "Arab-American" secret service agent on 25 December 2001. The pilot felt that the agent did not have the proper credentials in his possession, and, even though it was the second time the agent had been boarded, in accordance with airline policy they refused to board him. The pilot's decision was later upheld as proper.

---

* *Note:* Private security officers really have no more powers than private citizens. As citizens they certainly have the power to arrest, to investigate, and to defend themselves and to defend their own property and any property entrusted to their care. However, they have no police authority.

It has long been the practice of the FAA and the TSA to screen. Specifically, the FAA required in FAR Section 315 (a) that "all passengers and all property intended to be carried in the aircraft cabin in air transportation must be screened by weapon-detecting procedures or facilities employed or operated by employees or agents of the air carrier." TSA regulation Part 1544.201 (b) and (e) now provide that:

(b) Screening of individuals and accessible property. Except as provided in its security program, each aircraft operator must ensure that each individual entering a sterile area at each pre-board screening checkpoint for which it is responsible, and all accessible property under that individual's control, are inspected for weapons, explosives and incendiaries as provided in Sec 1544.207.

(e) Staffing. Each aircraft operator must staff its security screening checkpoints with supervisory and non-supervisory personnel in accordance with the standards specified in its security program.

Today, the screening is accomplished through the use of metal detectors, x-ray machines, explosive detection equipment, and residue-detection equipment; all calling for properly trained personnel as operators. Security personnel must remain proficient in screening all sorts of people and objects, constantly adapting to new technology as well. Screening both passengers and baggage has now become commonplace in airports all over the world, but training on Explosive Detection Equipment and Trace Detection Equipment require sophisticated and specialized protocols. Clearly, the system is not foolproof. For example, in May 2002, the FBI labeled the fact that a man clearing security in New Orleans Louis Armstrong Airport with two loaded handguns as a "massive failure." Regardless, in efforts to remove some of the "hassles" related to airport screening, the TSA announced in August 2005 a move to update and streamline the procedures. The TSA instituted major changes in how it screens airline passengers, including proposals to lift the ban on carrying razor blades and small knives as well as limiting patdown searches.

SCREENING BAGGAGE

The rules pertaining to the screening of carry-on baggage are clear. The original legislation in the Federal Aviation Act of 1958, Section 3 as amended, provided that to the maximum extent possible, the FAA administrator was mandated to require uniform procedures for the inspection, detention, and search of persons and property in air transportation and intrastate air transportation. The current rules are meant to prevent or deter the carriage aboard airplanes of any explosive, incendiary, or a deadly or dangerous weapon on or about an individual's person or accessible property. The TSA defines carry-on luggage as all accessible property under that individual's control. Any articles on the person of the passenger will be subject to search by means of a walk-through or hand-held metal detector. Despite the extensive public awareness of security screening at airports, it is surprising the number of people who either purposely or inadvertently break the law. Baggage can be screened physically, by use of x-ray equipment or newer explosive detection equipment or trace detection systems.

It must be remembered that law enforcement officers or hunters going on vacation who had not cleared their weapon with the airlines in advance carried some of the discovered firearms. Additionally, some were in the possession of citizens who were violating the law, but had no real intention of hijacking an aircraft or assaulting passengers as part of a political movement. Some even claimed to be bodyguards of celebrities or individuals maintaining they needed to protect themselves. Similar to the argument relating to the exclusionary rule and the Fourth Amendment, it is hard to statistically analyze how many terrorists choose not to attack an airport or hijack an aircraft because of the procedures in place.

The proper procedure, if a weapon is detected, is to stop the x-ray machine to keep the baggage away from the passenger. It makes no sense to return the baggage to the passenger so that the weapon could be accessible to them. If discovered by a metal detector, the passenger should be

asked to permit the security official, or a law enforcement officer, to confiscate the weapon. Under no circumstances should security personnel attempt to forcibly take the weapon. Nor should the passenger be allowed to retrieve the weapon and possibly take that opportunity to use it against security personnel or other passengers. Airport security personnel should cooperate fully with anyone brandishing a weapon. Subduing such an individual needs to be accomplished by a trained law enforcement officer.

An even more frequent scenario for screening personnel involves the potential discovery of large sums of currency or illegal drugs. The airlines do not wish to be placed in a position of law enforcement, and these situations are handled in a number of ways depending on the circumstances. It is an interesting piece of trivia that one million dollars can fit into a suitcase weighing no more than 35 pounds. However, at a minimum, the security officer should either alert a U.S. Customs official or law enforcement officer immediately. The security officer should also take particular note of the characteristics of the baggage owner and the luggage itself for later identification. Airport security personnel should also be cognizant of the direction the passenger takes when entering the sterile concourse. In all cases, the procedures developed by the airline should be followed.

Of even more danger to the traveling public is the fact that operators of x-ray scanners can become bored and distracted, thereby missing a truly dangerous set of circumstances. It is difficult to keep focused for long periods of time, especially when the work is tedious and repetitive. Therefore the operator needs to be relieved on a regular basis. It is best to maintain a 15- to 30-minute rotation schedule if possible. In addition, bonus rewards have proven effective in keeping personnel more aware and on the constant lookout for certain objects. Software to project false images to scanners is now available and in use in many airports. Suffice it to say, no x-ray machine can stop a terrorist with a weapon; the operator must see the threat and respond to it accordingly. Their extra efforts may not only stop a terrorist plot, but could provide the scanner with some extra income. Last, alert screeners are able to avoid instances in the improbable situation where babies or animals in carriers might be inadvertently screened.

Besides fatigue, the screener may be hindered by the fact that a discrepancy exists between the width of the conveyer belt of the x-ray machine and the width of the unit's field of vision. In other words, some parts of luggage may not be fully exposed to the operator. Problems also potentially arise when luggage is folded over itself and larger objects obstruct the view to objects beneath them. Newer equipment has improved the screener's field of view as well as the clarity of the picture. However, not all airports are equipped with state-of-the-art machines that are available.

THREAT ASSESSMENT

Every screener is only as effective as his or her skill in recognizing dangerous objects during the few seconds he or she has to observe each piece of luggage. A hair dryer might look like a gun, or the inside of a radio may just look like transmitters. Scanners must constantly be trained and retrained until they are proficient in distinguishing anything potentially dangerous from nonthreatening objects. Therefore, any doubt by the screener about the actual dangerousness of an object needs to be resolved with a physical hands-on search. Screeners must make quick assessments. A handy acronym is NOPE:

1. No threat exists; let the carry-on baggage pass.
2. Obvious threat exists; seek law enforcement assistance; stop machine, alert supervisor.
3. Possible threat exists; initiate physical search.
4. Emergency; alert supervisor, law enforcement, explosive ordinance disposal (EOD) personnel.

Under certain circumstances, physical inspections are preferable to x-ray screening. For example, plastic explosives can be rolled flat and sewn between the linings of luggage. Some articles

FIGURE 7.3 Air travelers may carry liquids, gels and aerosols in their carry-on bag when going through security checkpoints. (Source: Transportation Security Administration. www.tsa.gov).

also lend themselves to deception. Books can be hollowed out, and walking canes or umbrellas can be dismantled to discover a hidden sharp object. Alert security personnel have even dismantled a tube of lipstick to uncover a small, but lethal weapon. Airport security must also recognize it is not only poor security, but also bad public relations to physically inspect the contents of someone's luggage by emptying it out onto a table. No one appreciates the public viewing a change of underwear or other personal belongings. It is also particularly unwise to expose valuable jewelry or large sums of cash to the wandering and often opportunistic eyes of potential thieves. This bag dumping procedure is not sanctioned by the TSA, but does still occur at some airports. Carry-on bags are subject to inspection once they are placed on the x-ray machine's conveyor belt and electronically screened (e-screened) and inspected in accordance with TSA's Standard Operating Procedures. It is still important to remember that security has little defense against allegations that cash or valuables were stolen while the passenger's carry-on baggage was out of plain view. Physical searches should be accomplished with a witness nearby. The issue of the security screening officers themselves as being the thieves presents yet another problem and will be discussed in a later chapter.*

3-1-1 RULE

As a result of the recognition of a possible threat from the possible combination of liquid or gel ingredients on board aircraft and extensive explosive testing, all liquids were temporarily banned from aircraft. Now, liquids, gels and aerosols are once again allowed in carry-on baggage, but in limited quantities and with some very specific packing requirements by the TSA. All liquids, gels, and aerosols must be in three-ounce or smaller containers. Larger containers that are partially full and rolled up toothpaste tubes are not allowed. This security regimen applies to all domestic and international flights departing U.S. airports (see Figure 7.3).

Passengers must be aware of the fact that the rule is not just about shampoo and toothpaste. Food items such as jams, salsas, sauces, syrups, dips, and wine will not be allowed through the checkpoint unless they are in containers three ounces or less and in the passengers one-quart zip-top bag. This applies to gift items including lotions, creams, scented oil, liquid soaps, perfumes,

* *Note*: More than a year after pleading guilty to federal fraud charges and being put on three years' probation, Atlanta based Argenbright Security, Inc. was accused on 11 October 2001 by the Department of Justice (DOJ) of failing to complete background checks on workers. This indictment came on the heels of at least seven employees being suspended following a security breach at Chicago's O'Hare Airport approximately a month after 11 September.

and even snow globes that are in excess of three ounces even if they are in sealed gift packs. The TSA suggests that travelers ship these items prior to your trip or put them in your checked baggage. Any of these items will be allowed on the plane if you purchase them after the security checkpoint. TSA allows liquid items purchased after the checkpoint onto planes because these items have been previously screened.

All liquids, gels and aerosols must be packed in a single, one-quart, zip-top, clear plastic bag. Larger bags or bags that are not zip-top, such as fold-over sandwich bags, are not allowed. Each traveler may carry on only one plastic bag of liquids and gels, and it must be inspected separately. Travelers should remove their quart-sized plastic bag from their carry-on luggage and place it on the conveyer belt for screening.

Larger amounts of liquids can be carried in checked luggage.

Travelers may continue to bring the following items through security and on flights (www.tsa.gov/311.):

- Baby food and formula if an infant or toddler is traveling.
- Breast milk in quantities greater than three ounces as long as it is declared for inspection at the security checkpoint.
- Prescription medicine (prescription label must match the passenger's name). There is no quantity limit.
- Essential nonprescription medicines up to four ounces per container.
- Solid cosmetics and toiletries, including lipstick and solid deodorants.

SCREENING COMPUTERS AND LAPTOPS

Mention needs to be made as well on the ever-increasing numbers of computers and laptops now carried by passengers. Laptop computers have become commonplace, and passengers insist on using them while waiting for flights and during flight. Before gaining entrance to the sterile concourse, these devices must be inspected. They need to be turned on and booted up to be absolutely sure they are truly a laptop computer, but it is generally safe to just screen them. It should be noted that the x-ray machines on the market today have been extensively tested. They will not damage memory, destroy hard drives, or damage the computer in any way. On the other hand, a device that has been stripped of its computer components and refabricated as an explosive device poses a distinct threat that cannot be ignored. Consequently, all computers must be checked to make sure they are really computers. If necessary, checkpoint areas should be equipped with an outlet to boot up the computer, if the laptop is not equipped with a battery. Otherwise, computers can safely be scanned by x-ray equipment; however, it is good practice to remove them from carrying cases for clearer imaging.

Security personnel need not be trained to be computer experts; however they do need to be able to recognize when the internal workings of a laptop are really a computer and not a cleverly assembled bomb or the potential pieces of one. They should also be able to make simple distinctions between when a power source that might be more than is indicated for a laptop and consequently may pose a threat. Terrorists are very adept at smuggling the pieces of a weapon or explosive device on board an aircraft and assembling it on board.

DISCOVERED CONTRABAND

Regardless of airline, and federal employee reluctance to engage in law enforcement activities, some situations are unavoidable. Should contraband be in plain view and the screener has observed it, the passenger no longer has the option to withdraw baggage from inspection. Early case law, such as the language in *United States v. Skipwith, 182* F.2nd 1272 (1973, 5th Circuit) *and United States v.*

Herzburn, 723 F.2d 733 (1984, 11th Circuit) have reasoned that once an obvious threat is observed, there is no question that passengers have forfeited the right to change their minds. They have already consented to the search, and the consent cannot be withdrawn because contraband has been found. The real issue revolves around where to proceed from that point. As stated previously, an appropriate law enforcement officer needs to enter the scenario at this moment. It is likely that federal employees will follow similar procedures in the future.

BATTERY RESTRICTION

As of early 2007, air travelers were no longer able to pack loose lithium batteries in checked luggage. Passengers can still check baggage with lithium batteries if they are installed in electronic devices, such as cameras, cell phones, and laptop computers. If packed in plastic bags, batteries may be in carry-on baggage. The limit is two batteries per passenger. The ban affects shipments of nonrechargeable lithium batteries, such as those made by Energizer Holdings Inc. and Procter & Gamble Co.'s Duracell brand. The FAA has found that fire-protection systems in the cargo hold of passenger planes cannot put out fires sparked in lithium batteries. The National Transportation Safety Board contends that it could not rule out lithium batteries as the source of a cargo plane fire at Philadelphia International Airport in 2006. (Internet: http://tech.yahoo.com/news//ap/ 20071228/ ap_on_ hi_ te/lithium_batteries_travel)

SCREENING PASSENGERS

Originally, passengers who could not be cleared of unaccounted for metal were to be referred directly to a police officer for a patdown search. This procedure proved to be impractical and time consuming. Previously, the carrier or contract agency personnel hired by the carrier performed this procedure if all other means of clearing the passenger had failed. Those other means include having the passenger remove any extraneous metal they may have on their person such as pocket change, extra large belt buckles or the like and walk through the portal again. A hand-held metal detector may also be utilized. Airlines, always concerned about the free flow of passengers through the screening operation, also recommended, in the past, passengers who alarmed the metal detector were to be taken aside for further screening. Consequently, further procedures were automatically done behind a screen or somewhere else in private due to perceived embarrassment. Today, screening by hand-held metal detectors are so commonplace as not to warrant such measures.

Regardless of a slight delay in processing passengers, the best method of handling a passenger that alarms the equipment is to politely ask them to remove any metal in their pockets or on their person that they may have forgotten and reenter the metal detector portal. Today, most passengers will likely do this automatically without even being asked. Should the passenger persistently alarm the machine, further intrusive measures may be required. A useful acronym for the training of new security personnel is STOP:

1. Send the passenger back through the walk-through detector again.
2. Then try a hand-held metal detector to locate the metal.
3. Only then, outside the view of other passengers, perform a patdown search and only if absolutely necessary.
4. Perform a strip search if the passenger still believes they are clearable to board an aircraft and they consent. (It should be noted that TSA personnel never conduct "strip searches"; however, U.S. Customs and law enforcement can.)

Metal that is located on an individual should be removed, and the passenger should always, once again, be requested to walk through the metal detector again. It should also be remembered that metal removed from a passenger that has been located by the hand-held detector does not necessarily

mean that the passenger is metal free. Passengers seeking to outwit screening procedures are nothing if not creative. Some passengers have even been known to plant a piece of metal knowing they will alarm the walk-through detector. They are then scanned by a hand-held detector and happily reveal the alleged cause of the alarm, hoping the screener will let them pass. Unfortunately, a more insidious piece of metal may also have been the cause of the alarm. There is no limit to the extent of their deceit if they really want to defeat security procedures.

All airport security officers have there own war stories about the ingenuity of passengers in attempting to foil the screening process. However, one of the classic situations took place at O'Hare International Airport in Chicago many years ago. The first time the passenger alarmed the equipment he removed a knife. He was screened a second time and security officials located a gun. Unbelievably, the third time was a charm, and .22 caliber ammunition was discovered. Stories such as these reinforce the need to keep walking the passengers through the equipment until they are absolutely clean and no longer alarm the machine. Admittedly, this can sometimes annoy the passenger enduring the process as well as those waiting in line. Regardless, it is a must, and shortcuts should not be employed in the name of expediency. Federal employees, however, will not be directly subjected to airline expediency requests.

Often during rush hours, security personnel could feel pressure to hurry. However, when they do, oversights frequently occur. Another story, which has circulated in airport security circles for years, involved an airport in California many years ago. A woman failed to clear the metal detector. She later convinced security personnel that her bracelet had set off the alarm, but in reality the woman had a gun in her bra. Unfortunately, the hand-held detector could not differentiate between the bracelet and the gun when she raised her hand to a similar position as the location of the gun. She was eventually permitted to board and bragged to her seat companion that she had outfoxed security. Sometimes fate does kick in, though, as it turns out she had bragged to an FAA Security Investigator. Today, hand-held detectors have become much more sensitive, but care is still needed in thoroughly covering all possible locations on a person before clearing them for entrance into the sterile concourse.

Another dangerous procedure is to skip steps in the search procedure. U.S. law is quick to condemn a security officer that has not used the least intrusive method available to search a passenger. In *U.S. v. Albarado*, 495 F.2nd 799 (1974), the U.S. Court of Appeals ruled more than 30 years ago that the frisk of a passenger performed immediately after he or she activates a metal detector is not lawful. This case is still good law and summarizes the need for security personnel to exhaust other efficient and available means first, namely, to have the passenger rescanned by the stationary metal detector and a hand-held detector. Overall the use of a frisk or body search must not necessarily be a last resort to clear a passenger, but must be viewed within the context of a continuum of progressively more intrusive measures. After 11 September, the "frisking" of passengers has become more commonplace. It can only be reasoned that security officials are deeming these "patdowns" as consensual, even though passengers are arguably intimidated into it.

Exactly who does what to whom is also an issue in today's gender-sensitive legal environment. Technically, there is no specific legal prohibition against a male screening a female with a hand-held metal detector, especially if the operator is careful not to touch the individual being searched. The TSA does mandate a gender-specific policy in which enforcement is supported by regulation. Searches of this kind have become commonplace, and the public does not really attach a stigma to them. Of course, searches of the crotch and breast area need to be accomplished as discreetly as possible. Furthermore, if the operator inadvertently touches the individual with the wand, the search has changed character completely, and the legal repercussions change significantly. Professionalism is required at all times because the crotch areas, armpits, waist, and ankles are favorite hiding places of those inclined to pass potentially dangerous articles through security. At the same time, inexperienced security personnel may be reluctant to adequately search body areas considered "private." Specific policies should be developed and adhered to on a consistent basis. Allegations of inappropriate touching will probably continue.

All security personnel should be trained on the proper method to search a person, using a hand-held metal detector. It is simplest to start at the top of the body and to work your way down, keeping the equipment approximately three to four inches from the body. The safest method is to also ask the people being searched to raise their hands above their head, if this is practical, and to stand with their legs slightly apart. As always, the individual needs of each passenger must be taken into consideration. For example, the elderly may not be able to raise their arms very far, and those with certain physical challenges may have special needs. Individuals in wheelchairs also present some unique problems. Discretion is very important and courtesy is required at all times. Nonetheless, security and safety is the overriding goal, and these people must still be appropriately searched.

Cast Scope

In an effort to address the issues related to people with disabilities, the TSA has begun to test the CastScope Security System at airport checkpoints at four airports. In an effort to improve the screening of passengers with prosthetic devices, casts, and support braces, TSA awarded a prototype contract to Spectrum San Diego, Inc. The CastScope pilot began on 25 April 2007, at San Jose International Airport, (SJC). TSA also piloted the technology at Tampa International Airport (TPA), Nashville International Airport (BNA), and Reagan National Airport (DCA) in May and June 2007. In the pilot phase, passengers with prosthetics, cast, or a brace may participate on a voluntary basis. The system uses backscatter technology to produce an x-ray image to quickly and noninvasively identify any potential threats. Backscatter scans a narrow, low-energy x-ray beam over the body surface. The reflection, or backscatter, of the beam is detected, digitized, and displayed on a monitor. The high contrast image generated allows TSA to differentiate between articles such as braces, prosthetics, and external medical devices, and prohibited items.

The CastScope was designed to supplement the walk-through and hand-held metal detectors for passengers with casts, braces, heavy bandages, or prosthetics that may set off an alarm because of the metallic components of the devices by providing an x-ray image for TSA to assess concealed threats. The scanning cycle lasts approximately 2.5 seconds, and produces a computer-enhanced image of the 6×8-inch examination area almost immediately on the computer screen. It does not emit a magnetic field and will not cause any adverse medical consequences to implanted medical devices or any other disability-related equipment.

Rating Hand-Held Metal Detectors

The FAA rated numerous hand-held metal detectors in a report entitled, "Screening with Hand-Held Detectors," DOT/FAA/CT-95/49. Twenty-six experienced security officers rated 14 of the most commonly used devices. The criteria included:

- Alarm sound
- Maneuverability
- Ability to detect metal objects
- Weight and length and position of controls
- Grip comfort

Scanners should be proficient in the use of the equipment. If the device is too heavy or too large for a particular employee, either a smaller device is appropriate or a larger security officer.

Today it is no longer an issue; however, previously there was some question whether nonpassengers, air crews, visitors, and vendors should also be subject to search. The regulations were eventually amended to include everyone and 49 CFR 1540.17 (formerly) FAR 107.20 reads that "no person may enter a sterile area without submitting to the screening of his her person and property." The logic was simple. It serves no purpose to search only passengers when any of the other categories of

people were perfectly capable of terrorizing an aircraft or airport. They were also capable of simply passing something dangerous to a terrorist who had already cleared security. Air crews constantly complain about having to clear security the same as passengers and other employees. However, it is important to remember that uniforms are easily copied and or stolen, and therefore are accessible to terrorists. Wearing a uniform and impersonating a flight attendant, maintenance worker, or pilot is easy to accomplish.

Of course, none of these procedures are effective if the passenger or terrorist is successful in completely bypassing the security checkpoint. For example, Globe Aviation Security was the contract security service in the employment of Northwest Airlines at the Minneapolis/St. Paul Airport. Since 1999, police reports at the airport documented at least seven bypassing incidents, which indicated that people do masterfully evade the checkpoint screening procedures. In another documented case, a Trans World Airlines agent saw two men hastily walk right by a checkpoint without being screened. Globe personnel claimed they saw nothing, and the two men were never located. In another incident, the FAA while testing Globe Security, reported that while a screener was distracted with another passenger's baby stroller, the FAA agents were permitted to pass unchecked. Even though a supervisor did question them, they managed to convince even the security supervisor that they had already been screened. The agents eventually made it all the way to an aircraft (Internet: "Security Breach at Airport"). Such incidents were not occurring all over the planet and are not just a problem of Globe Security in Minneapolis. Security personnel, whether contract or federal, are never going to be able to provide 100 percent protection. All that can be expected is that they do the best job they can under sometimes very difficult circumstances.

Other loopholes in the overall procedures continue to exist. For example, as soon as you clear security, some restaurants and certainly the first-class lounges often have knives available for the taking. On top of that, almost anything can be used as a lethal weapon. It raises the question whether knitting needles and similar items should be confiscated from grandma's seeking to knit on the aircraft. Furthermore, even pilots have been known to attempt to circumvent the system. They have been known to bend sharpened metal or plastic restraints inside the rim of their airline hats, rationalizing their conduct as meeting their own self -defense needs once on board. The potential use of stun guns in the future will add to the mix.

Body Search

Should all efforts to clear an individual by means of walk-through or hand-held metal detectors fail, the possibility of a body search or patdown presents itself. Clearly, such a procedure requires consent, and the individual must be allowed the option of refusing the search. If a traveler chooses to leave the airport, that is certainly an option available to them. No force should ever be used by airport security personnel to perform a patdown search. Certified law enforcement officers engaged in an arrest or a Terry-type (as in *Terry v. Ohio*) search certainly constitutes another matter. Again, it is important to make the distinction that airport security professionals are seeking to deter individuals from gaining access to an aircraft with a weapon. They are not criminal investigators sworn to arrest and detain criminals. Additionally, never conduct a patdown search without a witness being present. The potentialities for lawsuits are always present. Therefore, not only for the protection of the person being searched, but also the person conducting the search, a witness is a must. For example, security personnel at Sky Harbor Airport in Phoenix were accused of inappropriately touching several flight attendants during the Spring of 2002.

It is also important to point out that some jurisdictions around the world are not held to the requirements of the U.S. Constitution and specifically the Fourth Amendment. For example, in Japan, people meeting certain profiles and some merely randomly selected passengers must submit to an entire body search regardless of whether they have alarmed a metal detector or not. Many other countries have laws that permit this type of conduct by local law enforcement or security personnel to meet their own stringent security needs. Generally, a gender-specific witness is usually

FIGURE 7.4 A TSA officer holds a baby alligator confiscated after a passenger admitted to having attempted to smuggle it on board an aircraft. (Source: Transportation Security Administration. www.tsa.gov).

present; however, international travelers should be aware that some areas of American sensitivity to physical contact of "private areas" are not necessarily universally recognized elsewhere.

Medical or orthopedic devices also present unique situations. Usually, the individual can be cleared by concentrating on the location of the device, such as a brace or a metal plate in the body. However, as always, such places may be ideal places to secret a dangerous device due to security's reluctance to hassle a person with such a disability or special need. Passengers who wear medical or prosthetic devices are generally not required to remove it; however, screeners will conduct alternative screening on the device in accordance with the TSA standard operating procedure (SOP).

There are even some special situations where an individual may choose a body search over the metal detector (see Figure 7.4). One such special circumstance is a heart patient with a pacemaker who regardless of the unlikelihood the metal detector will disrupt the surgically implanted device insists on avoiding the metal detector. Long ago scientific research failed to show any effect on pacemakers. However, certain individuals may still choose to request a body search in preference to walking through the metal detector. Security should permit them to do so. Another special situation concerns the deaf. It is important to be patient and explain any requests slowly and with courtesy so that they can read the lips of the person explaining the procedure. If an employee is familiar with sign language, all the better. If not, written materials should be made available to the hearing impaired. The same courtesies should be provided to the blind and non-English-speaking passengers, plus materials should also be made available in Braille.

Screening Airport and Airline Employees

In the early 1970s and under an old set of rules, ACSSPs often allowed flight officers and flight crew members with proper identification, and in uniform, to be exempt from screening, regardless of where they entered the terminal. The procedure could have led to some serious consequences and has since been recognized as setting a dangerous precedent. Remarkably, this practice lasted up until 1987 when new rules were implemented. It is well known that many airline employees consider the security requirements to be tedious; however, the relatively small inconvenience is reasonable under the circumstances.

It should be noted as well that as of 1989, all persons entering a restricted area or the operations area are now required to possess appropriate computerized access cards. Unfortunately, the airline employee identification documents are almost as easy to procure as uniforms. The advanced systems on the market today do permit airline personnel with a special form of unimpeded access. These special access cards are generally not furnished to tenants, concessionaires, or contractors,

as they are definitely not considered airline or airport employees per se. However, as technology improves, so does state-of-the-art duplication ability. New advances in biometric access controls have somewhat closed this loophole. Currently, all airport employees, vendors, and airline flight crews must also be screened prior to entering the sterile area of an airport's concourse.

It should be noted that TSA Administrator Edmund S. Hawley requested in a 5 August 2005 document a number of changes to airport screening, including proposals to allow knives, ice picks, throwing stars, and bows and arrows to be carried onboard airplanes. The TSA also announced that some individuals should be exempt from airport security screening, including Members of Congress, Cabinet members, state governors, federal judges, high-ranking military officers, people with top-secret security clearances, and airline pilots.*

Screening Diplomats

Generally, both U.S. and foreign diplomats are screened unless specifically exempted by the Department of State and the TSA. However, their proprietary documents are exempt from any form of screening such as x-ray or physical inspection. On the other hand, if a weapon or other contraband is discovered on properly documented foreign diplomats, international law provides they are entitled to diplomatic immunity. Diplomatic immunity is a concept that prevents them, in most cases, from being prosecuted in the country in which they are stationed. Diplomats have historically been afforded this protection, and the practice is not likely to be changed regarding airports. Additionally, of importance to security personnel is the fact that a diplomatic courier also has special status. Basically, a diplomatic courier, who presents official credentials, is entitled to board the aircraft with the diplomatic pouch unscreened. According to long-standing international agreements, the bag is never to be inspected. Unfortunately, some diplomats have abused these exemptions. Diplomatic privileges are a well-known and necessary concept enabling proprietary and classified materials to be moved without threat of exposure. It is when embassies and diplomatic personnel use this as a tool to smuggle weapons, dangerous materials, and terrorist-related support that problems arise.

Another related unique circumstance involves the carriage of classified material by members of the U.S. Armed Forces. Classified material is carried aboard aircraft by members of the Armed Forces Courier Service located at Fort Meade, MD. Formerly, FAA Advisory Circular 108 pertained to these materials and provides for transportation of them without inspection by airport security or law enforcement personnel.

REGISTERED TRAVELER PROGRAM

The registered traveler (RT) program, initiated in January of 2006, became available in 14 U.S. airports. The current phase of the RT program, known as the Registered Traveler Interoperability Pilot (RTIP), introduces interoperability among participating airports and air carriers. It is accessible to travelers who are U.S. citizens, lawful permanent resident aliens, or nationals of the United States who volunteer to undergo a TSA-conducted security threat assessment (STA) "to confirm that they do not pose or are not suspected of posing a threat to transportation or national security" (Internet:

* *Note*: According to the Association of Flight Attendants (Internet: *http://ashsd.afacwa.org/?zone=/ unionactive/ view_ article.cfm&HomeID=15826*), the TSA Office of Law Enforcement/Federal Air Marshal Service sponsors a voluntary crew member self defense training (CMSDT) program available to any actively employed flight or cabin crew member. This crew member self-defense training has undergone some changes. The old training program was three days of hands-on training. The new training program is a one-day hands-on training (8 hours). According to the new *TSA CMSDT website Overview*, the training "*is* available to any actively employed flight or cabin crew member. The program is delivered in two parts. First, the crew member receives and reviews a self-paced, interactive DVD and student manual designed to familiarize him or her with basic self-defense concepts and techniques. After completing the review and a short written assessment, the crew member attends one day of 'hands-on' training at a participating community college."

http://www.tsa.gov/what_we_do/rt/rt-travelers.shtm. Retrieved 16 Jan 2008). To enroll, applicants voluntarily provide sponsoring entities and service providers with biographic and biometric data. The program requires passengers to pass a full background check, including fingerprints and iris scans. The STA includes checking each applicant's identity against terrorist-related, law enforcement, and immigration databases that TSA maintains or uses.

Because this program requires the collection of personal information about members of the public, TSA is required to issue a Privacy Impact Assessment (PIA) to provide the public with an outline of how the information collected from an RT applicant will be processed and protected under the RT program. The reasonable TSA fee of $28 per year per RT applicant or participant was set via Federal Register Notice on 24 November 2006 and is standard for all initial enrollments and renewals. In addition, *Clear*, the name of one of the vendors or enrollment providers, charges the traveler an additional $100 per year, which entitles them to use special airport screening lanes that are supposed to significantly cut screening time by bypassing regular lines at the airport.

New York's John F. Kennedy International Airport RT program marked the opening of the official launch of the concept. Previously, Orlando International Airport had run the only sponsored program since 2005. Later San Jose, CA's Mineta San Jose International Airport, was the initial airport on the West Coast, and Cincinnati, OH in the mid-West began to provide fliers with a fast path through inundated security lines. Travelers must present their "clear cards" that compare the stored data of passengers against a fingerprint scan prior to approving a traveler. Around 2500 travelers have applied at San Jose for the cards, and more than 30,000 people have joined Registered Traveler at Orlando, FL (Internet: http://www.usatoday.com/travel/ news/2007–01–16–registered–tr avelerx.htm).

NO FLY LIST

Every time a passenger checks in at the ticket counter the name is run through a computer to make sure that individual is not on the "No Fly List." The list is part of a government database compiled after 11 September to prevent suspected terrorists from accessing airplanes. In 2003, President Bush directed the nation's intelligence agencies and the FBI to cooperate in creating a single watch list of suspected terrorists. A version of that list is given to the airlines and the TSA to prevent anyone considered a threat to civilian aviation from boarding a plane. Complaints have abounded regarding the list, including accusations that the names of babies are on the list and common Irish names that are similar to thousands of Americans who are in no way associated with the Irish Republican Army (IRA). In response, TSA Administrator Edmund (Kip) Hawley told the Senate Commerce Committee during a hearing in 2007 that "to assure the accuracy of the no fly list itself, we will shortly conclude a case by case review of every name on the no fly list. Working with our partners at the Terrorist Screening Center and in the intelligence community and law enforcement, this effort will effectively cut the no fly list in half" (Internet: http://www. govexec com/story _page. cfm?articleid=35890&dcn=to daysnews).

Consequently, in 2007, the TSA launched the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP), an easy-to-use, single point of inquiry for travel-related issues. DHS TRIP was developed to provide a central gateway to address watch list misidentification issues, situations where individuals believe they have faced screening problems at immigration points of entry, or have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at the nation's transportation hubs. DHS TRIP will share information it receives with the Department of State and airport and airline operators, as needed, to resolve issues. DHS TRIP will function in accordance with the routine uses identified in the applicable Privacy Act System of Records Notice (SORN), which, along with the notice of proposed rule making (NPRM), has been submitted to the Federal Register and will soon be published. To view the SORN and the NPRM, see http://www.regulations.gov/ Source: http://www.dhs.gov/ xnews /releases/pr1169062569230. shtm. Various estimates of the list's size, which is classified, have ranged from 50,000 to 350,000 names. Complaints have persisted. For example, Sen. Ted Stevens, R-AK, complained that his wife,

Catherine, was being identified as "Cat" Stevens and frequently stopped due to confusion with the former name of the folk singer now known as Yusuf Islam, whose name is on the list. Hawley explained that Secure Flight, the new passenger screening program, which he hoped would be running in 2008, would make such problems "a thing of the past."

FEDERAL BEHAVIOR DETECTION OFFICERS

Security screeners schooled in the psychology of observation now patrol several major airports, pulling aside passengers whose behavior may be a tipoff to hostile intention. The federal behavior detection officers are on the lookout for passengers displaying extraordinary stress and fear, or signs of deception during questioning. All of these traits constitute earmarks of terrorists who may be on scouting missions to find weak links in airport security. The practice, pioneered by Israeli airport security, involves picking apparently suspicious people out of crowds and asking them questions about travel plans or work. Meanwhile, their faces, body language, and speech are being studied. The TSA has trained nearly 2,000 employees to use the tactic, which is raising alarms among civil libertarians and minorities who fear illegal arrests and ethnic profiling. The issue is related to whether, in fact, the TSA should be operating a federal police force. The effectiveness of such a practice has clearly been validated by the Israelis, but others opine that the practice has really not been validated.

THEFT

Larceny at checkpoints by roving thieves is an increasing threat to passengers. Organized bands of "airport proficient" thieves have been known to work the airports looking for absent-minded passengers willing to separate themselves from their baggage for a sufficient period of time to have it ransacked. There have been repeated claims over the years of valuable possessions going into the x-ray machine but never coming back out. Diligent efforts need to be made to protect the passengers from some very organized airport thieves preying on the unsuspecting vacationing traveler.

Two or more persons usually effectuate this type of crime. Criminals well-organized and quite well-practiced at the crime have perfected an ingenious technique. Security personnel need to be trained, but individual passengers must also remain ever alert in the airport environment. "Criminal activity takes place at airports, and people who conduct the activity are always looking for opportunities," said Richard Doubrava, managing director of security for the Air Transport Association (*Star Tribune*, 2001).

For example, a woman was in line to pass through the metal detector placed a carry-on bag and her purse on the conveyor to be scanned when a man pushed in front of her. He set off the alarm as he went through the metal detector and was forced to go around again. By the time the woman got to the other side of the security check her purse was nowhere to be found. "A crime of this nature is a crime of opportunity," said Inspector Robert Belfiore, commander of the Port Authority of New York police precinct that includes the airport (*Star Tribune*, 2001). Passengers and security personnel need to constantly remain alert for organized and well-practiced larceny.

Belfiore recommends further that passengers traveling in pairs or groups should have one person without luggage pass through the metal detector to await a companion's belongings on the other side of the x-ray machine. A passenger traveling alone should alert security personnel immediately if there is a distraction or if the conveyor stops while a personal item is out of sight.

Many security companies did not really understand the liability that they were exposed to when their own employees or crackerjack thieves help themselves to passenger property. In *Gin versus Wackenhut,* 741 F. Supp. 1454 (D. Hawaii 1990), an airport security company was found to be liable for $140,000 when a passenger's bag, allegedly full of jewelry, was missing after it passed through an x-ray machine at a security checkpoint. Airlines who had attempted to limit liability by printing on the ticket a $1250 limitation of liability clause have been held liable regardless. In *Wachenhut Corp.*

v. Lippert, 591 So. 2d 215 (Fla. App 1991), the court held that an airline ticket's professed $1250 limitation on liability for baggage did not apply to passenger's loss of $431,000 worth of jewelry in a handbag while passing through a metal detector because negligence was found to have occurred. Federal courts had been somewhat more sympathetic to airlines and security companies at airports. In *Kabbani versus International Total Services,* 805 F. Supp. 1033 (D.DC 1992), the court held that damages in a woman's suit against a security company at an international airport, from alleged theft of her purse containing hundreds of thousands of dollars in jewels, was limited to $1000 under the Warsaw Convention. She was scheduled to fly on an international flight. The court did note that the security service would have been liable if the plaintiff could have proven "willful misconduct." All of this dicta, or judicial opinion, was elaborated on in the published decision, despite the fact that the security company had not even brought up the Convention liability restrictions as a defense. Civil suits against federal employees will have to be filed under the Federal Torts Claim Act.

POTENTIAL TSA ETHICS ISSUES

The TSA has undergone some significant criticism for lavish spending, questionable ethics, and subpar employee performance in three separate audits released in 2005. The reports, totaling 93 pages, were issued by acting Homeland Security Department Inspector General (IG) Richard Skinner. Two assess passenger and baggage screening procedures at domestic airports, whereas the third spotlights irregularities in the development of TSA's $19 million crisis management center. Evidence of suspicious purchases first surfaced in 2003 during an initial investigation by TSA's Office of Internal Affairs and Program Review. According to the IG, that investigation uncovered "unethical and possibly illegal" activities by employees, improper use of purchase cards, and a $370,000 expenditure for artwork and silk plants.

In another report, Skinner urged TSA to make better use of screening technology and to supervise screeners more closely to prevent baggage theft. He also recommended that TSA supervise screeners more closely and train them in ethics to prevent theft. Skinner also released an unclassified five-page summary of a longer report evaluating screener performance at 15 unnamed U.S. airports. Auditors visited the airports in 2003 and returned again between November 2004 and February 2005, both times trying to smuggle prohibited items through security checkpoints.

Screeners' ability to detect the hidden objects on people and in checked baggage was about the same in both tests, according to the report. The testers found most screeners to be diligent and conscious of their responsibilities, but, the IG wrote, "the lack of improvement since our last audit indicates that significant improvement in performance may not be possible without greater use of new technology." Skinner said auditors were not able to determine the extent of baggage theft either before or after TSA took over screening in 2002. But the report noted that TSA has fired 37 screeners for committing theft and settled or fully paid 7000 claims totaling $736,000 for items missing from passengers' bags. Based on that data, the report recommended that TSA beef up screener supervision, consider installing electronic surveillance tools near inspection stations, and add an ethics module to the screener training curriculum. TSA said it continually reviews its supervision and surveillance procedures to satisfy requirements in the 2004 Intelligence Reform and Terrorism Prevention Act. It said it plans to install electronic surveillance systems, but that funding is unavailable.

PUBLIC RELATIONS

Airport security personnel who look and act professionally are far more effective than those who do not. Security officers are walking advertisements as the quality of the security at any given airport. It is important for security personnel to recognize the special needs of the elderly, individuals with disabilities or impairing diseases, the homeless, intoxicated or drug impaired individuals, and those people not proficient in English. For example, the elderly may have Alzheimer's disease and may

appear intoxicated or confused. Additionally, those with epilepsy may require special attention. Security personnel should be familiar with the symptoms of those diseases and treat such individuals calmly, quietly, and with respect.

A disability is any physical or mental impairment that substantially limits one or more major life activities. The Americans with Disabilities Act (APA) passed in 1990, states, "No individual shall be discriminated against on the basis of disability in the full and equal employment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation." If found guilty of violating this particular law, private security firms could be potentially fined from $50,000 for a first offense, and up to $100,000 for subsequent offenses. Therefore, preparation for any individual with a disability covered by the Act is a wise precautionary measure. Compassion must be balanced against legitimate security needs.

AIRBORNE AIRCRAFT SECURITY

Of course, once the aircraft is airborne, security becomes the responsibility of the people on board. In a move, hopefully not approved by the Department of Transportation, United Airlines has begun training pilots to use stun guns for self defense. A United official was quoted as saying, "Our goal is to make sure we keep the bad guys off the airplane, and if they get on the airplane, to keep them out of the cockpit and if they try to get into the cockpit, that we have a way of absolutely stopping them" (Internet: http://www.cnn. com/2002/US/04/23/gen. united.stun.guns /index.html?related). In March 2002, Secretary of Transportation Norman Mineta publicly advised the Air Line Pilots Association he opposed the presence of lethal weapons in the cockpit. He did not, however, rule out the presence of nonlethal weapons. Despite the inherent problems, Congress later went ahead and approved the use of firearms by pilots.

Federal Flight Deck Officers

To be selected for Federal Flight Deck Officer (FFDO) training by TSA you must do the following:

- Successfully complete all selection assessments including any specified psychological, medical, or physical ability requirements.
- Be determined to meet all established standards of TSA.
- Be available to attend the training program in its entirety on your own time and at your own expense (the cost of the training and equipment are covered by TSA; volunteers are responsible for their own travel, lodging, and daily expenses).

Training

Initial training will be conducted in a one-week session that will typically require volunteers to arrive midafternoon on a Sunday and remain through conclusion of training the following Saturday afternoon.

- All trainees must be present for the entire training session.
- All trainees must attend the training on their own time and at their own expense (out-of-pocket expenses are estimated to be $200, plus travel).
- The training is physically demanding. It is recommended that volunteers for the FFDO program be of average to above average physical fitness to avoid any potential for injury.
- All trainees must participate in required firearms re-qualification activities on their own time and at their own expense.

- Successful completion of training is required for deputation (according to the TSA website Internet: http://www.tsa.gov/public/interapp/editorial/editorial_multi_image_with_table 0210.x).

There are airline pilots that disapprove of the rearmament of pilots. Many airline pilots were armed until 1987, when the federal government banned guns in the cockpit. Now pilots can become armed after volunteering for training and being deputized as federal law enforcement officers. In the five years since, the program has had an exceptional safety record, performing better than any law enforcement agency in the country, but of course they have not been required to use a weapon to date. The program regained a spotlight in the media when it became public that airport screeners were missing up to 75 percent of banned items. Pilots were the first to reiterate that pilots serve as the last line of defense and, additionally, that Federal Air Marshals are only able to guard a small number of domestic flights. Armed pilots provide a cheaper and more viable source of protection. However, there are significant problems with the concept. First, the gun can only be shot once. Additionally, if there is more than one terrorist, there is the problem of recharging and reloading the gun. In all likelihood, one of the pilots would subsequently be killed. With only three people on board competent to fly the aircraft this presents a huge safety issue.

CONCLUSION

Most if not all passengers arriving at airports today completely understand that they will be subject to search for weapons and explosives. The design of airports to accommodate security needs has advanced over the years. Major airports have generally accepted the placement of the security function at the entrance to major concourses, creating a sterile concourse past the security checkpoint. Smaller airports have not had the need to do this, and some of the larger international airports have chosen to establish a security checkpoint at both the entrance to the concourse and again at the gate boarding area. These decisions are based on the perceived threat at a particular airport and the perceived threat at the scheduled destination of the aircraft.

Since the 100 percent screening requirement has come into full effect, procedures have matured and adapted to the legal requirements imposed by the courts. The courts will also scrutinize any significant changes imposed by the TSA. Screeners are given the responsibility of the safety of billions of travelers each year. They possess one of the last clear chances to catch a potential terrorist before a catastrophe occurs. Proper training and dedication to duty is absolutely required if the airports of the world stand any chance of being protected. Procedures, which have already been scrutinized by the courts, need to be followed. Good judgment should attempt to be exercised at all times as well. The perception of the public is still very important. Passengers may well balk at repeated patdown searches and forced shoe removal. This is especially true if they do not feel more secure because of the procedures. Watching disabled elderly passengers randomly searched while healthy "potentially capable" hijackers walking through security uninterrupted sends the wrong signal to the terrorist and the public.

In addition, considering the diversity present in today's traveling public, the personal attributes of each traveler including physical, cultural, and linguistic differences must be recognized. Admittedly, good judgment is often impossible to teach someone who already does not have any. However, the day-to-day security of an airport is almost totally dependent on the professionalism of the security and administrative staff charged with that responsibility. The only way to keep that security at its peak performance is to hire good people. This is often easier said than done; however, the consequences of failure to do so are catastrophic. Another issue relates to the question of more armed officers or better preflight security. The following chapter will discuss hiring procedures and motivation elements of the security profession.

REFERENCES

ASI, *Airwise*, Internet:http://www.asi.com., 8 August 2001.
Association of Flight Attendants, http://ashsd.afacwa.org/?zone=/ unionactive/ view_article. cfm&HomeID=15826.
FAA, "Screening with Hand-Held Detectors," DOT/FAA/CT-95/49.
Fay, Jim, "FAA Downplays Former IG's Report on Airport Security Flaws: Reports Suppressed?" http://www. emergency.com/arprtrpt.htm. 8 August 2001.
http://ccfr.access.gpo.gov/otcgi/cgr. pg.1, 19 June 2002.http://tech.yahoo.com/news//ap/ 20071228/ ap_on_ hi_ te/lithium_batteries_travel.
http://www.alpa.org/internet/tm/ tm061198.htm. 22 April 01, pg. 2.
http://www.cnn. com/2002/US/04/23/gen. united.stun.guns /index.html?related.
http://www.dhs.gov/ xnews /releases/pr1169062569230.shtm.
http://www.govexec com/story _page.cfm?articleid=35890&dcn=to daysnews.
http://www.lindhdefense. info/ 20020613FactsSuppSuppress.pdf.
http://www.regulations.gov/.
http://www.tsa.gov/public/interapp/editorial/editorial_multi_image_with_table 0210.x).
http://www.tsa.gov/what_we_do/rt/rt-travelers.shtm. Retrieved 16 Jan 2008.
"Security Breach at Airport, http://www.kstp.com/index.cfm?viewer, 3 July 2001.
www.tsa.gov/311.
Registered Traveler, http://www.usatoday.com/travel/ news/2007−01−16−registered−tr avelerx.htm.
Star Tribune, "Thief who set off airport alarm made off with woman's purse," Sunday, 28 January 2001, pg., G2.
Tierney, John, "Didn't Pack Your Own Bags? Why Airports Want To Know," *Star Tribune*, Sunday 8 July 2001.

8 Private Security Personnel versus Transportation Administration Security Personnel—Increased supervision?

NEWS

June 2002: Security rescreened 5000 passengers when a passenger with a knife passed through security at Dulles International Airport. Over 30 flights were delayed for as long as 2 ½ hours.

1 July 2002: Airport screeners at 32 U.S. airports failed to detect replica weapons in 24 percent of undercover tests by the Transportation Security Administration.

25 January 2002: Police began cracking down on identity fraud at Miami International Airport after the airport's security admitted it failed to do background checks on more than 100 workers. New identification cards will restrict where workers can go and at what times.

6 January 2003: An airport screener was discovered asleep at his post, and security personnel were forced to search all concourses. Twenty-three incoming flights were delayed.

29 July 2005: The government plans to reshuffle its passenger and baggage screeners, drawing protests from some airports slated to lose workers. Pittsburgh, PA and Portland, OR, will be among those taking the biggest hits. Las Vegas, Dulles International Airport in Washington, D.C., and Los Angeles International Airport will gain, according to the plan.

INTRODUCTION

In the past, a vast majority of the people operating baggage and passenger screening systems in airport terminals were contract security guards. The airlines hired airport security firms to conduct essential searches, and passengers depended on their expertise to maintain the safety of airports and aircraft around the globe. They were poorly trained and poorly paid, often only receiving minimal training. Their training often consisted of instruction on the operating systems and procedures by someone simply employed longer than the new employee. The instructor or supervisory employee probably did not have very extensive experience, considering most contract firms experienced a 100 percent turnover rate per year or more. Demographically, they were young, women, retired, and representative of a minority segment of the population. Frequently, English was their second language. It was ironic that the public relied so heavily on the dedication of these people for their

safety and security, but failed to reciprocate with appropriate compensation to attract more qualified personnel.

The situation changed effective 14 November 2002. The federal government assumed this responsibility. After the tragic events of 11 September, the Bush administration had concluded that the government needed to step up to the plate and provide adequate security to the nation's airports. The government clearly had plenty of notice prior to September to boldly remedy the problem and simply failed to do so.

The General Accounting Office (GAO) had published a report in 2000 clearly portraying the inadequate security being previously provided. The report indicated that turnover among personnel was a huge problem. Specifically, the report stated that "from May 1998 through April 1999, screener turnover averaged 126 percent at 19 of the nation's largest airports. Five airports reported turnover exceeding 200 percent, and one experienced a 416 percent turnover rate" ("Internet: http://www.securitymanage ment.com/library /000855.html). The GAO strongly recommended that salaries and benefits be increased to attract more qualified personnel and to retain the competent employees.

In another report dated December 2000, the Department of Transportation's Inspector General stated that too many airport employees with unknown or questionable backgrounds are given access to secure areas. "Randomly pulling workers' files at six airports, investigators determined that 16 percent had undergone incomplete background checks, and 8 percent had no checks at all" (Morris, Jim, 2001). In early 2007, two Orlando-based airline workers were charged with carrying 14 guns onto a Comair flight. Consequently, the TSA stepped up screening of airport workers nationwide amid growing concerns that nearly 1 million employees can get into airplanes or other restricted areas without going through security (see Figure 8.1). The agency sent 160 security officers to five airports in South Florida and Puerto Rico after the incident.

Years previously, there had been some additional alarming studies on the need for improving security at U.S. airports. In 1987, a Federal Aviation Authority (FAA) evaluation at major airports discovered that screeners missed approximately 20 percent of the potentially dangerous items that passed in front of them. Another study revealed the chilling statistics that screeners in European airports detected twice as many test objects as U.S. screeners. An FAA report concluded that "people who had longer training, somewhat better pay and benefits, and better ongoing testing by screening companies had much better performance in detecting objects than comparable screeners in the United States." (Rochelle, 2000).

In response to strong encouragement from the White House, Congress quickly met after 11 September to draft new airport security legislation. It was signed into law on Monday, 19 November 2001. There has been renewed intense focus on the role airport security screeners play in protecting

FIGURE 8.1 In 2008 a TSA screener identified an undeclared firearm in a checked bag, and not just any firearm, an assault rifle with more than 10 empty magazines. (Source: Transportation Security Administration. www.tsa.gov).

Figure 8.2 The symbol of the new Transportation Security Administration (TSA). The agency, which has been tasked by Congress with monitoring and executing security plans and procedures at all United States' transportation facilities since 11 September 2001, faces an enormous challenge. In the aftermath of the terrorist attacks, TSA swelled rapidly to almost 65,000 employees. (Source: Transportation Security Administration. www.tsa.gov)

passengers and crew. Consequently, the new law made provision for the establishment of government paid airport security personnel. New federal duties include supervising passenger and baggage security, performing background checks, and training screeners and other security personnel. Other duties include purchase and control of all equipment and oversight of security patrols. The intent of the new law is to bolster training procedures and government supervision of all airport security personnel. The program was approved and was generally in place by November 2002. An evaluation of the success of the new program remains to be seen (see Figure 8.2).

Unfortunately, as of September 2002, a year after the tragic events, problems still plagued the airport security program at most airports. Over the Labor Day weekend, reporters from the New York Daily News concealed potentially deadly weapons on 6 major airlines, at 11 airports on 14 different flights. Seeking to test the more stringent requirements imposed post 11 September; the reporters carried boxcutters, razor knives, and pepper spray. Not a single item was discovered or confiscated. The failures were all a result of both technological and human error. Better equipment and better training are clearly a necessity for the future.

More than a million aviation workers, including pilots, mechanics, and flight attendants, eventually were included in the requirement of undergoing more thorough background checks. The Transportation Security Administration (TSA) took over the job of checking the backgrounds of 1.2 million aviation workers. The agency will also check anyone applying for a job requiring a federal aviation license. Previously, background checks had been done by the FAA. The increased scrutiny came as the Department of Homeland Security (DHS) cracked down on the possibility of attacks by workers who do not have to go through security checkpoints to get on a plane or enter sensitive areas. The TSA takeover meant every licensed aviation worker would be checked against the government's complete terror watch list, which the FBI runs, instead of a partial list the FAA had used. The FAA licenses 21 types of workers including flight instructors, air-traffic controllers, dispatchers, and flight engineers. Background checks are done automatically by a computer that compares biographical information about aviation workers to the terrorist watch list. Many airport workers, such as baggage handlers and store clerks, are not licensed, but already face TSA background checks. In addition, licensed aviation workers will be rechecked every time the Terrorist Screening Center's database is updated, which happens almost daily. Previously, the FAA checked people only when they applied for an aviation-worker license and did not have the resources to do "perpetual vetting."

CRIMINAL GUARDS: FOXES GUARDING THE CHICKENS

The caretakers of security at airports, unfortunately, were not above being bribed, engaging in criminal activities, or just being noncommitted to the job. These circumstances often resulted in significant laxness in security. The situation has not really changed all that much despite 11 September. Security at London's Heathrow Airport was overhauled in March 2002 after two multimillion dollar heists in a two-month period. The British government announced more stringent background

checks on employees, tighter restrictions on access to sensitive areas, and now requires security companies to be on an approved list.

The job as a contract screening employee was not one that children aspired to become while growing up. As mentioned, more often than not, the job paid poorly, provided little chance for advancement or promotion, and most likely provided little training for those that were even somewhat dedicated to the job. On top of that, the screeners were frequently subjected to verbal abuse by passengers, airline employees, allegedly by FAA personnel, and by their own coworkers. In fact, a national report cited this abuse as the most regularly cited cause of leaving the job, as opposed to low pay and virtually no benefits.

Of primary concern was the idea that most companies were struggling to find individuals willing to do the job at all. The government thought that it had more than enough applications to fill the first federal positions at Baltimore Washington International Airport in early 2002 only to realize many either would fail to show up, failed the background check, or failed the training to become a screener. Primarily, many companies either screened the applicants poorly or were simply willing to hire anyone who applied, regardless of their background. Those companies that did attempt to screen employees properly found the process expensive and often undependable. For example, the process of sending fingerprints off for a background check could be lengthy and time-consuming. Some firms were forced to let the potential employee engage in security functions prior to receipt of a completed background check because they were chronically plagued with understaffed checkpoints.

One company made some notable mistakes. Argenbright Holdings Ltd., the airport contract security company hired at Philadelphia International Airport was fined more than $1.5 million for allowing untrained employees, some with criminal records, to operate security checkpoints. The employees had convictions in crimes that included drug dealing, kidnapping, aggravated assault, and theft. On top of that, in October 2000, the company pled guilty to two counts of making false statements to the FAA. The company had already agreed in April 2000 to pay more than a million U.S. dollars in fines and costs for falsifying training and background checks. The company was also ordered to pay $350,000 to 38 different airlines and was scheduled to be on probation for three years. Three former employees were also sentenced for conspiracy and fraud related charges (Internet: http://www.apbnews.com /newscenter/ breakingnews/2000 /10/23/airport1023-01). Unfortunately, the company once again made the news as the providers of airport security at Boston's Logan International Airport, departure point of the two jets that crashed into the World Trade Center in 2001. Since that time, the Department of Justice also has indicted them for repeated failures to run appropriate background checks on its employees and also for falsely verifying that checks had been done. Additionally, they were allegedly permitting the test scores of screeners to be falsified and high school graduation credentials to be counterfeited.

In another situation, a traveler alert was issued for O'Hare International Airport in Chicago. The alert warned passengers that an organized theft ring was operating at security checkpoints. The alert, issued in 1997, was in response to the discovery of a five-man South American organized group of thieves preying on travelers as they processed through security checkpoints. One member of the ring would carry something in a pocket to set off the metal detector. Consequently, they would have to walk back through, in essence, holding up the line, thereby creating a distraction. Their partners in crime would walk off with someone's carry-on luggage. They were highly successful. Chicago Police Department Lt. Neal Sullivan of the O'Hare police unit was quoted as saying, "It's the same method of operation, the same training. Across the country, intelligence has shown they literally go to school for this" (*ERRI Daily Intelligence Report*, 1997).

Airport operators generally contracted for airport security by accepting bids from the nation's 10,000 or so private security companies. The FAA set forth regulations for air carriers, but put the responsibility of handling screening of baggage and people back on the airlines. More often than not, the lowest bidder won the contract regardless of quality of services. Generally, the airlines did not want to pay extra for training and the often fledgling security company could really not

afford it. Critics would argue that the airlines were more concerned with profits than safety; often disregarding the shortsightedness of this approach.

Poor operator performance was another principal weakness of passenger screening systems. Airport security screeners, who are preoccupied with interpersonal problems on the job and poorly trained, are still required to identify sometimes faint indications of infrequently appearing target items. Missing such indicators can have catastrophic results if a bomb or other explosive device survives the screening process. This problem will remain and will prove challenging to the federal supervisors.

The relationship between pay and performance is not necessarily a determinative one. Experts would argue that increased pay is not likely, in and of itself, to solve the problem. The government must place a renewed emphasis on attaining job effectiveness goals. This process will likely involve the application of two types of factors. Those factors will consist of those that attract and keep people on the job (maintenance factors) and those that lead to acceptable or enhanced performance on the job (performance factors; Guzzo, 1988).

Another challenge relates to the self-perception of people hired in this field. Higher levels of pay will possibly make up for poor working conditions, but do not enhance the cognition of the perceived low status of the job or organization. Improved training techniques will greatly improve this aspect. Even the weekly access to "intelligence" briefings on the assessed threat by qualified personnel will improve job satisfaction. People who believe they are actually important and contributing to combating a real threat will often live up to the challenge. Those employees referred to as "rent-a-cops" will not.

The use of trace detection technologies and explosive detection systems will also require specialized training. Trace detection equipment requires the use of specific protocols to be effective. Additionally, passenger screening settings may involve person-to-person contact or direct contact between the equipment and the passenger. Additionally, operators may feel *intimidated* by passengers. Training regarding the management of anger will also prove quite useful. To facilitate training of screeners, the FAA had been deploying a computerized training system called Screener Proficiency Evaluation and Reporting System, or SPEARS. One unique aspect of the system is a concept known as threat image projection (TIP), which consists of specific software to project fictitious images of bags with threat devices on x-ray screens to keep screeners alert and measure performance in real-time conditions. The government will likely continue the use of these systems.

It is also important to recognize the distinction between state-appointed law enforcement officers and "private" security officers. There are four basic differences. The significant distinctions include financial sourcing, profit orientation, goals toward crime prevention versus protection of assets, and the possession of statutory authority. Private security is employed by profit-oriented businesses. The police are statutorily appointed or sworn- into the service of the public and are paid by governments. Additionally, police officers are often focused on the investigation of crime that has already taken place or is taking place. Private security officers are supposed to focus on crime prevention and the protection of assets belonging to the business. The functions are similar and do overlap, but the motivational differences are worthy of note. Additionally, it will be very interesting to see whether the courts categorize the new federal government paid employees as "state agents," hence triggering more stringent Fourth Amendment restrictions.

ERGONOMIC SOLUTIONS

One method of improving security at airports involves the study of ergonomics. The objective of ergonomics is to ensure compatibility between task requirements and the capabilities and limitations of the employee. First, management needs to discover better methods to recognize the performance of employees. Second, employees, especially those entrusted with the public's safety, should be provided with opportunities for a sense of job satisfaction and achievement. Those same employees are entitled to a work environment that gives them the opportunity to grow on the job, either through openings for promotion or education and training.

In the United States, airport security employees did not previously have the opportunity to advance beyond a supervisory role at a security checkpoint. With nowhere to go, and theoretically no means to improve themselves, there was little incentive to improve job skills or dedication levels. Government supervisors will need to realize that some form of recognition for superior performance and continuing service is appropriate. Individuals can be rewarded with bonuses, extra vacation days, or other ways the airlines or government consider feasible. Similar to flight attendants and pilots, providing them with the same air travel benefits is another option.

Additionally, the concept of ergonomics in system design should be considered by management to improve the working conditions at security checkpoints. The goal of system design is to ensure that functions assigned to humans are compatible with human capabilities. If not, assigned functions will not be performed well, even if the best personnel selection, training, and motivation approaches are employed. In airports, current systems for screening carry-on baggage continue to suffer from human factors, i.e., pressure to keep passengers moving. Problems proliferate.

- The monitors on both x-ray machines and explosive detection equipment do not provide the operator with adequate size reference.
- Equipment controls are insufficiently distinguishable by shape and location coding to permit operation without looking at the control panel.
- Data integration and image processing techniques have not been sufficiently exploited to provide enhancements for image interpretation.
- Equipment design forces operators to position themselves improperly to view the display.
- Work-force constraints limit the ability of management to assign security personnel to tasks in accordance with their abilities.
- Passengers, airport staff, air carrier employees, and others sometimes subject security personnel to abuse (Airline Passenger Security Screening, 1996, pg. 26).

POTENTIAL OPERATOR CONCERNS WITH SPECIFIC SCREENING TECHNOLOGIES

For imaging technologies, alarm resolution probably will involve either taking additional images or having a more experienced viewer or supervisor interpret the initial image.

Studies have revealed the need for three approaches (Airline Passenger Security Screening, 1996, pg. 27):

1. Develop and apply selection methods to ensure that operators have the necessary aptitudes for the tasks to be performed;
2. Develop and administer training systems that provide operators with the needed knowledge and skills;
3. Incorporate elements into the system that enhance rather than degrade operator motivation and job satisfaction.

MEASURING OPERATOR PERFORMANCE

The government will have to adapt means by which to test whether dangerous objects, weapons and explosives are actually being detected. Such techniques include provisions for electronically inserting target objects on operational screening systems and a renewed focus on a human factors program. In June 1990, EG&G Astrophysics introduced a new function for its Linescan x-Ray™ baggage screening system. The new concept was called the False Image Protection (FIP) program. It was developed to not only test the alertness of operators but also can be used as a training device

to teach specific threat identification techniques to operators. The system gave the airport security supervisor the ability to activate the FIP, randomly, and to superimpose a false threat object on the monitor screen of an operator. If the operator was alert and recognized the threat object, he or she would have to verify so by pressing an indicator on the control panel. The successful or unsuccessful test could be recorded for later auditing purposes and also as proof that continuing training was taking place. They are a common feature today and are used on a regular basis; however it should be noted that TIP in such systems as the *Linescan 237*™ continue to be optional features. They should be made standard on all x-ray machines.

The documentation of individual screener testing is essential to avoid allegations of negligence. Management can protect itself by documenting adequate training has occurred. However, training adults should be distinguished from educating children. Overall, there are four fundamental tenets of adult education (Goodboe, 1995):

- Adults prefer to be self-directed, rather than instructor directed.
- Adults have unique life experience that they bring with them to the learning process.
- Adult readiness to learn is linked to what adults consider relevant.
- Adults want an immediate application of knowledge rather than the postponed application indicative of youth learning.

Cycles of training will provide security personnel with the best means of continuing education. They need some instruction in all of the following areas on a recurrent and documented basis:

- Proper screening procedures; especially on new technologies
- The threat to their specific airport
- Emergency medical procedures
- Anger management and conflict resolution
- Liability issues
- Performance appraisals for themselves and those they supervise

OPERATOR SELECTION

Historically, there were firms that maintained a rigorous screening hiring process. For example, the Guardsman Company had a 24-page application that demanded a plethora of information including residency verification. The hiring process also required interviewing neighbors and former employers. Some applicants were polygraphed, and all underwent drug screening. Guardsman's human resources personnel have confirmed that usually only 2 of 100 applicants survived the process. If you were a successful applicant, however, the job benefits included an hourly wage of approximately $16 per hour in the year 1994 as opposed to the average pay of $5.75 an hour prior to September 2001 at most other companies.

Since the U.S. government has decided to be directly responsible for the hiring and training of airport screeners, NCS Pearson, Inc., a Minnesota corporation, was selected to assist in developing a selection process. NCS won the $103.4 million contract to develop an Internet-based system to collect applications, establish hiring standards, and oversee testing of the candidates. The firm markets the famous Minnesota Multiple Personality Inventory test and others to detect unstable or dangerous attitudes and personality traits. Potential screeners are subjected to a number of tests. First, the Minnesota Multiphasic Personality Inventory 2 test can identify individuals who may be emotionally unsuited for demanding public safety roles. A second test tasks applicants to compare abstract traits and colors to identify cognitive ability. A third test measures 16 personality factors: "warmth, reasoning ability, emotional stability, dominance, liveliness, rule consciousness, boldness, sensitivity, distrust, abstractness, privateness, worrying, openness to change, self-reliance, perfectionism,

and tension. The process was eventually successful in screening the screeners before they took over security responsibilities at almost 500 airports on 14 November 2002.

To avoid the nonproductive cycle of high turnover rates and inefficient performance, it is essential to initially hire qualified personnel. Generally, if people are treated well, paid appropriately, and provided clear standards and expectations, they will identify with the workplace and perform better. In conjunction with the initial screening process, one of the first steps will be to recruit security officer candidates that are reliable, have some personal pride, and are orientated toward attention to detail. All information contained in an applicant's application form should be verified. Obtaining records waivers is a good idea so that the employer can note any problems at a previous place of employment. Because security officers are invested with quite a bit of trust, they should also be trustworthy. Current law does not authorize the dissemination of arrest and nonconviction data, but it is legal to authorize the release of conviction data. Therefore, criminal background checks are essential.

In addition, the TSA has set down some specific guidelines in Section 108.31 Employment Standards for Screening Personnel. They mandate the following:

Educational background: FAR 108.31 (a) (1) requires that screeners possess a high school diploma, a General Equivalency Diploma, or a combination of education and experience that the certificate holder has determined to have equipped the person to perform the duties of the position. Exactly what the last sentence means is open to interpretation.

Criminal background checks: FAR 108.33 (c) (5) does not require criminal records checks for every screener applicant, only those applicants who have specific deficiencies in their employment history, if there are other deficiencies in the application, or if the air carrier finds out that the applicant may have been convicted of certain kinds of crimes. Federal Bureaou of Investigation (FBI) records are reviewed, but this raises the question concerning non-U.S. citizen screeners and foreign criminal records.

Criminal history: FAR 108.33(2) states that a criminal records check must not disclose that the applicant has been convicted, or found not guilty by reason of insanity, in any jurisdiction during the previous ten years of a number of crimes such as aircraft piracy, interference with a flight crew or cabin member, assault with intent to murder, rape or aggravated sexual abuse, armed robbery, sedition, treason, extortion, or distribution of a controlled substance. Consequently, with a conviction older than ten years, the convicted felon meets the criteria of an airport screener.

Transportation Security Administration criteria: These individuals have taken over the screening at 415 of the 429 of the nation's commercial airports.

Level One Screeners are trainee screeners who must attend and pass both classroom and on-the-job security screener training administered by the TSA. They will conduct screening of passengers, baggage, and cargo under the close supervision of a Federal Civil Aviation Screening supervisor. These screeners must progress to Level Two or have their employment terminated.

Level Two Screeners are fully trained and certified screeners. They will conduct screening of passengers, baggage, and cargo. They have completed all training and certification requirements and have been on the job for over a year.

Level Three Screeners are fully trained and certified advanced screeners. They have been on the job in a Level Two capacity for over a year. They are also certified to use specialized explosives detection equipment to screen checked baggage and cargo.

Manager Level One Screening Supervisors are first-level supervisors of screeners who will provide direct day-to-day supervision of Level One, Two, and Three screeners.

Manager Level Two Supervisors supervise the Manager Level One managers and their subordinates.

TOUGHER THAN THEY THOUGHT

Initially, over 4000 people applied for 600 federal airport screening jobs at Baltimore Washington International Airport. The new TSA promptly removed the job application from the Web site. Soon thereafter, however, hundreds of applicants either failed the government's new test or did not even show up to take them. BWI, starting 1 May 2002, was the first airport in the nation to have federal workers manning the airport screening checkpoints. Starting pay ranged from $23,000 per year to $35,000 including paid leave, health benefits, and retirement benefits. Federal officials have estimated that they needed to hire approximately 65,000 security employees (approximately 30,000 screeners) to man the nation's entire network of airports. By the end of July 2002, only about 5000 had been filled. In the New York City area, by mid-July only 368 people had accepted the job offer where 2300 were needed (Associated Press, 2002).

Airports are now fully manned. However, former U.S. counterterrorism czar Richard Clarke has said he fears the government and public are falling into a false sense of complacency about security needs while Iraq had become a new breeding ground for terrorism against the United States. He also objected to the use of private screening companies, saying the creation of the TSA represented "the one great thing that we have done since 9/11 to increase security" and "an example of how the government can work" (Internet: http://www.govexec.com/dailyfed/ 0505/052605c1.htmr.) To encourage applicants to the TSA they now advertise the following *(http://www.tsa.gov/join/careers/)*:

> Our work is more than simply screening travelers. A wide range of challenging opportunities exists throughout our agency - just waiting for you to apply. From law enforcement to technology and from security operations to management, we are looking for dedicated people with the skills and desire to join us.

As stated, applicants are being screened by NCS Pearson, a private Minnesota company. The tests include such functions as placing a hand inside a bag and recognizing by touch the contents. For another test, the applicant must watch an x-ray screen and identify guns and knives superimposed on top of regular luggage contents, like toiletries and clothes. To test fitness, applicants must lift boxes of various weights and walk around some cones. The failure rate has been unexpectedly high.

The Department of Transportation also awarded a Phase II contract to Lockheed Martin Corporation's Mission Systems unit. Lockheed worked on airport passenger lane reconfiguration and the addition of new security technologies. The company received the $350 million base contract in June 2002, with additional work boosting the value to $490 million. Lockheed implemented a master schedule by 31 October 2002 to integrate federal employees into the system by November 2002. The same firm was awarded a contract valued at $105 million to train approximately 30,000 new screeners. Each screener was trained in the classroom for at least 40 hours and on the job at least an additional 60 hours. Generally, each screener had to be a U.S. citizen, have a high school degree, and be proficient in English. The requirement of a high school education was relaxed very quickly to also permit those with an equivalent one-year of work as an airport screener or other security job. The TSA had also discarded the hopes of filling half the positions with women. They readjusted the figure to one-third.

There had been some concern that the job could be accomplished in time. The TSA had planned to take over security at 15 of the nation's major airports by 1 June, but initially had only succeeded in partially taking over responsibilities at three. Federal employees first staffed the Mobile, AL, Louisville, KY, and Baltimore Washington International airports. As stated, government officials announced they met the Congressional deadline of 19 November 2002. They relied heavily on both Boeing Co. and Lockheed Martin Corporation to devise a way to get these federal screeners into the airports. Hundreds of employees from these two companies evaluated what needed to be done. Lockheed Martin deployed 146 teams, evaluating approximately 150,000 tasks necessary to set up passenger checkpoints. Program manager Tim Bradley had indicated at the time that they

would be hiring 15,000 to 20,000 federal screeners per month. Speeding up the process depended on cooperation between a significant numbers of people. Test programs were also conducted at five airports to determine whether private companies could meet federal requirements for screening: San Francisco; Kansas City; Rochester, NY; Tupelo, MS; and Jackson Hole, WY.

THE OPT OUT PROGRAM

The Aviation and Transportation Security Act (ATSA) also mandated a program to allow private contractors the ability to perform screening at airports in the future. As a precursor to the directive, a pilot program (PP5) allowed five airports, of different size and geographic region, to remain with a private screening workforce. This pilot program was intended to be used to evaluate future possibilities in passenger screening. The law required that screening at participating airports would be performed by employees of qualified private screening companies with oversight from federal authorities, and that those contract screeners would meet all the same requirements applicable to federal screeners (S. Res. 1447, 2001). With the relative success of the pilot program, the creation of the screening partnership program (SPP), went into effect after the sunset clause in the ATSA passed, allowing nonfederal screeners to operate again in U.S. airports. The SPP guidelines now govern these operations.

As mentioned, private companies involved in the pilot program function under TSA supervision and hire personnel using the same guidelines TSA uses for its own screeners. TSA provides the training for all private screeners, and they are supposed to be held to the same standards and mandates of the federal screeners. The airports selected for participation in the original PP5 included San Francisco International Airport, Kansas City International Airport, Greater Rochester International (NY) Airport, Jackson Hole Airport, and Tupelo Regional Airport.

Currently, the TSA operates six airports under the SPP, hence only one additional airport has been added to the list of airports that participated in the original pilot program, PP5. Considering the effort by Congress to ensure private contractors had the option to perform screening, the question posed is whether the TSA has in fact established a viable program to which airports will want to participate. It is clear that many airport managers and directors remain either uninformed or misinformed with regard to the overall program, thus resulting in little interest in the application process. Additionally, mangers are deeply concerned about liability issues, financial responsibility, continued federal funding of the program, and lack of incentives for participating airports. The federal government has spent millions to fund the initial PP5 and the now operational SPP, and it is worthy of support and further attention in terms of cost-benefit analysis.

Approximately a year after the inception of the PP5, BearingPoint, a private assessment firm under the direction of the TSA, began an evaluation of the performance level of the PP5 participants. Utilizing the existing data, BearingPoint was able to categorize the PP5 airports performance into three general categories:

- Security effectiveness: In quantifying and comparing security effectiveness, the independent evaluation team used four criteria to measure screener effectiveness: (1) screeners' performance in covert testing conducting by TSA, DHS, and the GAO, (2) screeners' response to images displayed by the Threat Imaging Projection System, (3) screeners' use of secondary searches to assess the effectiveness of initial searches at some airports, and (4) screeners' performance on a subset of recertification tests.
- Cost: In conducting cost comparisons, the evaluation team determined how much TSA spent for screening operations at each of the five pilot airports (which included not only contract payments, but also costs borne by TSA) and compared the results with estimates of how much TSA would have spent had it actually conducted the screening operations at those airports.

- Customer service and stakeholder impact: The evaluation team compared survey data on passengers' expressed satisfaction with screening operations, passenger wait times, and the level of complaints and compliments submitted by passengers. The independent evaluation found that the performance of the PP5 airport contract screeners, as structured under TSA's pilot program, is comparable to federal airport screeners.

Specifically, the report's findings in the three critical areas were as follows (BearingPoint, 2004):

- Security effectiveness: There is no evidence that any of the PP5 airports performed below the level of federal airports.
- Cost: The cost to perform the screening function at the five airports was similar to the estimated cost of federally conducted security operations at that same airport.
- Customer service and stakeholder impact: Data indicated that customer satisfaction at the Category X and I airports was mixed. For the other airports, there was insufficient data to draw any conclusions. However, a qualitative survey of stakeholders revealed no significant difference between privately and federally screened airports.

This encouraging evaluation of the participants permitted TSA officials to continue the PP5 pilot program. It is currently referred to as the "opt-out" program. In 2004, TSA provided information and program guidelines to all airport operators. This measure was designed to provide interested airports with the necessary information to make a qualified decision as to whether to opt out or not. The details of the report allowed airport operators to evaluate the results of the PP5 and to consider the possibility of returning screening to the private sector as allowed by law (GAO 03-1173). The guidance did not limit the number of airports that could submit applications. Funding for the program is supported from the same pool as the subsidy for federal screening operations nationwide.

In summary, the SPP gave airport operators the option of using private screening with TSA oversight. The operational experience learned from the PP5 program outlined a cost-effective, seamless transition to an SPP environment. It has worked so well that the five airports originally selected have renewed the respective contracts for private screening. The trend seems supported by the data. The system works, and screening contractors have expressed interest in expanding operations further to include additional airports. For example, Covenant Aviation Security has been renewed at San Francisco International Airport (SFO). This major international airport has effectively used the relationship developed with Covenant Aviation Security to collaborate on the installation and use of a closed circuit television system to monitor security lines, and the rotation of screeners to minimize wait times (Goo, 2004).

When Congress ordered a review of the PP5 program, the GAO found that a positive side effect of having private contractors in place was their capability to positively react when passenger wait times surged and to quickly bring that back to acceptable standards (GAO-04-055T). To date, Firstline provides screening for Kansas City International Airport; McNeil serves Rochester International Airport,; Tupelo uses Trinity Technologies Group, Inc.; and Jackson Hole formed their own company, Jackson Hole Airport Board. Although TSA opened its application window in late 2004, as of early 2005 the opt-out program had only two additional airports apply, Elko NV and Sioux Falls, SD. "However, after discussions with TSA officials, Elko Regional Airport submitted a letter to the TSA dated September 30, 2005, seeking to withdraw its application on the grounds that the City of Elko could not qualify as a private screening company. (GAO-06-166). In February 2006, Sioux Falls became the first new airport active in the SPP when Covenant Aviation Security assumed passenger and baggage screening operations (www.tsa.gov).

As stated on the TSA website, they have received several formal requests for participation in the SPP. On 22 December 2006, Key West International Airport and Florida Keys Marathon Airport applied, and on 2 February 2007, an additional request for participation in the program was received from the management at the Charles Schulz Sonoma County Airport. TSA has accepted

both applications and requests for proposal (RFPs) have been issued in both instances. The contractors will be selected by TSA from those that responded to the RFP. This activity has doubled the total applications TSA has received since opening the SPP. Industry sources have stated that up to 40 airports were anticipated to apply when the program was initially opened (Goodwin, 2004). In reality, most airline passengers are oblivious to the type of uniform worn by the actual individual performing the security screening. However, the following has become clear:

> "There is no doubt that private screeners are performing statistically better and are more cost effective than TSA screeners," said Congressman John L. Mica (R-FL) during his welcome to participants of NASCO's Contract Security Summit on 17 May in Washington, D.C. "Government, TSA, should set policy, define roles and responsibilities, conduct oversight, and let private security perform the screening." (Sikorski, 2006)

Remaining liability issues still present a troubling topic for all airport authorities, even those with a federal screening workforce. Eventually liability will be decided by the courts based on the individual merits of each case and current case precedent. The only high-profile case pending illustrates the reason for concern. Even though, pre-11 September, the FAA was responsible for the safety and security of the aircraft and the passenger screening was the responsibility of the individual airlines, Logan International Airport has been named as a defendant in the civil lawsuit filed on behalf of the deceased passengers. The Support Anti-Terrorism by Fostering Effective Technologies Act, or SAFETY Act, was enacted as part of the Homeland Security Act of 1002 (Title VIII, Subtitle G). The Act creates certain liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism…" (www.safetyact.gov), and has attempted to limit the liability for developers of new technology. The Act provides important legal liability protections for providers of "Qualified Anti-Terrorism Technologies," whether they are products or services. The goal of the SAFETY Act is to encourage the development and deployment of new and innovative antiterrorism products and services. However, the courts have yet to decide if the SAFETY Act's language and definition of "qualified antiterrorism technologies" applies to private screening contractors or even federal screeners (Goodwin, 2004). It was believed that federal standardization would serve as a basis to evaluate the performance level of the private contractors, thus making them eligible for the higher-level protection, albeit that level of liability has not yet been determined (Strohm, 2004). With Congress reconsidering the viability of maintaining federal screeners, this program deserves more attention.

CONCLUSION

This chapter has highlighted some of the major historical problem areas confronting airport screeners and airport passenger screening in general. Some recommendations were made on how to correct some of the deficiencies in current airport procedures and the hiring and training of security personnel. Hopefully, the attention span of the American public will remain focused on the need to adequately compensate and train airport screeners and security personnel in general. Means of measuring the performance of the screeners and how to enhance that performance were also discussed. Such tools as Threat Imaging Projections and SPEARS will continue to be critical to monitoring the performance of operators and need to be standardized globally.

It remains to be seen if government control of airport screening will improve the process. In April 2002, the U.S. government held a boot camp for the nation's new top airport security chiefs at Baltimore Washington International Airport. They were stressing customer service as well as security. These top security officials need all the security training they can get; especially those with little to no prior private airport security experience. Certainly, if they do not recognize the issues discussed above, they are destined to make the same mistakes as former private security screening companies. Hopefully, they will implement appropriate procedures to avoid many of the potential pitfalls. Additionally, the decision to make airport screeners federal employees will tantalize the

radar level of civil libertarians who will surely argue that the screeners are now state agents and hence answerable to the Fourth Amendment. The courts will ultimately have to determine future issues regarding the reasonableness of searches by federal employees. Further attention also needs to be given to the success of the opt-out program. Certainly, its cost effectiveness and accomplishments warrant supplementary review.

REFERENCES

Airline Passenger Security Screening, Chapter 5, National Research Council, Publication NMAB-482-1 National Academy Press, Washington, D.C., 1996, pg. 26.

Associated Press, 29 July 2002.

Bearing Point, 2004, April, Private Screening Operations Performance evaluation report. Retrieved 7 Nov 2006 from www.tsa.gov/assets/pdf/Summary_Report.pdf.

ERRI Daily Intelligence Report, Risk Assessment Services, 16 August 1997, Vol. 3, Pg. 228.

Goo, S.K., 2004, July, "Airport screeners' new guard: Private security firms want to replace government in 2005." Retrieved 10 April 2007 from www.washingtonpost.com.

Goodboe, Michael E., "Should Security Practice Andragogy?" *Security Management*, April 1995, pg. 65.

Goodwin, J., 2004, December, "Will U. S. airports convert to command screeners?" Retrieved 7 Nov 2006 from http://www.gsnmagazine.com/dec04/US_airports.html.

Guzzo, R.A., 1988. *Productivity in Organizations*, Jassey-Bass: San Francisco, CA.

http://www.apbnews.com /newscenter/ breakingnews/2000 /10/23/airport1023-01, "Airport Security Co. Fined $1.5 Million."

http://www.govexec.com/dailyfed/ 0505/052605c1.htmr.

http://www.securitymanage ment.com/library /000855.html, Screeners Under Fire, *SMO News and Trends*, May 2000.

http://www.tsa.gov/join/careers/.

www.safetyact.gov.

www.tsa.gov.

Morris, Jim, "Since Pan Am 103, a Façade of Security," *U.S. News*, 19 February 2001, http://www.usnews.com/usnews/issue/010219/safety.htm, pp. 1-3.

Poole, R., 2005, "What happened to airport screening opt-out?" Retrieved 31 March 2007 from www.rppi.org/security.

Rochelle, Carl, "FAA Calls for Security Improvements at US Airports," http://www.cnn.ru/2000/travel-news/01/07/bomb and baggage, 7 Jan 2000.

Sikorski, J., 2006, Private contractors continue to outperform TSA, Security Executive, Vol 1, No. 1. Retrieved 10 Apr 2007 from http://www.securityexecutive.org/downloads/junejuly2006.pdf.

Strohm, C. 2004, November, "Airport security contractors want government protection against lawsuits." Retrieved 10 Apr 2007 from http://www.govexec.com/dailyted/1104/111804cl.htm.

9 Metal Detectors, X-Ray Inspection, Explosive Detection, and Trace Detection Devices

Will the Public Tolerate the Intrusion?

NEWS

7 March 2001: The Aviation Security Manufacturing Coalition announced it has the technology needed to help major manufacturers *Invision*™ and *L-3* make and test the more than 2000 screening machines that are needed. Later, *Invision*™ Technologies publicizes that the FAA has given *Invision*™ a delivery order of approximately $9 million for the company's CTX 9000 Dsi™ and CTX 2500™ explosive detection systems.

24 September 2001: Secretary of Defense Donald Rumsfeld announces that the United States is taking seriously the potentiality that terrorists might use biological or chemical weapons.

7 June 2002: The Department of Transportation awards Boeing Co. a contract valued at up to $1.37 billion to provide explosive detection machines at U.S. airports.

30 June 2002: The Chisholm-Hibbing Airport in Minnesota will be the first airport in the nation to receive a new type of technology to detect explosives and narcotics. The *Itemiser*™ system can simultaneously monitor positive and negative ion modes for all substances.

July 2005: Ten new explosives-detection canine teams join the Transporation Security Administration's National Explosives-Detection Canine Team Program following graduation at Lackland Air Force Base in San Antonio, TX. The canine teams are being assigned to airports in San Francisco; Miami; Boston; Los Angeles; Indianapolis; Cincinnati; Nashville, TN; El Paso, TX; Tampa, FL; and Washington, D.C.

INTRODUCTION

The screening of passengers and baggage is now a routine part of air travel. Travelers automatically factor into their travel plans the necessary time to "clear security" before arriving at the aircraft gate. The government is adjusting to the requirement to provide such security services. The government also intends to pass on the fee for screening passengers and carry-on baggage as another cost of doing business, which is eventually passed onto the traveler in the price of a ticket. Airport planners redesigning existing airports and drafting the plans for new ones, currently automatically

reserve sufficient space at all airport facilities for adequate security arrangements. Advances in technology have supported the efforts of security and law enforcement. Research and development endeavors have improved the quality and available choices of screening equipment available for purchase. New x-ray devices for carry-on baggage and new metal detectors, both portal-type and hand-held, have revolutionized the ability of scanners to quickly and easily determine if an individual is carrying any unauthorized dangerous weapons. Furthermore, advances have been made in the production of explosive detection and trace detection devices with quadruple resonance devices and others on the horizon.

The equipment and the personnel have improved over the years. The latest controversy revolves around Explosive Detection and Trace Detection systems. Congress originally intended for the Transportation Security Administration (TSA) to buy thousands of explosive detection systems to be installed from 2007 through 2014. After 11 September, they shortened the deadline to 31 December 2002. Soon thereafter, and again similar to what has happened in the 1970s, the Department of Transportation concluded that it could not acquire and install enough machines within the required deadline. Subsequently, the government declared trace detection equipment a reasonable alternative. This chapter will attempt to provide an historical perspective on some of the initial problems and supporting equipment and how they have developed and improved over the years. The changes in improved and more-intrusive equipment will continue to affect everyone involved.

METAL DETECTORS

"Often domestic passengers are only required to pass through a simple metal detector before being allowed aboard an aircraft. Such rudimentary security measures have been shown time and again to be less than effective, but still they are used as the first and sometimes only line of defense against a determined hijacker," says Chris Yates, Editor Jane's Airport Security Standards and Technology (Internet:http://www.james.com/press/pc990723.shtml). Such comments are reflective of easily recognizable deficiencies of many current metal detectors. They simply do not catch all forms of dangerous weapons. More often, their greatest weakness is cited as not detecting metals incapable of being magnetized. Because a significant number of U.S. manufactured guns are made of mostly nonferrous metals, the shortfall is quite evident. Even though no such thing as a totally plastic gun exists, if the sensitivity setting on the detector is not set properly, some guns may remain undetected. The lightest guns with polymer grips, bodies, and slides normally have enough metal in them to trigger the detector, but they still require special scrutiny.

The detectors also cannot detect the organic materials contained in explosives. Metal detectors remain one of the most important sources of security for airports. There have been significant advances in equipment, which include software programs that can suppress ferrous detection while boosting nonferrous metals. Others suppress nonferrous materials while magnifying the detection response of ferrous objects. Newer trace detection equipment is also able to recognize organic explosive materials. However, most new technology comes with a rather high price tag. Regardless, the U.S. government mandated their use by December 2002.

The scientific principle on which metal detectors work is quite simple. The first airport screening device used, magnetometers, began as a retrofit from the machinery used in the logging industry to prevent nails (metal) from severely damaging the saws (Wu, 2005). Passive systems detect metal by changes in the earth's magnetic field. Active detectors operate by creating their own electromagnetic field and setting off an alarm when metal objects passing through it disturb the field. Metal detectors contain one or more inductor coils that are used to interact with metallic elements on the ground. A pulsating current is applied to an internal coil, which induces a magnetic field. When the magnetic field of the coil moves across metal, the field induces electric currents called eddy currents. The eddy currents induce their own magnetic field, which generates an opposite reaction in the coil, thereby inducing a signal indicating the presence of metal ("How a Metal Detector Works," 2001).

Active detectors use various frequencies usually 90 Hz to 25 KHz. Hand-held units usually utilize the bands from 100 KHz to 1 MHz. Metals such as aluminum, brass, and copper are highly conductive and, hence, provide greater signals at higher frequencies. Metals such as iron and steel produce greater signals at low frequencies. High-frequency detectors, which react to highly conductive metal, are more prone to false alarms. Low-frequency detectors, which react to less conductive metals, can disregard small metal objects; low-frequency detectors (below 500Hz) are more practical for walk-through screening.

SELECTING A METAL DETECTOR

The selection of an appropriate metal detector is an important decision. Each airport has its own unique characteristics and priorities. Various factors must be weighed and considered (see Figure 9.1). Unfortunately, one of the primary limitations is usually cost, and metal detectors are expensive assets that need to be maintained and routinely upgraded. Additionally, accuracy and utility are weighty considerations. The rapid flow of passengers is of major concern to airlines seeking to keep their balance sheets on the positive side of the ledger. To keep on making money, the airlines attempted to keep the passenger relatively agreeable to the delays caused by screening 100 percent of terminal traffic. Equipment causing too many false alarms, breaking down on a repeated basis, or otherwise causing delays was not marketable in this venue. Federal employees need not directly succumb to those pressures.

To satisfy market demand, many companies have been through eight or nine successive generations of equipment. Improvements have featured increased levels of security performance in metal detection capability, discrimination of personal metal objects, and immunity to outside interference. Safety precautions regarding the passenger with a life support device have also been tested and retested to protect the operator and manufacturer from prohibitive civil liability.

The calibration of metal detectors is somewhat a matter of preference, but all the metal detectors allocated to commercial airports are calibrated by the manufacturer according to TSA specifications. Texans with large belt buckles may require a certain level of detection different from an airport in the Bahamas. Sensitivity formerly recommended by the Federal Aviation Authority (FAA) called for a maximum false alarm rate of 15 percent. The ideal metal detector should detect a gun without fail while passing a person with an ordinary amount of pocket items and jewelry. Regardless, passengers are usually required to empty their pockets of any metal objects so that the equipment can be calibrated at the most effective settings. Newer procedures scan for even the smallest amount of metal.

Another determining factor in purchasing criteria is the mobility of the equipment. Many units are now permanent fixtures, but moving them is still necessary on occasion. Consequently, the cost of recalibrating them, the time involved, and the ease of doing so are all important considerations. If an engineer is obligatory, the cost and time involved increase. Furthermore, the TSA requires that they must recertify the capability of the device if it has been moved. The recalibration of TSA metal detectors, if required, is the responsibility of the checkpoint supervisors.

Of course, the bottom line for each metal detector is whether it actually accurately detects guns and weapons. The actual detection rates are not published for security reasons. Suffice it to say they must possess a high detection rate. Today's hardware and software programs improve their interference rejection, discrimination, sensitivity, detection, uniformity, vibration tolerance, and orientation responses. All these factors contribute to the bottom line that increased discrimination significantly reduces unwarranted alarms. Many metal detector manufacturers now also sell enhancement programs that help correct detection nonuniformity caused by vertically positioned external metal. Other programs allow the user to create customized security programs.

The manager circumnavigating the hundreds of pages of marketing materials on metal detectors still has to consider some basic concepts in determining the most appropriate system. Overall, managers need to contemplate such issues as external factors or sensitivity to environmental

FIGURE 9.1 Rapiscan's Metor 300 EMD was designed to speed up the security check process. It offers superior performance for demanding checkpoint applications in aviation and other security environments. (Photo courtesy of Rapiscan Systems)

factors (i.e., environmental magnetic noise), physical construction or size, ease of operation (i.e., ease of calibration, self-calibration, and required frequency of calibration), and last but not least cost and appearance.

Additionally, development has produced machines that now have a multizone advantage. In addition to indicating the location of targeted objects, multizone systems possess a multitude of advantages. They improve discrimination between weapons and harmless objects, reduce unwanted alarms, and permit higher traffic flow rates. In high-volume airports this translates into lower operating and capital costs. For example, pinpoint multizone detection is a concept currently utilized. One manufacturer uses a "block of real estate" example to explain the dynamics of the system. They explain that in "most detectors the blocks of real estate, called zones, are stacked up on each other and extend the full width of the archway. When an object passes through a zone, it is detected by the zone, and an alarm display shows its location. In this case, the alarm display depicts the height of the object above ground. The display can take the form of lights on the front edge of a side panel or a mimic display that represents the archway in graphic form" (Defining Multi-Zone Detection: Check Apple for Apples, 2001). Manufacturers do place different interpretations on the meaning of multizone detection. Appropriately, when a device claims to have six horizontal zones, it should mean that there are 12 detection channels with two sensors per zone. Each zone should be independently adjustable.

False alarms can be attributable to external electrical and electromagnetic interference and poor tolerance vibration. Good-quality interference rejection and mechanical design will lower false alarms. Multizone detectors reduce unwanted alarms caused by people literally wearing metal; jewelry, coins, and keys. Two conditions contribute to elevated undesired alarm rates. They include the cumulative signal effect and nonuniform detection. Cumulative signal effect lowers a detector's ability to separate weapons from harmless personal effects. It occurs when signals generated are processed as a single composite signal. Theoretically, in single-zone machines, the signals from someone's watch, keys, and some metal in shoes will be combined. If the cumulative signal is large enough, the machine will set off an alarm, causing delay and frustration for passenger and screener alike.

Correspondingly in multizone detectors, if the device has 18 zone detectors, six horizontal zones would be divided into three blocks. The machine would then display the object's height above the ground and also show if the object was to the right or left or in the center of the zone. Complicated mapping algorithms process the data and can very accurately tell the scanner where the object is. Because each zone has an adjustable control, the sensitivity can be focused on a particular object for a better analysis, thereby making a threat assessment easier and reducing unwarranted alarms.

Additionally, nonuniform detection can be caused by rebar in the floor or in the wall of the airport. External metal can distort a detector's magnetic field and may cause a loss in detection. In essence, a dead spot is created. This anomaly can be corrected by raising the machine's overall sensitivity level. The simple fix becomes impractical if a floor is heavily reinforced. The level of sensitivity setting may become so high that a disproportionate number of other unwanted alarms may take place. Multizone machines permit hot spots and dead spots to be eliminated with a simple adjustment to the equipment.

Although adjustable zones compensate for detection losses caused by metal in the floor, walls, or ceiling, a different solution is needed to counteract metal positioned directly next to the machine. The presence of a steel girder, for example, causes deterioration in detection uniformity across the horizontal axis of the archway. Because it is not possible generally to reposition an imbedded steel girder, or to move the sterile concourse entrance, the machine will need horizontal axis adjustments. These advanced features are now readily available.

Another feature to consider before purchasing a specific piece of equipment is the information the screener receives from the alarm panel during an alarm. The alarm panel should show the height at which the detected object is carried. For example, more advertised zones are not necessarily better unless the numbers of horizontal sensitivity controls are present to adjust those zones.

This is arguably more important than the actual number of zones. This significantly cuts down on the time needed to actually locate a weapon if there is one. Furthermore, the equipment should be continuously active and have self-testing diagnostics and a fast automatic reset. Electrical and electromagnetic interference rejection can be achieved through multiple-frequency selection, electronic filtering, and sophisticated software algorithms.

HAND-HELD BODY SCANNERS

The best hand-held detectors are lightweight in construction and have a comfortable grip and a large scanning surface. The detector should have a tight detection pattern, fast detection circuitry, and be ergonomically designed. These attributes contribute to higher efficiency and reduced operator fatigue. Another really useful feature is a switch that can transform the detector from a general use mode to a super-high sensitivity unit capable of detecting very small masses of metal. (see Figure 9.2).

They should generally be able to detect a medium pistol at 12 inches (300 mm); a small pistol at 9 inches (230 mm); and a razor blade at 3 inches (25 mm) and should scan about 3 to 24 inches per second. They also need to be adjustable. For example, the controls should enable the scanner to lower the sensitivity to avoid unwanted alarms for small harmless objects like key chains. Currently, of course, passengers place all of their metal objects in their pockets inside a divesture bowl for x-ray screening, including common electronic devices such as cell phones, APA's, portable GPS receivers, CD players, etc. Sensitivity adjustments can be made through a screwdriver access hole in the handle. Most quality devices encase the circuitry in a rugged high-impact case, which should detect both ferrous and nonferrous metals and alloys. It should be capable of not sounding an alarm when the scanner is used to screen at ankle height and in the vicinity of rebars in the floor. At airports staffed by the TSA, the manufacturer calibrates the hand-held metal detector (HHMD) to optimal levels, as specified by the TSA, and no manual adjustments by screeners are required.

Alarms are both visual and audial. They should remain activated while the search coil is over a metal object. The duration of the alarm is usually indicative of the size of the object. Most use alkaline batteries as a power source, which should last at least 80 hours. Low-voltage conditions,

FIGURE 9.2 Hand-held metal detectors are an integral part of the physical security screening process for all applications. The design of the Rapiscan Metor 28 hand-held metal detector allows security staff to thoroughly scan an individual, while keeping their hands away from the individual's body. (Photo courtesy of Rapiscan Systems)

like cell phones, should advise the user that the power is low. The average weight is a pound or less. Visual-only alarm indications are advisable if a weapon is detected. The screener can simply ask the individual to step to the side for the moment, giving security personnel time to respond accordingly. An audio alarm alerts the perpetrator that they are "trapped," and they may respond accordingly.

TESTING

No more than 15 percent of the people who set off the alarm should be false alarms. In other words, no more than 15 unarmed passengers of 100 should set off the alarm. To test a particular machine, the FAA developed a gun kit that could be used to test metal detectors but in actuality involves a tedious process. The offensive object was placed in seven different positions and locations on the body, and the detector was required to alert appropriately. Because of the cumbersomeness of the process, some airport security officials have used such things as a block of metal, large wrenches, and pairs of pliers to achieve the same adequate test results. Regardless of what metal object is used, the machine must be tested weekly, if its use is continuous. If a piece of equipment fails the test, it should be replaced within 48 hours. At TSA manned airports, TSA checkpoint supervisors are supposed to conduct daily walk-through metal detector calibrations in accordance with standard operating procedures.

Additional improvements are considered necessary. The law enforcement community has requested improved detection performance, performance tests, and performance specifications for both walk-through and hand-held detectors. For advancements to be made, further research will be required to compile reliable data on the electromagnetic properties of weapons-grade metals from which to perform computer simulations of detector performance. The data on conductivity and permeability of many metals has yet to be fully researched.

METAL DETECTORS, COMPUTERS, AND PERSONAL MEDICAL DEVICES

Millions of travelers have been processed through metal detectors, and there has not been a single recorded incident of any damage to a computer, a diskette, or a CD. The allowable electromagnetic field permitted from a metal detector (1 Gauss) is about twice the earth's magnetic field you experience every minute of your life. Consequently, no metal detector is likely to damage a computer because exposure is only a few seconds, and the field is weak. However, it is not outside the realm of possibility that someone might seek to disguise a computer with an explosive device inside it. After the tragedy of Pan American Flight 103, the FAA even proposed that all small computers and other electronic devices be banned from aircraft. In today's working world, however, this was not considered a reasonable request by business travelers, journalists, and a host of others. Early fears that the use of computers on board might interfere with navigation devices have proved groundless. The FAA permits their use, except during take-off and landing procedures.

Personal medical devices (PMDs) are another story. Walk-through and hand-held metal detectors may affect some of the more sophisticated devices in medical use today. Walk-through and hand-held metal detectors might cause cardiac defibrillators, infusion devices, or spinal cord stimulators to malfunction. More research is required to develop and test an affordable magnetic field emulator so that the medical devices can more accurately be tested for interference from the metal detectors. The Food and Drug Administration (FDA) should assess interference thresholds and issue regulatory susceptibility standards for PMDs (Development of Systems to Evaluate Magnetic Fields Produced by Walk-Through and Hand Held Metal Detectors, 2001). Currently, the National Institute of Science and Technology, in collaboration with the FDA are working on more accurately evaluating the effects of metals detectors on PMDs, specifically regarding metal detector-induced failure or malfunction.

X-RAY INSPECTION UNITS

X-ray inspection units of carry-on luggage and of people all use the low dosage, low energy, or low radiation type. The x-rays are reflected from the subject to create an image. The newer emerging technologies can detect metallic and nonmetallic explosives and other contraband concealed under multiple layers of material. Modern imaging technologies either scan subjects for natural radiation emitted by a human body, called passive imaging, or expose objects to reflected radiation, called active imaging. In first-generation baggage screening units, low dosage units produced a weak image that had to be amplified on a closed circuit television to be adequately used. Many units operated on a short pulse equaling about 1/120th of a second. Some units kept the image on the screen in an image storage unit until the next image needed to be viewed. Others operated in a continuous emission mode. Both of these analog systems created poor contrast in comparison with the systems now available. Today, digital video storage enhances the ability to eliminate background radiation scatter, making the picture clearer. The newest technology uses either x-ray or millimeter wavelength electromagnetic radiation usually from a pulsed x-ray source. The entire system is digital, including the image transfer mechanism.*

PASSIVE MILLIMETER-WAVE IMAGING

This technology operates on the principle that any object not at absolute zero temperature emits electromagnetic energy at all wavelengths. These systems will operate in the millimeter wave range or near 100 gigahertz. Any energy should be detected by an appropriate receiver and can be mathematically manipulated to produce a visible image. The system gathers information from radiation naturally emitted from a human body. Regardless of how clear the image, an operator must be trained to distinguish any threatening objects from the natural clutter of nonthreatening objects.

The area of passive millimeter-wave imaging (PMMW) continues in development. However, in 2006, millimeter-wave technology researchers at Northrop-Grumman Space Technology announced advances made in a technology that enables small cameras to look through clothing and other inert materials to detect weapons or other contraband. PMMW technology can also see through heavy clouds to perform aerial surveillance on bad weather days. It potentially can provide a system that offers a lot of contrast. Although there are applications in which active millimeter-wave sensing may be more appropriate, passive sensing can avoid glint. Old equipment used to be quite bulky, but the new technology allows sensing from small integrated chips. In a military application it can penetrate fog, dust, smoke, and light rain, including military target acquisition and aircraft navigation. In a civilian aviation capacity, it could be used to enhance autonomous landing guidance systems under development that might aid pilots in landing during Category III conditions. Because of the penetration of millimeter-wave frequencies, imaging systems could also be used to fight fires by seeing through the smoke and for inland waterway navigation in foggy conditions. In the field of airport security, it can penetrate solids and is able to detect concealed weapons that are metal or plastic through as much as 0.5 inches of sheetrock (Carts-Powell, 2001).

Testing of millimeter-wave technology in airports began in Phoenix, AZ, PHX, in October 2007. The PHX system works as follows (Internet: http://www.tsa.gov/approach/tech/mwave.shtm):

- Beams of radio frequency (RF) energy in the millimeter-wave spectrum are projected over the body's surface at high speed from two antennas simultaneously as they rotate around the body.
- The RF energy reflected back from the body or other objects on the body is used to construct a three-dimensional image.

* *Note*: Energy, frequency, and wavelength are fundamentally related. Energy is inversely proportional to wavelength. Basically, long wavelength radiation is low energy and low frequency or short wavelength radiation is high energy and high frequency.

- The three-dimensional image of the body, with facial features blurred for privacy, is displayed on a remote monitor for analysis.

This system provides a voluntary alternative to a patdown during secondary screening. This technology can detect weapons, explosives, and other threat items concealed under layers of clothing without physical contact in a very short period of time. So far, when passengers have been presented with the choice of a patdown search or submitting to this technology, they have overwhelmingly chosen the millimeter-wave imaging systems.

ACTIVE MILLIMETER-WAVE IMAGING

Active millimeter-wave imaging technology functions as a short-range radar system that projects a narrow beam of millimeter wavelength energy against the object and detects the reflected rays. The beam starts at the bottom of an object or person and scans up or down and produces an image of the object or person. Millimeter-wave technology uses low energy, low intensity x-rays reflected from the subject to create an image. The screener must interpret the image to determine whether a metallic or nonmetallic weapon is present. The x-rays are actually reflected off the surface of the body. When a patient is x-rayed by a doctor, the process involves energy that is transmitted through the body; a completely different set of circumstances.

SELECTING AN X-RAY UNIT

There are multiple x-ray units available on the market. Selecting a suitable unit for a specific airport can require a great deal of research. Of primary consideration is the picture (imaging) quality and sensitivity of the machine. Previously, no system on the market produced an acute photographic quality image, but today's digital systems are quite good. No unit is totally effective unless the scanner can easily recognize threatening objects and quickly distinguish them from nonthreatening objects. Effectiveness, in turn, substantially depends on the machine's ability to deliver a clear picture. An operator's ability to clearly and accurately identify objects, which could be threatening, in a reasonable amount of time with reasonable precision, is critical to a successful security operation. In screening passengers and carry-on baggage, the equipment on the market seeks to give the screener six seconds to evaluate the image. A typical unit will be able to distinguish 36 American wire gauge (AWG) in air, 32 AWG behind 1/8th-inch thickness of steel, and. 0.2 AWG behind 3 mm of steel. They can have a total penetration of 15 mm of steel. (Portable Digital x-ray Imaging System-RTR-4, 2001).

Stored image units essentially store the image information produced on a display unit where it can be viewed for as long as several minutes. This furnishes the operator important time to conscientiously review the image at hand. At present, the use of digital memory devices is prolific and quite effective. In continuous beam units, the actual x-ray beam is activated throughout the time the object is being inspected, usually 3 to 6 seconds. A smear effect can also appear from an object's continuous movement along a conveyor belt, making the system less desirous than digital storage methods. Older systems had to be stopped so the screener could maintain a clear viewing image.

It must be remembered that not all airports have the latest technology instantly at their disposal. Much of the x-ray equipment in use today is several years old. Not too long ago, there had been reports that "guards are watching black, white, or snow-filled screens that would make any sort of real detection of weapons or explosives impossible." (Clark, 2001). A cynic might agree with highly underpaid and undereducated former contract guards when they quipped that the federal government requires that the bags and people be scanned, not that the guards are actually capable of detecting any dangerous items. Such attitudes are more widespread than expected. Congress did appropriate $100 million in fiscal year 1999 and $157 million in both 1997 and 1998 to continue deploying state-of-the-art security equipment to airports (Airport Security, 2001).

In the past it was also important to distinguish between those x-ray units that projected an x-ray horizontally and those that had the x-ray emanate from the top of the machine down vertically. If the machine projects horizontally across the viewing surface, some luggage, especially foldover bags, may be difficult to adequately scan. Newer L-shaped detector arrays provide 100 percent package screening. Most machines manufactured currently and used for checked luggage employ high speed x-rays. They send a computed axial tomography (CAT) scan-like beam through the luggage to get a "slice" image of anything it is programmed to examine.

Another issue for discussion is the speed at which the system works. The FAA had established the standard flow-through rate as no more than six seconds per item. This equated to about ten pieces of luggage per minute. Most machines will process carry-on baggage at a rate much faster than this; however, the training of the screener comes into significant play in this regard. If the screener just wants to process people and baggage, they can hurriedly and negligently process a lot of people quickly. Conveyor belt speeds on most pieces of equipment are adjustable, making this possibility often very tempting. Most machines have a conveyor speed of around 48 feet per minute at 60 Hz (14.4 meters per minute at 50 Hz). They are also reversible.

SIZERS

Other factors to consider when purchasing a particular piece of equipment include safety, mobility, ease of maintenance, and relative cost. At issue is also the inspection size capability of the system. Some manufacturers were providing airlines with multitask machines, which combine the x-ray screener function and the ability to "size" the luggage. Not only was the carry-on luggage x-rayed, but it was "sized" to see if it would fit into the overhead compartments on board the aircraft. If the particular piece of luggage was larger than 9 by 14 by 22 inches, it would not fit through the x-ray machine. The passenger was encouraged to return to the check-in counter with the bag, or the airline would have an airline employee or "skycap" takes control of the baggage right there at the security checkpoint. Unfortunately, not all the airlines were in agreement on the acceptable size of carry-on luggage.

When several airlines share the sterile concourse, problems can arise. For example, Continental Airlines prided itself on permitting its customers to carry on some rather large items. They are so committed to this marketing concept that they had sued Delta over the "sizer" issue in the San Diego airport. The lawsuit filed in a San Diego court alleged that sizing equipment had created traffic jams at the security checkpoint and forced some Continental customers to return to the check-in counter with bags. Vice-President of Airport Services for Continental said, "Continental customers should not be penalized by Delta's imposition of its unfriendly baggage policies" (Arrillage, 1998). Delta had installed Plexiglass cutouts in front of two x-ray security machines to make sure all bags were small enough to fit under the seat or in the overhead bins. The lawsuit sought an injunction and unspecified damages alleging interference with contractual rights and unfair competition. It was settled out of court. Continental had also sued United Airlines for similar procedures at Dulles International Airport, alleging the sizers interfere with security screening.

In September 2002, the TSA announced it intended to remove the plates, arguing that the templates slowed security. They did not state that it hindered the process. So far, the TSA has asked airlines to remove the plates but has not made it a formal requirement. The removal could delay takeoff times even further when passengers reach aircraft and luggage will not fit into the overhead compartment. Although it is arguable that they should remain in place, air carrier employees are often reluctant to enforce that provision of applicable security directives for fear of the upsetting passengers.

FILM AND LAPTOPS

Passengers are always inquiring whether the x-ray machine is film safe and computer safe. Some travelers continue to insist that the CAT-scan type beam from an x-ray machine will leave a bluish

stripe or line on unprocessed slide, print, or picture film. They claim the "line" remains after the film is developed. The effect of the much stronger x-ray machines used in scanning checked baggage makes this a distinct possibility. Some experts have advised travelers that the powerful x-ray and neutron tomography machines will destroy film. They further advise airline passengers that x-ray protection bags sold in camera stores are "absolutely useless" (x-ray Advice, 2001). Admittedly, the screener can just increase the beam on the bag until he or she can see through it. At least one manufacturer, SIMA, disputes this advice. They claim that FilmShield XPF™ bags protect film, withstanding multiple passes through high-dosage security equipment, even the CTX-5000™. (New Filmshield XPF Protects Film from High Dosage Airport Security Equipment, 2001). The best advice is to not check sensitive film.

Film in carry-on baggage would have to be repeatedly screened, up to as much as 10 times, to make any difference whatsoever. The average machine in use at today's airports is more likely to generate a dosage of only 0.1 mR. It should be recognized that not all low-dosage scanners are calibrated equally. As long ago as 1973, the Film Technical Services Division of Eastman Kodak found, "The results of our tests thus far have led us to the conclusion that a cumulative exposure not exceeding 5 milliroentgens (mR) would seldom cause a noticeable photographic effect, providing the exposure is made in increments not exceeding 1 mR and the orientation of the film luggage combination is changed between exposures" (Debenham, 1973).

However, much has changed from 1973. The Photographic and Imaging Manufacturers Association Inc. tested the CTX-5000SP. They concluded that "The CTX-5000SP will cause significant fogging of all color negative films with an ISO speed of 100 or higher when the film sustains a direct hit by the machine's high intensity x-ray beam" (Technical Report Confirms Film Damage, 2001). The FAA, now TSA, had already addressed the issue. They amended Part 108 on 24 September 1998 to post warnings to travelers. In general, even though some international airport signs still say, "This machine will not harm film" the more correct information is that, while a single low-power scan would not harm "slow" or "moderate" speed film (i.e., 400 ASA or less), the effects of x-ray exposure can be cumulative, and in the course of a journey you may end up giving your film half a dozen or more exposures, which will start to affect faster-speed film. Furthermore, explosive detection systems are now being used in U.S. airports and international airports to scan (x-ray) checked baggage. This stronger scanning equipment will fog any unprocessed film that passes through the scanner. However, x-rays from airport scanners do not affect digital camera images or film that has already been processed, i.e., film from which you have received prints, slides, CD disks, or picture CDs.

PASSENGER X-RAY SCREENING DEVICES

Since the initiation of screening procedures, x-ray imaging, microwave holography, and acoustic detection have all been tested as a means for detecting weapons and contraband hidden in and on a human body. Passenger imaging is an umbrella term used to describe technologies that visually screen travelers. The TSA is currently using two different types of passenger imaging technology: backscatter and millimeter wave. Some of this new technology has been considered quite intrusive by some individuals. American Science and Engineering Inc., located in Billerica, MA, now manufactures an x-ray machine that essentially sees through clothes. U.S. Customs officials had previously tested the devices at several major airports. The controversy has been immediate and vocal. The equipment initially was developed to have the capacity to specifically target drug smugglers. If a passenger was considered suspicious for some reason, they were given the option of submitting to a traditional patdown search or standing in front of the x-ray machine, which renders an image of the individual virtually naked. Obviously, the equipment has the capacity to be used to search for dangerous weapons as well.

The idea was to build a device less intrusive than the patdown search. As mentioned, U.S. Customs officials have been criticized for allegedly focusing too much on minority passengers.

This was originally seen as an alternative. Others have labeled it an electronic strip search that is extremely graphic. Some passengers, especially public figures, fear that dishonest security personnel might retain the images of them without clothes to sell them later for profit. For some people, the "naked" photo of a movie star or other celebrity might be worth the deceit of selling it for publication. The temptation to a poorly paid screener might be too great. Currently, the TSA states that the agency immediately deletes the raw images, but opponents insist there is no law or regulation that prevents the agency from saving the original, detailed images. The TSA also emphasizes that the passenger-imaging units have zero storage capability.

To avoid raising the specter of Fourth Amendment search and privacy issues, U.S. authorities were originally required to first obtain a signed consent form from the passenger, and the viewer was supposed to be of the same sex. These machines generate cartoon-like images of passengers, using a "privacy algorithm" that protects their privacy, according to the TSA. Screeners can still easily see metal objects, although it would be fairly easy then to defeat the scene behind the privacy-algorithm screen. These algorithms or privacy filters, however, arguably render the images now useless as a security device in that the blurring can make it difficult for screeners to see the weapons the equipment was supposed to illuminate. Additionally, the image is displayed on a remote monitor.

The advertised level of radiation is quite small, but pregnant women are not provided with this option to be on the safe side. Backscatter technology has been waiting on the sidelines for nearly four years but seems poised now to move to the forefront of the aviation security. As stated, the machines were already used by U.S. agents at 12 airports to screen passengers suspected of carrying drugs. They are also utilized at one of the terminals at London Heathrow Airport, the first major airport to use them to detect explosives and dangerous instrumentalities. The $100,000 machines bounce low-radiation x-rays off a person's skin. The technology produces photo-like computer images of metal, plastic, and organic materials hidden under clothes, explains American Science and Engineering, the manufacturer. The TSA is testing the BodySearch machine at its laboratory in Atlantic City as well.

PORTABLE DIGITAL X-RAY IMAGING SYSTEMS

Police are now using portable x-ray imaging systems to efficiently search for weapons or contraband in areas either too difficult or too time-consuming to search manually. The RTR-4 is one of the latest, and according to its manufacturer, only fully digital portable x-ray equipment available to EOD personnel. Americana Impex Consulting Co. manufactures the product that weighs approximately 15 pounds. It can be used to investigate suspicious packages, mail, and vehicles wherever they are located. It can also be mounted on bomb disposal robots, but it is fully operational in a stand-alone mode.

The unit could be carried onto any aircraft or used to inspect a cart full of baggage while sitting on the flight line. Because it is mobile, its applications could extend throughout an entire airport environment. This tool can enhance the safety margin for innocent passengers and air crews. It can be deployed to search the control tower and be quickly moved to a restroom where a bomb threat has been made. It is cost effective and should be considered a necessary tool at any major airport (Portable Digital x-ray Imaging System, Internet: http://www.americanaimpex. com/x-ray.htm, pp. 1-5).

TESTING X-RAY EQUIPMENT

The government requires that all x-ray units be tested daily. This responsibility falls onto the shoulders of the screening supervisor. A step wedge testing procedure is usually used. The American Society for Testing and Materials (ASTM) step wedge reduces in size through the procedure. Ultimately, each unit must detect the 24-gauge wire under the fifth step of the step wedge. The

original rationale was that the test would certify that each piece of equipment would be capable of detecting the smallest gauge of the common lead wire used for blasting in the majority of blasting caps. Today's equipment requires a more sophisticated approach. Most pieces should detect #38 AWG wire of ASTM (#30 AWG through the seventh step wedge). It should also have a penetration of 17 mm cold rolled steel. All machines must minimally comply with former FAR 129.26 "Use of x-ray Systems."

DETECTION CAPABILITIES

It is clear that detecting and recognizing a gun either by use of a metal detector or an x-ray machine is not an absolute and foregone conclusion. A successful detection is still dependent on the competency of the operator. In addition, a bomb is obviously more difficult to recognize than a gun. Terrorists do not submit baggage for screening with labels of "fragile, bomb included" stamped in clear view. Terrorists, or those seeking to do harm at airport facilities or while airborne, have used advances in technology to help them evade security procedures. New "toys" like the OSA gun are real and deadly and have turned up at airports. They look like a key chain but are really a low caliber gun capable of holding two bullets. The gun costs about $20, is about three inches long and an inch wide, and does not set off metal detectors (Klaidman, 1999). Despite its size, it can be used to kill. Interpol had even sent out a worldwide notice warning law enforcement of the potential danger. Plastic guns such as the Glock and Sigma pistols pose further threats. Even though they are not true plastic guns, because of the plastic content of the gun they can potentially evade security. An alert screener, however, can still detect the barrel, slide, and one spring, which are made of metal. Consequently both guns and explosives are becoming more and more difficult to detect, requiring the constant vigilance of the airport screener.

Using x-rays to detect a bomb and using them to disarm it are different procedures; however, the United States lags behind many countries in research to make these systems more viable. Some unique work has been accomplished at the Police Scientific Development Branch in the United Kingdom. Equipped with a lead-lined laboratory, the Explosive and Weapons Detection Group has done extensive work on the general requirements of x-ray imaging systems as well as the related health and safety issues associated with the equipment.

PRIOR X-RAY EXPLOSIVE DETECTION DEVICES

In June 1990, ESG&G Astrophysics introduced yet another option: False Image Protection (FIP). The purpose of the equipment was to test operator alertness. It also became useful in training operators to recognize specific threat objects. According to Kenneth Moore, "At a location away from the operator's station, a supervisor can activate an FIP and, on a random basis, superimpose a false threat object on the monitor screen showing an x-rayed bag. Thus, if the outline of a Glock 17 Automatic appeared on the monitor screen, the operator would have to press the control panel to acknowledge they had seen the false threat object. The operator's actions are recorded on a diskette for auditing purposes" (Moore, 1991). Even more sophisticated software has been developed (see Figure 9.3) and will be discussed in another chapter.*

* *Note*: The federal Food and Drug Administration (FDA) is responsible for the monitoring of scanning devices used in U.S. airports. They are tasked with assuring that the devices are designed to minimize the public and the employee's exposure to harmful rays. The contact point at the FDA is Division of Consumer Affairs, Center for Devices and Radiological Health, FDA, Rockville, Md. 20857, 301-443-4190. The National Institute of Justice sets the standards for metal detectors. Details can be viewed in NIJ Standard-0601.01, "Walk Through Metal Detectors for Use in Weapon and Contraband Detection," September 2000 and NIJ Standard-0602.01, "Hand Held Metal Detectors for Use in Weapon and Contraband Detection," September 2000.

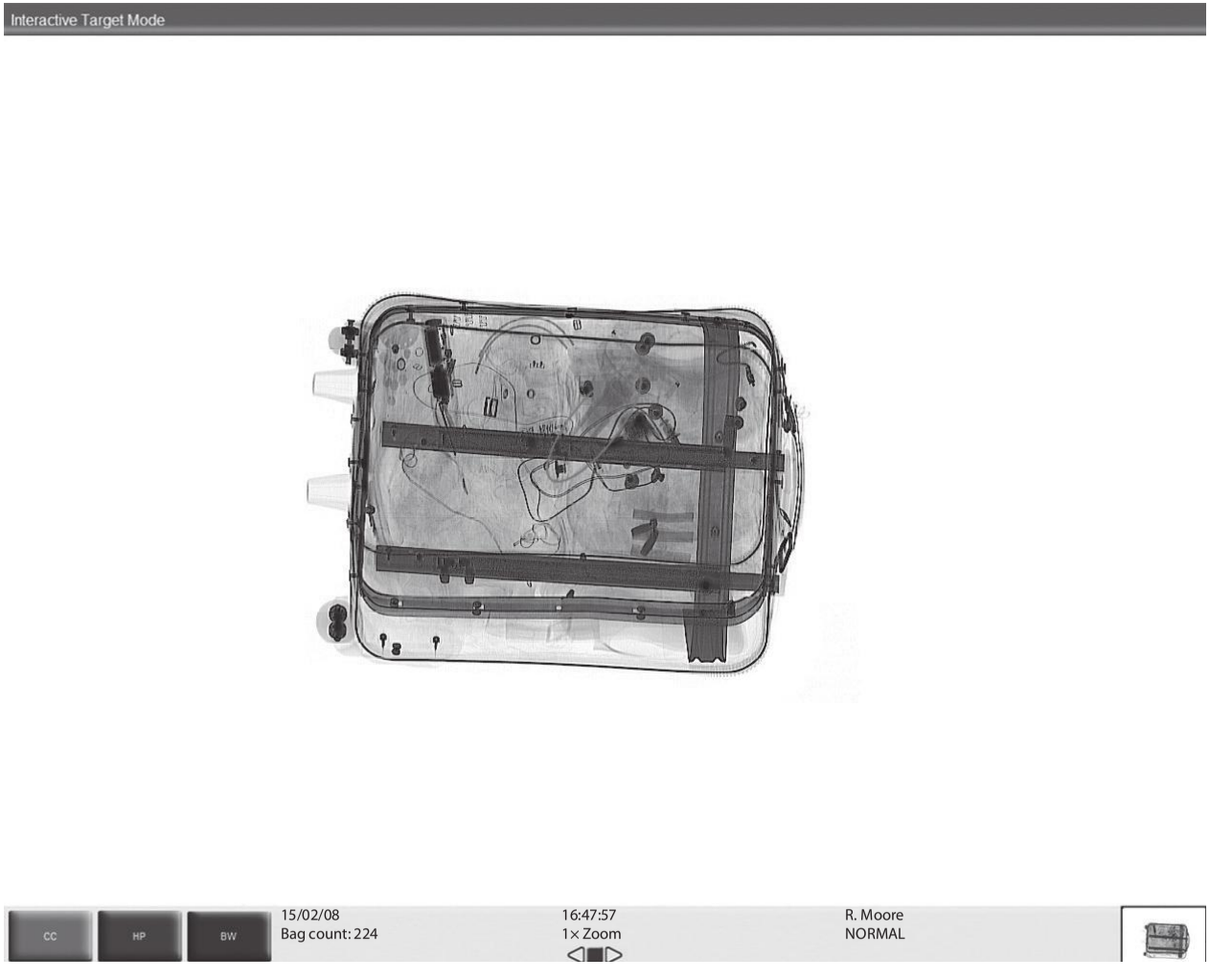

FIGURE 9.3 Rapiscan's Target™ system is a Screener Assist Technology (SAT) that uses software algorithms to search the X-ray image for targeted materials. The algorithm analyzes the mass, size and atomic number of items in the image against preset thresholds; objects that match the defined criteria are identified for the operator. Target™ has been used to aid screeners in identifying the explosives, drugs and narcotics, agricultural products (fruit and meat), gold, and currency. (Photo courtesy of Rapiscan Systems)

U.S. STANDARD ON RADIATION PROTECTION

The U.S. standard, originally developed by the National Committee on Radiation Protection, concluded that members of the public shall receive no more than 170 millirems per year from all man-made radiation sources other than medical exposures. As a point of reference, it is interesting to point out that cosmic radiation from the atmosphere can be over 200 millirems per year at high altitude cities such as Katmandu, Nepal, and Denver, CO. Radiation badges worn by operators record the amount of radiation they are receiving during a work period. A control badge is kept separate, away from the area in which the x-ray machines are operating. This enables the staff to have an environmental level of radiation exposure for comparison with the badges worn by the operators. The levels are recorded and maintained. All devices are designed to comply with the ANSI/HPS N43-17 standard and recommendations of the National Council on Radiation Protection and Measurement. Both standards detail procedures for measuring the radiation emissions from the source (scanning head). Certified personnel check the radiation emissions periodically per the procedures outlined by the ANSI and NCRP standards and recommendations.

In that the TSA implemented the use of explosive-detection machines, there was some concern regarding the potential of exposure to increased radiation to screeners. Between the dates of November 2202 and March 2003, National Institute for Occupational Safety and Health (NIOSH) received three health hazard requests concerning radiation exposure from explosive-detection system (EDS) machines. In response, TSA requested that NIOSH perform an independent study to determine the levels of radiation emissions from the various TSA screening equipment. The study recommended that the L3 EDS entrance and exit tunnels be reengineered, that the tunnels be bolted to the gantry, and that they improve conveyor and interlock safety systems. They also acknowledged that there was a "hot spot" about eight inches from the Invision EDS, but that it was correctable.

NEW COMPUTER SOFTWARE

Newer x-ray-detection machines contain threat image projection (TIP) software. It provides managers with the ability to test the alertness of employees. The software enables the manager to project x-ray images of weapons or bombs onto the scanner monitor. The employee must signal the manager that the "dangerous object" has been recognized. The system injects these random threat images into real bags going through the machine as well as onto images of bags created by the program. When a screener detects a threat and stops the bag, the software flashes a note of congratulation. The screener's performance, good or bad, is recorded. The system allows the airport security company to monitor each and every scanner's performance. Individuals that may need more training can be identified. Those that have difficulty detecting dangerous objects can be moved to another function. As once overheard by the author, screeners should at least be able to detect the difference between an UZI and an umbrella.

The system also allowed the FAA to oversee the performance of the airport security company. Companies could lose FAA certification if their screeners did not meet FAA standard detection criteria. On 22 May 2000, a spokeswoman for the FAA reported that "About $50 million to $65 million is to be spent on the better-resolution x-ray systems with TIP software, and about one-third of the airports (450 of the nation's busiest) will receive new equipment in each of the next three years" (New Airport x-ray Machines Can Train As Well As Protect, 2001). In July 2000, the FAA announced three contracts worth a total of up to $120 million to Rapiscan, Perkin Elmer, and Heimann Systems that allowed the agency to purchase up to 800 TIP installed x-ray machines from each vendor (FAA to Receive Award for Airport Security Screener, 2001).

In November 2000, *Aviation Week and Space Technology's* Innovation Award went to the FAA for implementing the TIP software. They received the award jointly with Rapiscan Security Products of Hawthorne, CA and Perkin Elmer Instruments of Long Beach, CA. the two companies that developed the imaging system. The FAA Administrator had announced that "We are extremely

pleased to receive this award honoring the most innovative new technologies in global aerospace, especially since this is the first time the FAA had been named as a recipient" (FAA to Receive Award for Airport Security Screener, 2001). The TSA continues to utilize this software daily and updates the programming on a regular basis to address new threats via an automatic image updates from the TSA technology laboratory.

EXPLOSIVE-DETECTION SYSTEMS

Screening all baggage is a gargantuan task. Screening all baggage at a reasonable throughput rate is an even greater challenge. Plainly, the vulnerability of aircraft to explosives placed in the cargo hold still poses a significant threat. In the 1970s, airline officials were forced to use technology already on the market. The most available device at the time, the EDS ION Track M97 used by the U.S. Army Explosive Ordinance Disposal units worldwide, was tested. It proved to be effective in detecting explosive materials but was not a practical method to screen the high volumes needed at a busy airport.

The FAA, therefore, awarded several contracts to a number of firms for developing a vapor-detection device. In mid-1987, *Thermedics* was developing a vapor-detection device, and Science Applications International Corporation (SAIC) was working on thermal neutron activation (TNA) as a detection method. However, TNA uses nuclear radiation, and even though it had been shown to have the highest degree of explosives-detection capability available at the time, it had its drawbacks. The system works when luggage passes through a cloud of very low energy "thermal neutrons." The neutrons are very penetrating and cause gamma rays to be instantly produced in the luggage, consequently revealing the presence of explosives. However, in 1991, the Congressional Office of Technology Assessment told a Senate committee that the TNA was flawed, and they recommended no new purchases of the equipment.

Technology has progressed a long way in the last decade. Mandated to screen all checked baggage by using explosive-detection systems at airports by 31 December 2003, the TSA has deployed two types of screening equipment: explosive-detection systems (EDS), which use computer-assisted tomography x-rays to recognize explosives, and explosive trace detection (ETD) systems, which use chemical analysis to detect explosive residues. EDS technology had been under development for many years and, as previously stated, is based on the same core technology as medical computer assisted tomography (CAT). CAT scans create a multidimensional image. As the conveyor moves each bag through the machine, the system creates a scan projection x-ray image. From this image, the computer determines which areas need "slice" images, taken by the rotating x-ray source. The scanner measures density more precisely from different angles as it circles the bag. Using sophisticated computer algorithms, the machine analyzes these images and compares their CAT properties with those of known explosives. If a match is found, the system sets off alarms and displays the object on the screen. Potential explosives are highlighted in red, detonators in green, and metallic objects such as circuitboards are shown in blue. The operator views the screen image to determine whether a real threat exists and follows established protocols for threat resolution.

Invision Technologies was founded in 1990 for the express purpose of adapting sophisticated medical computer assisted tomography technology for the detection of explosives at airports. The FAA Act of 1996 authorized the purchase of 54 CTX 5000™ luggage scanners (Nojeim, 1998). The company's *CTX 5000*™ products were the first systems to meet FAA certification requirements for automated explosive-detection systems. The CTX5000™ was certified in 1994 and has been operating in airport environments since that date. Invision's third-generation EDS was the CTX 9000 and was certified by the FAA in April 1999. It was originally one of the fastest EDS machines on the market and was certified at 542 bags per hour. According to the manufacturer, the system had the lowest false alarm rate and an actual throughput rate of 800 bags an hour. In addition, its 1-meter aperture allowed for smooth integration of standard airport baggage as well as oversized baggage. One of Invision's related products included the *CTX 2500EDS*™. It was designed specifically for

smaller airports, low-traffic areas in large airports, and mobile applications. It is smaller, lighter, and less expensive than many other models. The TSA ordered 400 model *CTX 2500* and *CTX 5500 DS* explosive-detection systems. L-3 Communications is also certified to manufacture the machines.

In 2004, General Electric acquired Invision Technologies for approximately $900 million, and the company is now known as GE Homeland Protection Inc. Prior to the acquisition the Securities and Exchange Commission charged InVision Technologies, Inc. with authorizing improper payments to foreign government officials in violation of the Foreign Corrupt Practices Act (FCPA). Simultaneous with the filing of the commission's charges, InVision agreed, without admitting or denying the charges, to disgorge $589,000 in profits from its FCPA violations plus prejudgment interest of approximately $28,700, and pay a $500,000 civil penalty (Internet: http://www.sec.gov/litigation/litreleases/lr19078.htm).

The CTX 9000 DSi is now one of the most widely used TSA-certified explosives-detection systems. According to the manufacturer, the CTX 9000 DSi has a certified throughput rate in excess of 500 bags per hour, arguably the fastest in the world, and has the widest aperture of any certified checked baggage screening device. The system was first installed in San Francisco for field testing as early as 1998.

Since then, GE Security has introduced the CTX 9400, which offers the potential for reduced false alarm rates, increased operational throughput, reduced operational costs, and increased uptime as part of the first step in a new multigenerational product plan for the CTX 9000 product line. GE's multigenerational CTX plan allows customers to choose the CTX 9400 as either new equipment or, thanks to backward compatibility, as an upgrade to existing CTX 9000 units. GE expects that future additional upgrades will provide customers with the opportunity to continually improve performance and extend the lives of their GE systems (see Figure 9.4).

The CTX 9400 DSi is the first aviation security device to allow "active" participation in a sensor-fused network, which can dramatically improve effectiveness by sharing data among sensors. Sensor fusion allows networked systems to modify their operation based on these inputs.

FIGURE 9.4 The CTX 9400 is GE Security's most sophisticated inline explosive detection System (EDS) and the second EDS in its Multi-Generational Product Plan for such systems. The system utilizes core technology derived from medical computed tomography. The projection x-ray images initially created determine which bags or cargo need slice images taken by a rotating x-ray source which can then be further analyzed and compared with the properties of explosives. (Image courtesy of GE Security)

Sensor-fusion integrations, such as the recently announced combined CTX 9000 DSi/XRD 3500 system-of-systems, can add significantly to screening effectiveness and efficiency. As of early 2008, approximately 100 of the new CTX 9400 EDS had been sold to the TSA and airports around the world as complete new units and upgrades to existing CTX 9000s.

The Department of Transportation award to the Boeing Co. included an initial contract of $508 million for the period June through 31 December 2002, the date that the Aviation and Transportation Security Act originally mandated that all checked luggage be screened for explosives. As mentioned, the total contract was valued at $1.37 million. Boeing was scheduled to install up to 1100 explosive-detection machines and 4800 to 6000 explosive trace detection machines. Boeing had indicated it would utilize 14 subcontractors to fulfill the contract.

The most common machines weigh about 9350 pounds and are about the size of a sport utility vehicle. Most machines are stand-alone models and are placed near the check-in counter. Some are integrated into an airline's baggage handling system, which greatly speeds the process. A machine can take several months to install, and some airports needed to reinforce the floors to support the equipment. The floor space or footprint must also be wide enough and be near a power source. Both Invision and L-3 Communications had gone on record indicating that they would be hard pressed to manufacture sufficient quantities of machines to meet the government's original December 2002 deadline. Additionally, the maintenance costs associated with these systems is significant.

TSA spent almost $470 million from fiscal years 2002 through 2005 for EDS and ETD maintenance. In fiscal year 2006, TSA estimated it would spend $199 million and had projected it would spend $234 million in fiscal year 2007. TSA was not able to provide the General Accouting Office (GAO) with data on the maintenance cost per machine before fiscal year 2005 because, according to TSA officials, its previous contract with Boeing to install and maintain EDS and ETD machines was not structured to capture this data. Regardless, it must be recognized that EDS machines and the supporting operating costs are quite high. Oversight of this process will require significant diligence in the future.(GAO -06-795).

THREE-DIMENSIONAL IMAGING: EXPLOSIVE ASSESSMENT COMPUTED TOMOGRAPHY

Since the British police frustrated a plot to smuggle liquid explosives onto U.S.-bound commercial aircraft in carry-on baggage, the TSA has been rushing to develop technologies that could recognize such items. Analogic Corp. (Peabody, MA) announced that they had developed a third-generation scanner that can detect objects of any shape that are massive enough to be a threat, including liquid explosives. The system known as King Cobra (Carry-On Baggage Real-time Assessment Explosive & Weapon Detection System), XLB1100, or Exact, was scheduled to pass certification by the TSA in the summer of 2008. The system contains a computer that not only recognizes the shape of threatening objects, such as guns and knives, but also measures the density of objects so as to recognize when an unidentified mass, including liquids, is of sufficient volume to be a potential threat, said developer John W. Wood Jr., former president and CEO of Analogic. In March 2008, the company announced that Analogic and L-3 Communications LLL have concluded an agreement awarding L-3 exclusive, worldwide rights to market and service Analogic's KING COBRA(®) and XLB(™) 1100 security imaging systems 3DX (®) inside their explosive-detection system for air carrier checked baggage applications.

The system has adapted computer software to look for the newest recognized threats, from butane lighters and liquid binary explosives to flammables. The underlying technology has been integrated into third-generation scanning devices that check carry-on bags for new threats, scan up to 300 bags per hour as a stand-alone system, or 400 bags when integrated into an automatic baggage handling system. Cobra scanners sell for approximately $350,000 to $450,000 (US dollars), compared with $40,000 to $70,000 for a standard x-ray machine. However, the manufacturer argues

that the scanners will pay for themselves in a couple of years because their automated 400-bag-per-minute speed will eliminate the need for two human screeners at each checkpoint. The technology draws on Analogic's expertise in making medical scanners. By the late 1990s, Analogic was already adapting what is known as CAT scanners-- for use by airport security.

Cobra scales down the larger and original technology "Exact" to a size and cost that makes it economical for use in screening carry-on bags. According to Analogic Corp., "There are currently 42,000 screeners that cost approximately $2 billion annually, but by using our Cobra at passenger checkpoints, we could reduce the number of screeners required" (MSNBC, 6 March 2008). Analogic's CAT scanners use a single emitter of a fan-shaped x-ray beam on a rotating gantry that encircles the bags passing through. By virtue of thousands of detectors on the other side of the gantry, intelligent software can recreate a three-dimensional image of the bags and all their contents. The image can then be rotated to any angle for quick viewing.

The detectors first convert incident x-rays into visible light that is subsequently directed at integrated photodetectors, which send the data, via brushes on the gantry, to a computer workstation. The software also performs automatic object recognition, puts a red square on possible threats, and presents the results to the screener, who uses a touchscreen to rotate the image to any orientation. The images are also transmitted over a network to a server for subsequent viewing. Thus, if an aircraft goes down, the images of the bags that were on it can be studied after the fact. The third-generation CAT technology uses dual power settings that measure the density of objects and are represented to screeners as different colors.

A relatively new emergent to the field, Reveal Imaging Technologies headquartered in Bedford, MA, has developed the first EDS technology designed for integrated 100 percent checked baggage inspection in airports. Reveal's product is a smaller model, dual energy CAT scanner. Reveal's scanner is significantly more cost-effective and space-efficient than many current EDS systems, less than half the size and cost of currently available screening options. The scanner offers a viable option for carry-on baggage inspection and facility protection applications in locations that cannot use large EDS systems due to space or cost constraints (see Figure 9.5).

BOTTLED LIQUID SCANNERS

Bottled liquids scanners utilize EDS technology to differentiate liquid explosives from common, benign liquids. This technology is capable of scrutinizing substances within a bottle by aiming sensors at the bottle aperture and analyzing the intake of certain vapors. TSA has piloted two hand-held explosive detection systems in the airport environment: the Nomadics, Inc. Fido PaxPoint and the Smiths SABRE. The challenges of screening bottles for concealed explosives or flammable liquids have been explored for a decade plus, but previous technology was not operationally viable due to commonalities in materials and high alarm rates. The challenge has been twofold: the range of physical properties of liquid explosives and potential flammable liquids, and the broad range of benign, common liquids with which people travel. The TSA anticipated deploying up to 200 bottled liquid scanners at the nation's busiest airports in FY 2007.

The TSA began experimenting with liquid explosive detection devices in the wake of the disruption of an alleged airline bombing plot in August 2006. Funds were earmarked for this research through the Homeland Security Advanced Research Projects Agency (HSARPA), under the Department of Homeland Security (DHS)-sponsored Rapid Technology Application Program (RTAP) established to meet the needs of emergency responders and internal DHS customers. The FIDO system weighs less than three pounds and can even be inserted into plastic baggies holding liquid containers. The highly sensitive device is capable of detecting trace levels of explosive materials in parts per quadrillion (ppq). If the detector sounds an alarm, each bottle must be removed from the bag and tested individually.

Bottled liquid scanners have been deployed at the following airports (Internet: http://www.tsa.gov/press/releases/2007/press_release_05222007.shtm):

FIGURE 9.5 A law went into effect in December 2003 requiring that all cargo, both domestic and international, be checked for explosives by using a myriad of detection devices and techniques. The Reveal Imaging M CT-800 scanner is shown here. Reveal Imaging Technologies has developed an EDS designed to easily and inexpensively integrate into the operational flow of an airport or facility. (Photo courtesy of Reveal Imaging Technologies, Inc.)

- Miami International (completed)
- Newark Liberty International (completed)
- Detroit Metro (ongoing)
- Los Angeles International (ongoing)
- Las Vegas McCarran International (ongoing)
- Chicago O'Hare International Airport (ongoing)
- Boston Logan International (ongoing)

TRACE DETECTION TECHNOLOGY TODAY

Trace detection technology today is based on the immediate identification of either particles of explosive or vapor containing the explosive material. Actual explosive material must somehow be transported to the equipment for analysis. The amount must be sufficient for the equipment to recognize the material for what it is. Of course, electromagnetic and imaging technologies do not require the equipment to actually analyze the weapon's chemical makeup, only its image. For trace detection equipment to function, a two-step process is involved. The material must be actually collected and then quickly identified. All equipment must be approved by the TSA, and it is currently required that all baggage on international flights be screened (FAR Section 108.20 Use of Explosives Detection Systems, 2001). The new rules effective December 2002 require that all domestic cargo be screened as well.

Initially, research and development efforts focused on collecting the vapor around a person or a piece of baggage to search for various types of commercial and military explosives, including dynamite, Semtex, C-4, and TNT. Unfortunately, they do not really give off a great deal of vapor that can be evaluated. Therefore, research has expanded to the breakdown of the particulates of explosive material as well. If explosive material is to be detected from an air sample or removed from a

substrate (i.e., a person's clothing), the technology required is sophisticated. Both have their own pluses and minuses. Basically, "Vapor technologies are more effective for detecting explosive materials with high vapor pressures, while particulate technologies are more appropriate for explosive materials with low vapor pressure, such as military plastic explosives" (Airline Passenger Security Screening, 1996). Samples for both methods can be acquired by having the passenger walking through a portal or by using a hand-held device.

Devices today can be either contact or noncontact. They combine chemiluminescent detection with gas chromatography. Gas chromatography is the most widely used scientific technique for the positive separation and identification of explosives in a complex mixture. Sample material is heated into gaseous form. It is added to a carrier gas and separated into its individual components by controlled temperature cycling. The components are sent to the chemiluminescent detector in the carrier gas. All nitrogen-based high explosives contain nitrogen chemical groups. For baggage, the operator swipes the surface of the object. In a contact device, the passenger must actually push on a door to get into the portal scanner. In a noncontact device, air passes over the passenger and collects the necessary material for analysis. Hand-held devices can also be used but do require a significant investment in time to process each passenger. Developmental efforts continue because it remains difficult to extract the explosive vapors or particulates from a passenger and adequately test them for every known explosive material. An additional problem revolves around clearing the system once a positive detection has been made. A trained security officer must constantly monitor the baseline readings of the equipment to make sure that subsequent readings do not become cumulative and thereby false. Future technologies under development in this area include pyroluminescence, chemical sensors, and ion drift spectroscopy.

EXPLOSIVE DETECTION DEVICES FOR BAGGAGE

In response to the President's Commission's findings, in November 1990, Sec. 108 of the Aviation Security Improvement Act amended the provisions of the Federal Aviation Act of 1958 pertaining to explosive detection equipment. Section 320 Deployment of Explosive Detection Equipment reads:

> General Rule: No deployment or purchase of any explosive detection equipment pursuant to Section 108.7(b)(8) and 108.20 of Title 14, Code of Federal Regulations, or any similar rule, shall be required after the date of the enactment of this section, unless the Administrator certifies that, based on the results of tests conducted pursuant to protocols developed in consultation with expert scientists from outside the Federal Aviation Administration, such equipment alone or as part of an integrated system can detect under realistic air carrier operating conditions the amounts, configuration, and types of explosive material which would be likely to be used to cause catastrophic damage to commercial aircraft.

The European Civil Aviation Conference (ECAC) had mandated a deadline of 2002 for trace detection device implementation of 100 percent hold baggage screening in Europe several years ago. Currently, in the United States only international flights undergo a 100 percent scanning of cargo, but as stated the rule has been expanded. However, cost factors will likely be determinative of the final discussion as to when to implement them. The debate over aircraft and airport security, particularly in the cargo hold, intensified in the aftermath of the Trans World Airlines Flight 800 disaster and again after 11 September. The midair explosion over Long Island, NY, in 1996 at least forged a consensus in government and by the public that drastic measures may well be needed. At the time, President Clinton established the White House Commission on Aviation Safety and Security led by Vice President Al Gore. They recommended new technology to be utilized for surveillance and screening. Unfortunately, at the time, some of the much-needed technology did not really exist.

In April 2002, the U.S. government announced the Department of Transportation (DOT) would deploy approximately 1100 EDS and 4700 ETDs by 31 December 2002. The date was later extended. The TSA has in turn concluded that a mix of these two technologies will provide sufficient protection. This was in reality the first example that insufficient numbers of EDS machines simply did not exist to meet the deadline. The DOT has determined they will decide the mix of equipment based on the following:

1. Peak bag loads
2. Ability of the airport and air carrier to integrate EDS into the baggage handling system
3. Physical restrictions of EDS having to do with weight and size
4. Construction cost associated with EDS installations due to excessive structural modifications needed
5. Availability of EDS from the manufacturers

ENHANCING ETD CAPABILITY

On 12 May 1997, the FAA and TSA announced the purchase of $12.2 million worth of trace detection security equipment. This equipment was designed to detect extremely small amounts of explosives on such items as electronic equipment and small articles in carry-on baggage. The concept was to develop equipment that would enhance the x-ray machines already in use with little or no interruption of passenger or baggage flow. The FAA awarded contracts to Thermedics Detection Inc. of Chelmsford, MA, Barringer Instruments Inc. of New Providence, NJ, and Ion Track Instruments of Wilmington, DE. The companies developed the devices described below (AAR Technology R&D Fact sheet, 2001). Prospective purchasers need to evaluate the systems' sensitivity features, ease of use, false positive rates, and ability to detect International Civil Aviation Organization (ICAO) taggants.

THERMEDICS EGIS 3000, EGIS II, EGIS III

These devices use high-speed gas chromatography with chemiliminescence detection. It is made up of a free-standing analytical unit that takes up relatively little space. Sample collection is accomplished by wiping a surface with a specially designed filter. The filter is then placed in the analytical unit, and the EGIS begins an 18-second analysis to determine the presence of an explosive. If one is detected, the unit also identifies the substance. The German Ministry of Interior has selected the EGIS III system for all explosive detection at German airports. The selection was based on the result of an ECAC performance test. It already is used to screen passengers and freight on the Channel tunnel that links the United Kingdom with the European continent.

BARRINGER IONSCAN 400B, CENTURION, SENTINEL II

This device uses ion mobility spectrometry. IONSCAN is a detection-identification device designed to screen and search for trace amounts of explosives that contaminate the baggage it has come into contact with previously. Sample collection is accomplished by either wiping a surface with a cotton swab or by using a battery-operated small vacuum cleaner-type device that deploys a filter card. The sample is then placed onto a sample tray and slid into an analyzer. Within 5 seconds the unit confirms the presence of and identifies explosives.

Barringer Instruments, part of Smiths Detection & Protection Systems (DPS), announced in May 2002 that it continued to receive additional orders from the TSA for its IONSCAN® trace explosives detectors. Since December 2001, orders totaling approximately $9.7 million have been placed. These instruments have already been deployed at numerous U.S. airports. The IONSCAN® was widely deployed at Salt Lake City Airport for the 2002 Winter Olympics. Over 80 systems

were installed at the ticket check-in counters to screen checked baggage. The deployment of these systems continues to proliferate.

ION TRACK ITEMISER 3, ENTRY SCAN

This device also uses ion mobility spectrometry. It also seeks out and detects trace quantities of explosives that can contaminate various objects. Either wiping a surface or collecting the sample with a vacuum device also accomplishes sample collection. The sample is processed through the unit, and an analysis provided within five seconds. Ion Track Instruments' ITEMISER desktop contraband detection and identification system is simultaneously detecting and identifying traces of both explosives and narcotics on virtually any surface. ITI's Ion Trap Mobility Spectrometry (ITMS) surpassed conventional Ion Mobility spectrometers (IMS) in ionization efficiency and sensitivity due to its patented ion trap. Adding high-speed switching technology that allows identification of time-of-flight peaks for substances in both positive and negative ion modes has further enhanced it. Conventional IMS detectors are restricted to operating in only one mode per sample, making screening for explosives and narcotics with one instrument a complex and time-consuming process. Extensive use of the latest computer technology software in the design of ITEMISER3 has produced an instrument that requires no user intervention or interpretation. Consequently, operators can concentrate on obtaining good trace samples of explosives or narcotics. An operator need only sample the surface of an item that is suspected of being contaminated with traces of explosives or narcotics and insert the "sample trap" in the slot located in the front of the instrument to trigger analysis.

ETD nuisance alarms can be caused by the presence of actual explosive residue on a passenger as a result of their job or medical condition, for example, construction workers, law enforcement personnel who handle explosives, or a passenger using nitroglycerine as a heart medication. Appropriate procedures need to be in place to resolve these alarms in a timely manner.

TAGGANTS

The practice of "tagging" or using " taggants" to render explosives detectable by gas analysis methods that are currently available have become commonplace. Their implementation was discussed earlier in relation to the successful international coordination by ICAO to tag these materials. In 1990, a special subcommittee of the legal committee of ICAO drafted a treaty to require the addition of taggants to all explosives manufactured in one of the contracting states. The United Staqtes signed this convention on the Making of Plastic Explosives for the Purpose of Detection in March 1991.

Security experts generally agree that all explosives and all explosive precursors should be labeled so to be able to readily identify the source and disposition of these kinds of materials. Some manufacturers have expressed the concern that a problem with direct labeling of explosives is the unknown effect on the stability, life, function, and sensitivity of the additive. Commercial explosives can be labeled with ceramic particles. These particles or chips are mixed with the granular support of the explosive. The chips are multilayered, and the layers are colored to form a readable tag. The tag or code identifies the manufacturer and the batch number. The outside layer of the particle glows under ultraviolet light, and the particles can be easily recovered from an explosion site. This is possible chemically because commercial explosives are not really granular; the ceramic particles are actually trapped in the mixture. Because the added particles are separate from the explosive, suspended in the mixture, the taggant does not accelerate decomposition or a change in the behavior of the active ingredients. Detonators are not labeled with taggants because of the known effects such an additive would have on the explosive's stability.

Explosives need to be distinguished from smokeless propellant and black powder. Smokeless propellants are the "granular materials that are often called smokeless powder but which are not explosives and which burn but do not detonate." They are used in firearms. Advocates of airport security and the international tagging of explosives are not really concerned with the tagging of

materials used in firearm ammunition. They are concerned with the tagging of materials used in high-density explosives and certainly with the tracking of weapons-grade nuclear materials as well as the components of biologic and chemical weapons.

PROJECT HOSTILE INTENT

Researchers at the DHS are developing technology that could analyze a person's behavior to determine if they are a terrorist attempting to deceive airport security. They have even been trained by the best: the Israelis. Project Hostile Intent aims to develop technology that could automatically analyze behavioral and physiological signs associated with lying. DHS plans on demonstrating the technology to the TSA in 2008, with test deployments in 2010 and full implementation no later than 2012. Researchers have already developed technology that has an accuracy rate of around 80 percent in a controlled setting. The technology analyzes three areas of behavior: gestures and microfacial expressions, speech variation, and the physiological characteristics tested by polygraphs. DHS officials hope that the technology will be more accurate than polygraphs, which are inadmissible in court because of questions about their effectiveness. Critics of the initiative argue that researchers do not have the technology available to develop an effective system by 2012, with one expert estimating that a successful system could not be created for at least 15 years. One problem is differences in cultural background and personality type, which affect how test results should be analyzed. While researchers are working toward a technological solution, the TSA is training its screeners on how to recognize suspicious behaviors and microexpressions.

CONCLUSION

New innovations in scanning equipment will only enhance airport security personnel's ability to detect dangerous weapons and explosives, even in minute qualities. The equipment will be faster and more accurate than ever before. Additionally and to the dismay of opponents, weapons and explosives are becoming continually more intrusive. Advancements in imaging and detecting concealed weapons and explosive devices have made rapid advancements in the last few years. Current EDS nuisance alarms are usually the result of the similarity of densities of some materials with the densities of some explosives. However, detectors for locating electronically detonated bombs, improved surveillance cameras, human and vehicle recognition systems, and x-ray systems for bomb disarmament are all undergoing some serious research and development programs. It will be interesting to follow whether both the public and the courts continue to perceive these advancements as contrary to constitutional law or acceptable intrusion. New quadruple resonance (QR) systems can operate as a stand-alone machine or integrate into an airport's baggage-handling system. A pass or fail test immediately tells the operator whether or not an explosive threat is detected. An x-ray image can confirm an explosive device is present. Public reaction since 9/11 has been positive. However, acceptance is waning, and the hassle factor at airports has received and deserves some attention.

Many companies receive government funds to fund their research. Others see the field as worthy of their own resources and envision the ability to make profits from the production of detection products. In other words, industry recognizes that the ongoing problem of possible terrorism at airports will be with us for many years to come.

REFERENCES

AAR Technology R&D Fact sheet, "Trace Detection Security Equipment," http://www.faa. gov/aar/trdfs/tdsefs. htm, 3 Aug 2001, pp 1, 2.

Airline Passenger Security Screening, New Technologies and Implementation Issues, National Research Council, Publication NMAB-482-1, National Academy Press, Washington D.C. 1996, pg. 17.

Airport Security, http://www.skyguide.net/html/travelresources/ security.html, 14 February 2001, pg. 2.

Arrillage, Paula, Associated Press, *Texas News*, 25 November 1998.
Carts-Powell, Passive Millimeter Wave Imaging, http://www.spie.orf/web/oer/march/mar 97/ passivemm.html, 13 August 2001.
Clark, Staten, "Airport Safety and Security: Minimal Acceptable Standards," http://www.emergency.com/air-prtsc.htm, 4 June 2001, pg. 1.
Debenham, J.K., A Brief Description of the Effects of x-ray Inspection on Unprocessed Photographic Film, Film Technical Services Division, Eastman Kodak, 1973.
Defining Multi-Zone Detection: Check Apple for Apples, http:// www.omni-security.com/wthru2/wtindex.html, pg. 2, 3 May 2001.
Development of Systems to Evaluate Magnetic Fields Produced by Walk-Through and Hand Held Metal Detectors", Office of Law Enforcement Standards, Internet:http://www.eeel.nist.gov/810.02/detection.html, pg. 1, 11 July 2001.
FAA to Receive Award for Airport Security Screener, *Air Wise News*, http://news.airwise.com/stories/2000/11/974208505.html. 3 Aug 2001.
FAR Section 108.20 Use of Explosives Detection Systems, http://www.faa.gov/avr/AFS/FARS/far-108.txt, pg.15, 24 April 2001.
How a Metal Detector Works, http://micro.magnet.fsu.edu/ electromag/ java/detector/ pg. 1, 24 July 2001.
http://www.sec.gov/litigation/litreleases/lr19078.htm.
http://www.tsa.gov/approach/tech/mwave.shtm.
Klaidman, Daniel, "The New Secret Weapons," *Newsweek,* 18 May 1999, pg. 37.
MSNBC, 6 March 2008.
Moore, Kenneth, Airport, Aircraft and Airline Security, Butterworth Heinemann, 1991, pg. 137.
New Airport x-ray Machines Can Train As Well As Protect," *Scripps Howard New Service*, http://www.caller.com/cfapps/printhis/ index.cfm, 3 August 01.
New Filmshield XPF Protects Film From High Dosage Airport Security Equipment, Iternet:http://www.sima-corp.com/xrayinfo.htm, 3 Aug 2001, pg. 2.
NIJ Standard-0601.01, "Walk Through Metal Detectors for Use in Weapon and Contraband Detection," September 2000.
NIJ Standard-0602.01, "Hand Held Metal Detectors for Use in Weapon and Contraband Detection," September 2000.
Nojeim, Gregory T., "Aviation Security Profiling and Passengers' Civil Liberties", 13 *Air and Space Law*, 1998, pg3.
Portable Digital x-ray Imaging System-RTR-4, http://www.americanaimpex.com/x-ray.htm, 24 July 2001, pg. 4.
Portable Digital x-ray Imaging System, http://www.americanaimpex. com/x-ray.htm, pp. 1–5.
Technical Report Confirms Film Damage, *Air Wise News*, http://www.airwise.com/news /headlines/scanners2.html, pg. 1–4, 3 Aug 2001.
Wu, 2004, The history of airport screening. retrieved 3 March 2007 from www.savvytraveler.publicradio.org.
X-ray Advice, Internet:http://sung3.ifsi.rm.cnr.it/~dargaud/Photo/xray.html, 3 Aug 01, pp. 1, 2.
Yates, Chris, Ed., Jane's Airport Security Standards and Technology, Internet:http://www.james.com/press/pc990723.shtml.

10 Cargo Security
A Loose End

NEWS

17 June 2002: L-3 Communications publicizes that it has successfully completed its acquisition of the detection systems business of Perkin Elmer, which has an installed base of over 1600 units at airports for checked and oversized baggage, break bulk cargo, and air freight.

19 June 2002: Invision Technologies Inc. announces multiple orders for its CTX brand explosive detection systems. The order totals approximately 6.6 billion U.S. dollars.

29 May 2003: "We are aware of that deficiency with regard to the inspection of cargo," Ridge says in a speech to the House Select Committee on Homeland Security. "We focused on the baggage, we focused on the passengers, and now we're beginning to focus on the cargo. Presently, only about one-fifth of cargo boarded onto commercial planes is screened, and there is no immediate plan to correct the problem."

10 August 2005: Nearly four years after 11 September 2001, Americans flying on passenger planes remain vulnerable to another terrorist attack in the air because of lax screening of the millions of tons of cargo loaded into the belly of aircraft.

2005: Although screening of passengers and their luggage has been shored up dramatically since hijackers commandeered four planes and crashed them into the twin towers of the World Trade Center, the Pentagon, and a Pennsylvania field, little has changed regarding the security of cargo, according to an FAA inspector and the vice chairman of the 9/11 Commission.

26 March 2007: The Department of Homeland Security will begin testing air cargo screening technologies this spring at the Cincinnati Northern Kentucky International Airport (CVG) as part of the department's previously announced $30 million Air Cargo Explosives Detection Pilot Program.

INTRODUCTION

Cargo screening and inspection is just as important as the screening of passengers and their carry-on luggage, even more so if it is assumed that the terrorist does not want to sacrifice his or her life for the cause and seeks to hide the bomb on board an aircraft unaccompanied. The catastrophe of Pan American Flight 103 over Lockerbie, Scotland, is the perfect example. The attack on 11 September raises the question, what next? The disaster reinforces the concept that no matter how demanding the present security cargo procedures seem, under current standards, a bomb may somehow find its way into the cargo. Prevention before the event is of course a key element of any solution. However, all available efforts also need to be made to minimize the damage once the inevitable is about to happen. Speed, volume, and on-time delivery requirements drive today's cargo business strategy of supply-chain management. The increase of sophisticated threats from terrorists, international crime organizations, and cyber-crime potentially could have a catastrophic impact on global trade. The new cargo criminals are nationally networked and internationally financed.

New technology needs to be developed in the specific field of cargo security. For example, blast containment and blast resistant technology need to be further developed. Additionally, the screening of sealed U.S. mail must be further analyzed and addressed. Regulations and controls on indirect shippers is yet another issue worthy of follow-up research. This chapter will discuss some of the topics pertaining to cargo, airmail, "unknown shippers," and the general consigning of cargo by air.

The challenge is readily apparent: how to screen literally billions of bags and consigned cargo quickly enough to prevent massive backups at airports, but thoroughly enough to prevent a tragedy. The task is a daunting and often frustrating one. Initial cargo-scanning machines were slow, huge, and were prone to false alarms. They were also very expensive. Invision's CTX 5000™ was the first and initially the only one certified by the Federal Aviation Authority (FAA). These machines, as discussed previously, are essentially the same as medical computed axial tomography (CAT) scanners, although much more powerful and connected to powerful computers. The cost for each machine remains at approximately 1 million U.S. dollars each or more. This raises the cost of cargo security considerably, especially for smaller airports unable to absorb the high cost. Therefore, the public's awareness of the need to purchase, update, and maintain this equipment, before another tragedy occurs, is absolutely critical. A plethora of other companies now also manufacture a variety of x-ray scanners and metal detectors. The name brand is irrelevant, but the quality of the machine and its practical use in airports is essential. The Transportation Security Administration (TSA) had proposed rules to make the screening of domestic cargo as stringent as is already required for international cargo, and Congress has initiated legislation in this area. However, complications have arisen, and the implementation of some of the new rules has been delayed.

Clearly, there can be no total security guarantee given to the concept of protecting aircraft against incendiary or explosive attacks. However, if properly addressed, the risk to baggage and cargo handling can be greatly reduced. New technology pertaining to compartmented baggage containers and even more sophisticated explosive detection and trace detection devices will enhance protective efforts even further. Additionally, in November 2004, the TSA issued the following Notice of Proposed Rulemaking:

> The Transportation Security Administration (TSA), an agency within the Department of Homeland Security's Border and Transportation Security Directorate, proposes to amend current transportation security regulations to enhance and improve the security of air cargo transportation. The Aviation and Transportation Security Act directed TSA to implement measures to enhance the security of air cargo transported in both passenger and all-cargo aircraft. In discharging this responsibility, TSA conducted analyses of internal and external threats, risk and vulnerability assessments, and security measures already in place. This proposed rulemaking would require the adoption of security measures throughout the air cargo supply chain; these security measures will be applicable to airport operators, aircraft operators, foreign air carriers, and indirect air carriers. These proposed regulatory requirements would impose significant barriers to terrorists seeking to use the air cargo transportation system for malicious purposes. This proposal would also change the applicability of the requirement for a "twelve-five" security program from aircraft with a maximum certificated takeoff weight "of 12,500 pounds or more" to those with a maximum certificated takeoff weight of "more than 12,500 pounds." This change would conform the regulation to recent legislation.

Comments were received through 10 January 2005. In May 2005, bill HR 2649 was introduced into the 109th Congress stipulating the following:

> Not later than 3 years after the date of enactment of the Strengthen Aviation Security Act, the Secretary of Homeland Security shall establish a system to inspect 100 percent of the cargo transported on passenger aircraft to ensure the security of all passenger aircraft carrying cargo operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation. "(2) MINIMUM STANDARDS. The system referred to in paragraph (1) shall, at a minimum, require that "(A) equipment, technology, and personnel meets the same standards established to inspect passenger baggage;"(B) 35 percent of cargo carried on passenger aircraft is inspected by the end of fiscal year 2006; "(C) 65 percent of cargo

carried on passenger aircraft is inspected by the end of fiscal year 2007; and ''(D) 100 percent of cargo carried on passenger aircraft is inspected by the end of fiscal year 2008.

Additionally, HR 2688, introduced in 2005 by Rep. Nita Lowey (D-NY), would require the physical screening of all people, goods, property, vehicles, and equipment before they are allowed into the secure area of an airport. The bill would take effect 120 days after it is enacted. Until the measure took effect, the bill would require that the government conduct random screenings and inspections of such articles. Under the measure, the TSA would have been required to report to Congress on ongoing efforts and projected timelines for developing screening standards for airport personnel, assessing available technologies for securing airport perimeters, and developing and implementing a standardized approach for conducting airport vulnerability assessments. Neither bills became law but were stalled in committee.

CARGO CARRIER RESPONSIBILITY

Baggage was previously covered in the FAA regulations in Part 108. In particular, FAR 108.13 (b) required the baggage carried in an airplane be checked by a responsible agent and that identification be obtained from all persons, other than known shippers who seek to ship goods or cargo aboard the airplane. Today 49 CFR Chapter XII Part 1548.9 Acceptance of cargo states:

a. *Preventing or deterring the carriage of any explosive or incendiary.* Each indirect air carrier must use facilities, equipment, and procedures described in its security program to prevent or deter the carriage of any unauthorized explosive or incendiary on board a passenger aircraft in cargo.
b. *Refusal to transport.* Each indirect air carrier must refuse to offer for transport on a passenger aircraft any cargo if the shipper does not consent to a search or inspection of that cargo in accordance with this part, and part 1544 or 1546 of this chapter. The indirect air carrier must search or inspect cargo, and must request the shipper for consent to search or inspect cargo, as provided in the indirect air carrier's security program.

When airlines leave the baggage unattended, the ramifications can be quite serious. This was evidenced clearly as regards Pan American Flight 103, where the baggage container had been left unattended for over 30 minutes. Appropriate access control procedures are not only mandated by the TSA, but also represent a commonsense approach to security. It is crucial that once cargo has been accepted from the passenger or shipper that it be under continuous control. Once the airline accepts baggage at the check-in counter, or curbside, it is usually placed on a conveyor belt where it is transported to a centralized sorting facility. Not every piece of baggage can be observed every minute; however, restricting access to the cargo will reduce both pilferage and unauthorized tampering. Even when the baggage is loaded onto a baggage cart from the central location for transportation to the aircraft, the baggage carts are rarely if ever sealed. Just restricting the public to the cargo-baggage area is insufficient. This is an area where the prescreening of employees and stringent access control standards are essential. It does not matter if every single piece of cargo has been screened or manually inspected if an employee who has access decides to tamper with it.

Another issue revolves around unaccompanied baggage. Anyone who travels knows that there are numerous reasons why bags become separated from their owners. Most travelers do not really appreciate arriving at their destination without bags, and the reasons are mysterious to the traveler who arrives at his or her destination without luggage. It is the same cosmic question as where do those socks go in the dryer. However, there are many legitimate reasons why unaccompanied bags present no real threat; including bags in which the owner has taken an earlier flight or misdirected baggage caused by airline error. On the other hand, the separation may be deliberate, causing a hazard to flight or for the illegal movement of drugs or other contraband. These instances, although

statistically insignificant when compared with the total amount of baggage processed, are highly significant when a terrorist operation is underway.

Formerly, Parts 108 and 129 of the FARs required U.S. and foreign air carriers to adopt and carry out a security program. Each program had to have been approved by the FAA. Within the United States, the requirements for U.S. and foreign carriers mirror each other. TSA 49 CFR Chapter XII, Part 1548.7 Approval and Amendments of the Security Program require the air carrier to have the TSA approve its security programs 90 days prior to implementation. Many amendments have been made to the original rules. One significant amendment changed the definition of the "known shipper" concept. Too many airlines were accepting cargo for carriage without really knowing the origination of the cargo. During 1995, the FAA started to record air carrier and airport inspection data into a new national data base. The program developed the Air Carrier and Airport Inspection Reporting System (ACAIRS). The system records data on all aspects of an air carrier's security obligations, including cargo security requirements. One of the greatest threats to aircraft safety remains the unauthorized shipment of hazardous or dangerous cargo. Shippers often attempted to ship such dangerous cargo mixed in between permissible cargo, attempting to seal it with black plastic, hoping the airlines or the FAA would not check it.

REPORT TO CONGRESS ON AIR CARGO SECURITY

In May 1998, a report was submitted to Congress in response to the requirement in Section 313 of Public Law 104-264 of the Federal Aviation Reauthorization Act of 1996. Section 313 (a) stated that the Secretary of Transportation shall transmit to Congress a report "on any changes recommended and implemented as a result of the White House Commission on Aviation Safety and Security to enhance and supplement screening and inspection of cargo, mail, and company-shipped materials transported in air commerce." The annual reports have consistently pointed out some significant discrepancies still exist within the airport security context (see Figure 10.1).

The Aviation Security Advisory Committee (ASAC) created the Baseline Working Group (BWG) in July 1996 in an effort to strengthen the everyday airport security efforts in place across the nation. It was created prior to the formation of the White House Commission on Aviation Safety and Security, but its efforts were related to the recommendations of the Commission. The BWG also formed the Cargo Working Group (CWG) to specifically deal with the unique problems related to air cargo. The groups were dissolved in December 1996 when the ASAC issued the ASAC Domestic Security Baseline Final Report. The President's Commission, assembled on 25 July 1996, also

FIGURE 10.1 Air cargo being unloaded. Cargo remains a major source of vulnerability in the context of overall airport security both on cargo and passenger aircraft.

recommended that the FAA implement a comprehensive plan to address the threat of explosives and other threat objects aboard aircraft. To consolidate all the recommendations and views, the FAA requested that ASAC reconvene another CWG to be known as the Cargo Baseline Working Group (CBWG). In 1997, this group published some expanded recommendations.

Overall, the CBWG concluded that (1) the FAA should implement a comprehensive plan to address the threat of explosives and other threat objects in cargo and work with industry to develop new initiatives in this area; (2) the FAA should place greater emphasis on the work of teams such as the ASAC and the BCWG to address cargo issues. The FAA agreed with the two recommendations and had pursued further cooperative efforts with the Postal Service, the U.S. Customs Service, and the air carriers. Some important issues persist pertaining to airmail security, indirect air carriers, unknown shippers, and international cargo standards. In fact, a Department of Transportation (DOT) Inspector General report indicates security for cargo carried on passenger planes is "easily circumvented." The report describes an air cargo system that has no routine scrutiny of packages and contains serious gaps in ensuring that shippers actually follow the approval security programs (Schneider, 2002).

Unfortunately, security measures designed to prevent terrorists from placing bombs in the cargo holds of passenger planes still have huge loopholes. As previously stated, the Department of Homeland Security issued new proposed rules on 10 November 2004. Industry and interested parties had until 10 Jan 2005 to respond, and they did quite prolifically.

ARMING CARGO PILOTS

Cargo pilots say that employees with access to the planes on the ground are not screened as well as employees on the passenger side of the airport. The passenger side has a Secure Identification Display Area (SIDA). Anyone who is not escorted into that area must at all times display a badge issued by the airport authority and undergo a 10-year criminal background check that includes fingerprint checks by the Federal Bureau of Investigation (FBI). Cargo ramps are often outside the SIDA boundaries. In Memphis, a major Federal Express hub, MD-11 freighters are in an area where employees generally have not had background checks that include FBI fingerprints. The same is true in Louisville, KY, where United Parcel Service (UPS) aircraft are outside the SIDA. The cargo carriers say they perform extensive checks on employees allowed near aircraft, but cannot do fingerprint investigations unless ordered to do so by the government. Some friction between pilots and administrator's has developed, and cargo pilots are now more attuned to who is actually permitted on the plane, especially when the passengers are not employees. Pilots' ability to protect themselves and their crew is an important issue and applies to all operators of transportation vehicles. The rules have proved to be inconsistent.

In an unusual twist of fate, a 40-year-old FAA rule that allowed commercial airline pilots to be armed was inexplicably rescinded two months before the 11 September terrorist attacks. The FAA adopted the armed pilot rule shortly after the Cuban missile crisis of 1961 to help prevent hijackings of American airliners. It had remained in effect for four decades. According to the FAA, the rule required airlines to apply to the agency for their pilots to carry guns in cockpits and for the airlines to put pilots through an agency-approved firearms training course. The aviation agency said, however, that throughout the life of the rule not a single U.S. air carrier took advantage of it, effectively rendering it "moot." Why it was rescinded remains a mystery but the TSA has resisted implementation of new legislation since 11 September permitting pilots to carry weapons.

Cargo pilots will now also be permitted to carry weapons under new legislation that closes a loophole in the Homeland Security Act. A bill was introduced in the U.S. Senate in March 2003 by politically ideological opposites: Senator Barbara Boxer (D-CA) and Senator Jim Bunning (R-KY). Permission to carry weapons was originally extended to both passenger and cargo pilots in the Arming Pilots Against Terrorism and Cabin Defense Act of 2002. Previously, the language covering pilots was woven into the Homeland Security Act, which was riddled with politically motivated

attachments. One change was a one-word change covering weapons in the cockpit. The word "passenger" was inserted before the word "pilots", which effectively excluded cargo pilots from the Act. In fact, lobbyists for Federal Express Corporation (FedEx), UPS, and others led the charge for the addition of the word.

The cargo carriers would prefer never to arm cargo pilots and stand by their original approach of a ground-based systematic approach to security. Bill HR 3262 would allow cargo pilots and flight deck crew members to carry firearms and tasers. The bill has no cosponsors and as of February 2004 had been referred to the House Transportation and Infrastructure Committee's Subcommittee on Aviation and has since been implemented. Many have criticized the government's failure to pursue the program with much vigor. However, when applying standard risk assessment methods to the concept, it appears the cargo carriers are correct: arming cargo pilots will do little to protect the cargo.

The cargo industry continues to argue that weapons, including stun guns, actually pose a threat to cargo and crew. However, on 10 November 2004, Korean Air became the first carrier to receive U.S. government permission to equip jets with stun guns. They conduct about 50 flights into the United States per week. The tasers are designed to deliver an electric shock that briefly incapacitates an individual, allegedly without injuring him or her; however, deaths have been reported. In testing, the TSA fired tasers at cockpit instruments before agreeing to the fact that they did not damage a jet's complex electronic systems.

The program lost momentum when Congress decided that specially trained pilots should be armed with handguns. In a separate program initiated by the TSA in April 2003, 48 commercial passenger pilots began training in the use of .40-caliber semiautomatic pistols. Thousands of U.S. passenger airline pilots are carrying these government-issued weapons. The weapons on board the aircraft are required to be locked in cases inside nondescript bags while pilots walk through airports and if the pilot exits the cockpit at any time. The program remains voluntary. FedEx, UPS, and other cargo pilots may now also carry guns as of 1 May 2004. The first group of cargo pilots began 56 hours of training in April 2004, and those who completed the course were deputized as federal officers. Training is conducted at a law-enforcement center in Artesia, New Mexico. In actuality, fewer than two percent of passenger flights have armed pilots, said David Mackett, President of the Airline Pilots Security Alliance. The pilot group backs legislation that would encourage additional volunteers by dropping requirements such as carrying the weapons in locked boxes. The group also advocated use of armed pilots on cargo aircraft.

As stated previously, the cargo carriers including Memphis, TN-based FedEx and Atlanta-based UPS had opposed the expansion, saying weapons should be barred from being in the workplace. Regardless, the security agency is spending $25 million this year on pilot training sessions that run twice each week (Internet: http:// quote. bloomberg. com/apps/news?pid=10000103&sid=a7uf6ljzROg0&refer=us. 14 May 2004). The bill, which authorized the concept, estimated the TSA would need about $16 million in 2004 and $83 million over the 2004 to 2008 time frame. The Congressional Budget Office went on to calculate that about 25 percent of the 8000 active cargo pilots would apply for the program. The program will spend about $8000 for each pilot and an additional $500,000 to maintain a staff to manage the program. The law supersedes any local laws and permits cargo pilots to carry firearms within and across state borders and protects them from liability for certain actions.

SUICIDES

This section may initially appear to be an odd place to discuss suicide. However, passengers checking explosive or incendiary devices who are intent on killing themselves either out of depression or to make a statement is always going to pose a threat. Individuals who have decided to attempt to leave their dependents substantial sums of money by dying in an aircraft crash also present a continued

threat. Prompt investigation of such incidents has often established the death as a suicide, making most insurance policies nonpayable; however, the concept of successfully doing so continues.

Because of the potential for this type of criminal misconduct, the Air Line Pilots Association (ALPA) has vigorously objected to the availability of flight insurance in airport terminals. Insurance vending machines in airports used to be a common site but are no longer readily available in the United States. The need for greater care in writing all kinds of flight insurance remains very important. The American Express platinum card currently has an automatic flight insurance program for anyone who purchases a ticket using the card, providing the perfect opportunity to perpetrate a fraud. Certainly, attempts to commit suicide on board an aircraft are likely to continue, especially with a payable benefit of one million US dollars is at stake. Insurers, on the other hand, consider the risk small and the income potentially great. The platinum card benefit tacks on $18 price per ticket, but American Express rarely has had to pay any death benefits.

Another problem involves the psychological health of the pilots. A suicidal pilot can be as lethal a weapon as any bomb. According to the FAA, a suicidal pilot intentionally crashed an Egyptian Airlines plane into the Atlantic Ocean in 1999. Psychologists have published warning signs criteria, providing employers with guidelines to determine whether employees are indeed suicidal. Insurers need to be alert to the same warning signs. An automatic insurance machine in an airport terminal cannot evaluate any of these criteria, and does indeed provide a suicidal individual, pilot or passenger, with an unnecessarily available opportunity.

Acts of homicide should also not be overlooked. In 1955, a United Airlines DC-6B on a flight from Denver to Portland blew up minutes after takeoff. A bomb had detonated in one of the baggage compartments killing all on board. Fortunately, forensic experts were able to trace the bomb to the luggage of the mother of Jack Gilbert Graham. He had placed a bomb in her luggage and had taken out a sizable insurance policy on her life. He was eventually convicted of homicide and sentenced to death for the crime. This single occurrence literally confirmed the perceived need to ask all travelers, "Have you packed your own bags and has anyone asked you to carry a package for them?" Many people question the utility of this question. It is hard to believe under current security conditions a passenger would do this, but apparently some gullible individuals do. The TSA announced in late August 2002 that the airlines would no longer be required to ask the question; citing the lack of effectiveness of the question.

BAGGAGE TAGS

It was not that many years ago that an individual could drive up to the curb and check a bag on an airline and simply drive away. Today's security has unquestionably come a long way since that time. Baggage tags are viewed as valuable assets. Currently, baggage tags are locked up and far less vulnerable to pilferage than previously. Curbside check-in can be a fast and furious operation, especially before large flights where this service is viewed as a distinct competitive marketing feature. The traffic in and around the curbside check-in desk is often heavy, and the risk of loss is increased when skycaps are distracted. Everyone wants to check in with as little hassle as possible. Not having to drag your baggage into the terminal and through the waiting line can be a tantalizing airline discriminating feature in a very competitive business. On the other hand, the chance for fraudulent claims and unaccompanied baggage shipments are made particularly vulnerable at the curbside check-in point. It is fairly easy to snatch a tag, attach it to a bag, and expect it to be loaded, especially on a busy domestic flight. Currently, this service is unavailable for international flights and is sometimes made unavailable for domestic flights, depending on the threat. Tracking the use of all baggage tags is an essential practice. Otherwise, potentially dangerous explosives can make it to the cargo hold. For example, such a restriction was put into place at all U.S. airports for both domestic and international flights during the Persian Gulf War and immediately after 11 September. The threat was increased, and the added precaution was deemed appropriate; however for security reasons it should be standard procedure.

PASSENGER AND BAGGAGE RECONCILIATION

As already discussed, on 21 December 1988, a terrorist in Frankfurt, Germany, loaded a portable radio packed with explosives into his checked baggage on Pan American Flight 103. He chose not to travel with his baggage. The pallet loaded onto the Pan American jet containing the explosives had been consolidated in Hamburg, Germany, and contained baggage from Malta and elsewhere. The plane eventually exploded over Lockerbie, Scotland, killing all souls on board. President George Bush, Sr., subsequently created yet another President's Commission on Aviation Security and Terrorism. Based on the recommendations of the commission, U.S. carriers instituted a strict bag-matching policy to remove the baggage of any passenger who failed to actually board an aircraft. The process is fairly routine in the United States; however, not all overseas airlines and airports meet the requirement of such a program. The Joint Aviation Authorities (JAA) an associated body of the European Civil Aviation Conference (ECAC) governs this policy in Europe.

By the end of the 20th Century, 100 percent passenger and baggage reconciliation had been made mandatory for all international flights leaving U.S. airports. The system requires certification that a piece of luggage is not transported aboard an aircraft without the corresponding passenger on board. Before 100 percent matching became commonplace for departing U.S. international flights, the air carrier was only required to have security maintain control over all checked baggage. That concept, established in December 1997, was interpreted to necessitate passenger luggage matchups, x-ray screening, physical inspection, explosive detection screening, or a combination of any number of them. However, all of them were not required. New technologies have without a doubt improved the airlines' ability to match luggage to a specific passenger. Many airlines now use a computer link between the luggage tag and the boarding pass, scanning the boarding pass when the passenger begins to actually board the aircraft and matching the individual to each piece of luggage. Again, not every airline in every city has implemented these procedures.

If the airline determines that a passenger with checked baggage does not board the flight, his or her bags are located and removed from the flight. The process is known in the trade as "originating" passenger-baggage match, meaning it is accomplished at the beginning of the first leg of the flight. Unfortunately, the process does not consider any bag that may already be in the cargo hold of the aircraft. If a person exits the aircraft during a flight change of aircraft or airline, the baggage may continue without the passenger on board. Consequently, an originating passenger-baggage match system is really only a partial bag match if it does not reconcile the baggage and passengers already on board the aircraft after each and every stop. This, of course, could be administratively quite costly and time consuming. A situation similar to this was a direct contributing factor of the Pan American 103 Lockerbie crash.

As of 2008, this major vulnerability remains. The government still does not require airlines to match passengers with their checked luggage on connecting flights. It has no specific timetable to even test such a system. In Europe, checked baggage is routinely cross-matched with passenger manifests to ensure that no baggage is placed in an aircraft's cargo hold unless the corresponding passenger is on board. The U.S. government only requires that baggage be cross-matched on the originating legs of the flights. A potential bomber could therefore defeat the system by checking explosives onto a multistop flight and leaving it behind at a connecting stop.

President Clinton established the Gore Commission, which also recommended a profile selectee or random passenger-baggage match procedure until all airlines, to all destinations, could electronically track the passenger lists, boarding passengers, and baggage on all flights. Currently, the process tracks only those passengers that have been singled out for some reason or randomly selected for further scrutiny. The procedure, as mentioned previously, has been the subject of much criticism. If a particular passenger meets the profile, or is selected at random, the passenger's bags receive additional screening both by x-ray and by an explosives detection system when available. This procedure does not scan the terrorist who does not meet the profile or is not randomly selected. The Commission called for the development of a national database on passenger travel habits and

history, called the Computer Assisted Profiling System, or CAPS, which has also been discussed previously. The FAA, commenting on CAPS, revealed that "soon, if not already, airline agents who enter a passenger's name at check-in will get either a red light or a green light, depending on whether the passenger fits a targeted profile" (Scanning Equipment for Customs Searches is Set for Six Airports, 1999). The original concept proposed a database based solely on travel information; however, it could later be cross-referenced with FBI, Central Intelligence Agency (CIA), or criminal records, even though the FAA denies that this was done. This system indeed cuts down the risk. It also assumes that a terrorist is not very bright. Even though profiles are not published, their parameters can be easily guessed.

AIRPORT LOCKERS

Anytime a facility is open to the public, there exists at least a minimal threat that someone will seek to do some damage to people or assets at that facility. As already discussed, there had been a trend away from hijackings in favor of bombing either the terminal or the aircraft on the ground. Some incidents, of course, are nonterrorist connected and consist simply of criminal misconduct. An airport is like any other slice of the societal pie and is subject to the same ongoing criminal activity as any other location. For example, there is an ample amount of theft, damage to property, assault and battery, and general criminal misconduct that are daily occurrences at an open public airport terminal, including the parking lot.

An individual, who is not necessarily suicidal, but wants to disrupt the normal activities of an airport terminal, has the option of a leaving a bomb in one of the self-service lockers. Most airports have at least now moved these lockers to inside the sterile concourse. The items are at least subject to screening prior to entrance into the concourse. However, prior to such measures being implemented, a bomb exploded in a locker in 1974 at Los Angeles International Airport, killing three people and injuring more than 30 others. Again, in 1975, a bomb in a locker at La Guardia Airport in New York killed 11 people and seriously injured another 57 people. Both of these incidents took place before the government recommended more stringent rules.

The Minneapolis-St. Paul Airport (see Figure 10.2) has been testing luggage lockers that open with a fingerprint. Coin-operated lockers are located past the security check in both the Lindbergh and Humphrey terminals. The TSA originally permitted a six-month test program to include 185

FIGURE 10.2 Cargo operations at Minneapolis–St Paul airport.

biometric lockers. All rentals are limited to 48 hours. Unfortunately, many international airports retain the coin operated lockers. For example Tokyo Narita's Airport, Terminal 2, which is generally considered to be a very security-conscious operation, permits their usage. The need for such lockers at all should be analyzed. The small service they provide individuals may not be worth the risk to the public.

CONTAINER HARDENING

In 1993, the FAA was asked to study different types of technology designed to protect aircraft against certain explosives and to report back to Congress. Prior to that, the aircraft hardening program was initiated in 1991. The overall purpose of the project was to achieve systems that would protect commercial aircraft from catastrophic structural damage or critical system failure due to in-flight explosions. The program parameters focused on susceptibility and vulnerability. First, a determination of the probability that explosives of a particular nature and amount can be successfully placed on board an aircraft was to be standard. Second, the study concentrated on an estimation of the conditional probability that an aircraft will be destroyed or damaged by such a device.

According to the report, tasks were designed to determine and identify the following (Internet: http://cas.faa.gov/ reports/98harden.html):

- The minimum amount of explosives that will result in aircraft loss
- The methods and techniques that can be applied to the current and future fleets of commercial aircraft to decrease their vulnerability to explosive effects

Mitigation techniques have converged on the development of blast-resistant airline luggage-cargo containers. This technology exists, but research into other mitigation techniques still will be needed because only wide-body aircraft currently use such containers. The report concluded that it is critical to find a solution to the effects of a blast across the spectrum of aircraft being used in the airline industry. As always, the good guys will need to keep pace with future advances in criminal-terrorist explosive capabilities. The hardened container was considered to be only a near-term solution.

Currently, the LD-3 container is the most frequently used luggage container in the industry. It was extensively tested, beginning with low charge weights and increasing the amounts until failure occurred. Results clearly indicated that the blast loading was dependent on the density of the luggage that contained each explosive, exactly where the explosive was situated in the container, and what other luggage was placed around the target luggage. After extensive analysis it was decided that the containers had very little inherent blast-resistance capability. In other words, if a terrorist is successful in getting a bomb onboard, if detonated, it will likely bring the plane down.

BLAST CONTAINMENT VERSUS BLAST MANAGEMENT

Engineers have studied the effectiveness of both blast-containment and blast-management techniques. The blast-containment design attempts to completely suppress the results of an explosion within a container. The blast-management design concept considers the container as part of a placement system inside the cargo bay of the aircraft. They both have advantages and disadvantages.

Tests have determined that the blast-containment concept offers the best alternative for suppressing the potentially catastrophic effects of postblast fires. This system is also an independent unit. It stands alone and needs no special handling or placement within the cargo bay. On the other hand, the blast-management concept allows a container to essentially fail and bases its control on the ability to vent the detonation products into adjacent containers. The airline must arrange the cargo appropriately for the system to have any usefulness. This could prove to be tedious and quite time-consuming; another drawback as far as the airline is concerned. Consequently, early on it

was decided to focus on a blast-containment container to construct state-of-the-art high-strength composite materials with fragment penetration resistance and fire-retardant properties.

Full-scale tests were conducted in the early 1990s, and many LD-3-type containers were tested. The Society of Automotive Engineers assisted the FAA in developing container specifications. The FAA solicited developers for designs that would meet the established requirements for blast resistance, FAA airworthiness, and airline operational requirements. Unfortunately, in 1996, no design actually met the required specification, but later models did. The newer models will also, as is to be expected, involve a higher cost. Aluminum containers range in price from 1000 to 3000 U.S. dollars. The blast-resistant containers cost about 38,000 U.S. dollars each, at least when they were produced as prototypes. Therefore, life-cycle costs are a serious consideration in any further development of containers possessing a legitimate chance of ever seeing widespread use.

The House Subcommittee on Transportation and Infrastructure, which convened in 2000, heard testimony on blast-resistant baggage containers. Prior to that in March 1998, the FAA had approved a blast-resistant container, but as discussed they are prohibitively expensive. One estimate from the Air Transport Association projects that such containers would cost airlines 5 billion U.S. dollars a year. Additionally, the containers are only available for wide-body aircraft, which includes only 25 percent of the aircraft in service. Most aircraft are narrow-body aircraft, and 70 percent of the bombings have been directed against them (Screeners Under Fires, 2001). More recently, the National Intelligence Reform Act of 2004 (P.L. 108-458) included provisions establishing a pilot program for evaluating the deployment of blast-resistant cargo containers.

AIRMAIL SECURITY

In late 1979, an incident aboard an American Airlines flight involving a bomb inside a metal postal container prompted the FAA and the U.S. Postal Service (USPS) to sign a Memorandum of Agreement (MOA). It required that all direct and indirect carriers, including the USPS, implement an air parcel security program with procedures to prevent, detect, and deter the introduction of any unauthorized explosive or incendiary device into airmail parcels. Unfortunately, the USPS clung to the position that the airlines could never be allowed to screen the mail and that the USPS could only screen mail under very limited circumstances. The MOA proved to be unworkable.

Originally, standards for the security of mail were different from those of air cargo, which were also different for checked baggage. Carriers receive the mail from the postal service in already sealed bags, and they are marked for destination. The FAA had literally relinquished the responsibility for airmail security because the mail was sealed on receipt by the airlines. The carriage of mail by commercial aircraft constituted and continues to constitute big business to the airlines. However, following the Desert Storm military action, in January 1991, the USPS attempted to shift the shipment of most packages to "all-cargo" carriers instead of passenger carriers as a simple safety measure.

In the past, the postal service, by virtue of its own regulations, had taken the legal position that x-raying or other screening of mail "sealed against inspection" cannot be accomplished without first obtaining a search warrant. Title 18 USC Section 3263 requires the postal authorities to maintain "one or more classes of mail for the transmission of letters sealed against inspection." It also states "no letter of such a class of domestic origin shall be opened except under authority of search warrant authorized by law." Postal Service Regulations, Part 115.4 and 115.5 state that no person may "open, read, search, or divulge the contents of mail sealed against inspection," without a warrant unless extraordinary circumstances create a reasonable suspicion to an inspecting authority that a letter or parcel could be dangerous. Additionally, 18 USC Section 1702 makes it a federal crime for delaying the mailing of a letter or parcel by anyone who does so "with design to obstruct the correspondence, or to pry into the business or secrets of another, or opens, secretes, embezzles, or destroys the same." These provisions severely limit the screening of the mail prior to being loaded on board an aircraft.

In May 1994, a second MOA between the FAA and USPS was signed. The agreement improved coordination between the two agencies. The purpose of the agreement was to prevent the introduction of explosive or incendiary devices into mail parcels that could be loaded onto commercial aircraft and attempted to redefine the category of "sealed against inspection" mail. One of the vulnerabilities of screening baggage intended for aircraft rested squarely on the shoulders of the USPS. Admittedly, the history behind these regulations is lengthy. It forms part of the bedrock foundation of a democratic state. Keeping the government out of private mail is an important and fundamental right. However, like many other constitutional rights, it is not absolute. There are some justifiable exceptions, and the situation of a potential bomb on board an aircraft may constitute one of those exceptions.

As a result of an extensive review of procedures by both agencies, some revisions have subsequently been made. The USPS canceled its "airport to airport" service under which a mailer could specify a particular flight. It also began a system of weekly internal security audits under which certain "profiled" mail parcels are separated from the mail tendered to air carriers. Also, the USPS modified the Customs forms for outbound overseas parcels. These forms now require a "safety" certification for each parcel with a copy retained by the post office of origin. Since 1996, even stronger security measures have been implemented. Currently, a "profiled" parcel placed in a drop box is returned to the sender. The mailer must present the parcel in person if it is to be transported through the mail. More specifically, all mail pieces weighing over 13 ounces bearing only postage stamps as postage must be presented to an employee at a retail service counter at a post office. Canine teams, which have been advocated by industry for increased use in screening and inspecting air freight, currently provide the only means approved by the TSA for screening mail weighing more than one pound that is put on passenger aircraft under a long-running pilot program in place at 11 airports (U.S. Department of Homeland Security, 2003).

INDIRECT AIR CARRIERS

An indirect air carrier is a company that is in business for the purpose of accepting and shipping items on commercial airlines. Freight forwarders typically execute all aspects of the shipping process, from handling goods and paperwork to clearing shipments through Customs and making delivery to the end cosignee. Significant loopholes in the system opened the airlines to specific vulnerabilities when they accepted these shipments. Theoretically, a package could be forwarded through several indirect air carriers before it ever reaches an airline. This makes tracing the origin of the original shipper very difficult. FAR Part 109 was signed into law in 1979. It required indirect air carriers to develop and file for FAA approval a security program designed to "prevent or deter the unauthorized introduction of any explosive or incendiary device into any package cargo intended for carriage by air" (Internet: http://www.faa.gov/ars/ AFS/FARS/far-109.txt, 24 April 2001). The goal was to place the requirement for screening at the point of acceptance rather than put the burden on the airline.

A major problem became apparent based on the fact that the FAA did not really know the identity of most of the nation's indirect carriers. In the President's Commission on Aviation Security and Terrorism, dated 15 May 1990, it was determined that the United States had between 4000 to 6000 indirect carriers but that the FAA could only identify and track the practices of about 400 of them. Consequently, improved indirect air carrier standards were put into effect. The FAA issued a standard security program for indirect air carriers containing definitions, terminology, and requirements for the acceptance of cargo by indirect carriers. These requirements became effective in 1994 (Internet: http://cas.faa.gov/reports/98cargo/98cargo.html, pg. 6). The TSA now governs all indirect shipping, and specific administrative regulations will likely be improved and strengthened again. TSA 49 CFR, Chapter XII, Part 1548, formerly Part 109, essentially detailed the security program requirements for indirect carriers. This section requires the shipper to draft a program. Forcing both carriers and indirect shippers to implement an adequate program is another issue.

KNOWN SHIPPER

The known shipper rule prohibits passenger airlines from accepting cargo from customers that have not done business with them on a regular basis in the past unless the carrier visits the shipper's premises to ensure it is a legitimate operation. The FAA had already tightened the rule in 2000. The FAA imposed new definitions of known versus unknown shipper. Either the manufacturer must demonstrate that it has shipped at least 24 times with the same fright forwarder since 1 September 1999, or it must have completed all of the following: the manufacturer must have a customer record with the freight forwarder, it must have a shipping record of six months or longer or a formal contract with the freight forwarder; it must ship three times with the forwarder on nonconsecutive days, and the freight forwarder must visit the manufacturer's offices and fill out the form "Aviation Security Known Shipper Revalidation." The TSA had mandated that all passenger flight cargo must be screened by the 19 November deadline. However, it has yet to determine by what means. Physical inspection of all cargo would be astronomically expensive. A current loophole permits the cosignee to be considered the shipper. The industry's nightmare is for the government to ban all cargo shipments on passenger flights, much the same way it had previously banned passenger flights from carrying individual pieces of mail weighing more than a pound. Postal volumes for U.S. passenger carriers have dropped significantly, throwing airlines cargo revenues in the red. A new air cargo industry group, the Cargo Aviation Security Coalition, was created to ensure that any new security measures not put a stranglehold on air commerce. Today, the U.S. government requires all cargo companies to receive verbal confirmation from the end recipient before shipping goods. As a result, shipments are often delayed, especially when handling shipments with a time difference.

A known shipper is defined as a person or company that meets one of the two requirements listed below:

1. Shipped with the same freight forwarder or indirect air carrier (IAC) at least 24 times within the past 24 months and has been an active account with the freight forwarder since 1 September 1999
2. Meets each of the following requirements:
   a. Has a customer record (accounts receivable)
   b. Has established a shipping record with the freight forwarder or IAC of six months or longer, or have a formal contract (a formal contract may consist of the tariff signed by both the shipper and a representative of the forwarder or IAC)
   c. Has shipped three times with the forwarder or IAC on nonconsecutive days
   d. Has visited the shipper location and one of its representatives has completed an "Aviation Security Known Shipper Revalidation" form

UNKNOWN SHIPPER

Some air carriers and some IACs are still experiencing difficulty identifying unknown shippers to review all shipping documents appropriately. The government eventually extended the previous "unknown shipper" rules to all cargo and required inspection of cargo from all "unknown shippers" and known shippers. Passenger air carriers are required to obtain a Shipper's Security Endorsement and identification check for all cargo. In the past, these endorsements had only been needed for cargo from "unknown shippers." In addition, foreign air carriers and indirect air carriers were also required to obtain similar information from all shippers known or unknown and to certify each shipment had an audit trail. The FAA also had mandated air carriers to apply security controls to cargo accepted from all-cargo flights as well as passenger flights, closing yet another loophole in providing adequate security controls on cargo. Restrictions for unknown shippers as of 9 October 2002 are as follows:

- U.S. freight cannot be moved on a passenger flight.
- U.S. freight can only move on all-cargo flights subject to the carrier's acceptance.
- Shipments from the United States cannot be consolidated with the other shipments.
- Shipments from the United States have to be held for seven days after the freight forwarders complete the documentation to move them to "known shipper status."

GAO STATUS REPORT ON CARGO SECURITY 2002

The Government Accounting Office, GAO, decided to investigate the status of air cargo security in 2002. They reasoned that U.S. air carriers transport billions of tons of cargo each year in both passenger planes and all-cargo planes. Typically, about half the hull of each passenger aircraft is filled with cargo. As a result, any vulnerability in the air cargo security system potentially threatens the entire air transport system. The GAO agreed to determine the security vulnerabilities that have been identified in the air cargo system, the status of key recommendations that have been made since 1990 to improve air cargo security, and ways in which air cargo security can be improved in the near and long term.

They found numerous vulnerabilities. These vulnerabilities occur in the security procedures of some air carriers and freight forwarders and in possible tampering with freight at various handoffs that occur from the point when cargo leaves a shipper to the point when it is loaded onto an aircraft. As a result, any weaknesses in this program could create security risks. The FAA and now the TSA have implemented a number of key recommendations and mandates to improve air cargo security made since 1990 by numerous government organizations. For example, the FAA and the air cargo industry developed security training guides for air carriers and ground personnel who handle air cargo.

However, a few recommendations by those groups, such as conducting research and operational tests of technology to screen cargo for explosives, are ongoing and not yet completed by the TSA or have not been implemented. Federal reports, industry groups, and security experts have identified operational and technological measures that have the potential to improve air cargo security in the near term. Examples of the measures include checking the identity of individuals making cargo deliveries and implementing a computerized cargo profiling system. In addition, long-term improvements, such as developing a comprehensive cargo-security plan, have been recommended by the above sources, but not fully implemented by the TSA. Each potential improvement measure, however, needs to be weighed against other issues, such as costs and the effects on the flow of cargo. Without a comprehensive plan that incorporates a risk-management approach and sets deadlines and performance targets, the TSA and other federal decision-makers cannot know whether resources are being deployed as effectively and efficiently as possible in implementing measures to reduce the risk and mitigate the consequences of a terrorist attack (Internet: http://www.gao.gov/htext/d03344.html). See the full text at the Internet site on Vulnerabilities and Potential Improvements for the Air Cargo Security, http://www.gao.gov/ new.items/ d03344.pdf.

STRATEGIC PLAN OF TSA

As stated, the U.S. TSA did publicize a proposed plan in a 17 November 2004 press release. The plan responds to comments made in September 2003 by working groups of the TSA's ASAC, as well as recommendations from the GAO and the Department of Transportation's Office of Inspector General. The Strategic Plan supports the Notice of Proposed Rule Making (49 CFR Part 1540, et.al.) and is intended to complement security programs and initiatives. Transportation Security Administrator Admiral James Loy said that the main objective of the air cargo strategic plan is to provide an effective framework that does not "unduly impede the flow of commerce" (Loy, 2003).

Specifically, the TSA announced that the plan called for prescreening all cargo shipments to identify suspicious cargo, inspecting all such cargo, establishing a data base of vetted "known" shippers,

banning cargo from unknown shippers, and strengthening the security of the air cargo operating areas at airports as well as the security standards for air cargo personnel. In another 17 November 2003, news release, the TSA advised that domestic and foreign commercial planes carrying cargo will be subject to random inspections on flights within, into, and out of the United States.

The TSA maintains that the first main objective of the Strategic Plan calls for augmentation of TSA's Known Shipper Program, which prohibits air carriers from accepting cargo that does not originate from shippers who meet TSA's Known Shipper requirements. The plan provides for full deployment of the program's Known Shipper Automated Database and Indirect Air Carrier Database, which will allow the TSA and air carriers to have faster access and more thorough information on applicants for Known Shipper status and those seeking to ship cargo aboard passenger aircraft.

A second component of the Strategic Plan is the development of a cargo prescreening system similar to that used at national borders. The TSA intends to use terrorist watch lists and federal and commercial databases to identify suspicious or higher-risk shipments. From this they will develop a "risk score" for cargo shipments. The TSA is working closely with Customs and Border Protection to build on existing prescreening technology in place in the maritime industry.

The current air-cargo security strategic plan falls under legislation ongoing in Congress titled the Aviation Security Improvement Act. On 6 February 2007, the bill was introduced by Senator Inouye (D-HI) and several other members of the Senate. The bill was then forwarded to the Committee on Commerce, Science, and Transportation. The air-cargo security strategic plan was designed to create barriers for the terrorist who intended to use air cargo for devious purposes. The plan is controlled by the TSA under the Department of Homeland Security and is closely aligned with the National Homeland Security Strategy, National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, and the TSA's Strategic Plan. As the plan was developed, it was given four objectives:

- Strategic Objective 1: Enhance Shipper and Supply Chain Security
- Strategic Objective 2: Identify Elevated Risk Cargo through Prescreening
- Strategic Objective 3: Identify Technology for Performing Targeted Air Cargo Inspections
- Strategic Objective 4: Secure All-Cargo Aircraft through Appropriate Facility Security Measures

AIR CARGO STRATEGIC PLAN

November 2003

EXECUTIVE SUMMARY

This Air Cargo Security Strategic Plan sets forth TSA's commitment, as a component of the Department of Homeland Security's Border and Transportation Security Directorate, to working closely with our federal, state, local, and industry partners to ensure that 100 percent of cargo that is deemed to be of elevated risk is inspected, and ensuring that the entire air cargo supply chain is secure. In so doing, this plan addresses the security and functionality of a critical element of the nation's aviation transportation system. Like other elements of the aviation system, air cargo presents a potential risk to air travel and simultaneously underpins the economic vibrancy not just of the aviation industry, but also of the nation's high-value, just-in-time supply chain that services countless industries.

Accordingly, the air cargo security challenge is daunting, and TSA has worked with its partners in the Department of Homeland Security, including the Bureau of Customs and Border Protection (CBP), to develop an Air Cargo Strategic Plan that uses a threat-based, risk-managed approach to strengthen the security of air cargo. That work also involved reaching out to the air cargo community through

TSA's Aviation Security Advisory Committee's Cargo Working Groups. The Air Cargo Strategic Plan addresses issues raised by those industry groups, as well as issues raised in two separate reports: one by the General Accounting Office (released in December 2002), and the second by the Department of Transportation's Office of the Inspector General (released in September 2002). This plan provides a road map to realizing the Department's vision of an air cargo security system that will deny the terrorist the opportunity to exploit the air cargo system by using an optimal combination of information and technology-based solutions while preserving the high-value just-in-time air cargo supply chain.

The Strategic Plan takes advantage of a multi-layered approach to security, recognizing the benefit of grant programs and other security efforts within TSA as well as CBP's current targeting and screening activities, and other security enhancements undertaken by private industry and other governmental agencies, non-federal as well as federal. The Plan will be supported by a Notice of Proposed Rule Making, which TSA will publish in the coming months, and accompanying specific programs and initiatives.

Relying on the best available, currently operational technologies, the Strategic Plan takes a threat-based, risk-managed approach that will reach throughout the air cargo supply chain. In developing the Strategic Plan, TSA carefully evaluated the feasibility of physically screening 100 percent of all air cargo. Limitations of technology and infrastructure make such an undertaking impractical, from both a flow-of-commerce and resource point of view. For this reason, the Strategic Plan calls for the focused deployment of currently available tools, resources, and infrastructure in a targeted manner to provide effective security in the air cargo environment today, and lays out a path for accelerated research and development of even more effective and comprehensive tools for tomorrow.

TSA has tailored the air cargo security program to manage various security risks in a cost effective manner. It is based on the Department's goal of securing the air cargo supply chain, including cargo, conveyances, and aircraft, through the implementation of a layered solution that includes:

- Screening all cargo shipments in order to determine their level of relative risk;
- Working with our industry and federal partners to ensure that 100% of items that are determined to be of elevated risk are inspected;
- Developing and ensuring that new information and technology solutions are deployed; and,
- Implementing operational and regulatory programs that support enhanced security measures.
- TSA's agenda for achieving this goal can be divided into four strategic objectives:
  - Enhance shipper and supply chain security;
  - Identify elevated risk cargo through prescreening;
  - Identify technology for performing targeted air cargo inspections; and,
- Secure all-cargo aircraft through appropriate facility security measures. (http://www.tsa.gov/public/interapp/press_release/press_release.)

ENHANCED MEASURES

The Air Cargo Final Rule announced in 2006 makes permanent some practices already in place and adds others. New security measures include:

- Consolidating approximately 4000 private industry known-shipper lists into one central database managed by the TSA
- Requiring background checks of approximately 51,000 off-airport freight forwarder employees
- Extending secure areas of airports to include ramps and cargo facilities, which will require an additional 50,000 cargo aircraft operator employees to receive full criminal history background checks

These new measures are enforced by an expanded force of 300 additional air cargo inspectors hired by the TSA and stationed at 102 airports where 95 percent of domestic air cargo originates.

On 23 October 2006, the TSA issued further enhanced cargo security measures that may or may not subject cargo to inspection. The new security measures relate to air cargo directly, and indirectly require additional procedures to be implemented by several portions of the air transportation supply chain including air carriers, freight forwarders, and shippers. On 8 January 2007, the TSA issued seven new security programs to the air carriers, all-cargo carriers, and indirect air carriers that were to become effective 12 March 2007 (Internet: http://www.tsa.gov /what_we_do/layers/aircargo/07102006 changes.shtm). The new security programs involve cargo security changes that affect all modes within the air cargo supply chain.

The U.S. cargo industry has resigned itself to congressional passage of a comprehensive cargo screening bill. What the industry fears most and what has happened is that new measures mandate that all cargo shipped aboard commercial airlines be screened for explosives. The TSA has already said that screening all six billion annual pounds of cargo transported each year in the United States is "impractical from a flow-of-commerce and resource perspective." The TSA instead proposed complete screening of "elevated-risk cargo." A remaining issue involves how to screen the baggage, whether through technological means or by use of sniffing canines, or both. The TSA has been testing explosive-detection systems at San Francisco and Seattle-Tacoma international airports and ordered $40 million worth of eXaminer 3DXs from L-3 Communications. The Air Transport Association (ATA), opposed to 100 percent screening, says measures already in place, such as the known-shipper program, should be a key component of any bill. They argue that the measures also might eliminate cargo service to many small communities. Additionally, the National Industrial Transportation League says full screening would push more cargo toward the trucking industry.

According to the TSA, it claims to ensure the security of the air cargo supply chain by mandating air measures contained in the various carrier security programs that are labeled sensitive security information (SSI). Consequently, they are prohibited from public distribution. Although some of the security measures required by the carriers are visible to the public, most are carried out behind the scenes. A shipper's refusal to provide this information and consent to inspection may have the carrier refuse the shipment and decline subsequent air transport.

Concurrently, U.S. lawmakers had introduced two amendments to the 2006 Department of Homeland Security Authorization bill in May 2007. The first amendment would have made necessary the inspection of all cargo before it is shipped on passenger aircraft by 2008, and until that date, the second amendment would oblige airlines to notify passengers of unscreened cargo shipped in the cargo hold of a passenger aircraft. According to a coauthor of the amendments, 22 percent of all air cargo that is transported in the United States is loaded aboard passenger aircraft. Representatives of the airline industry argue that regardless of Congressional legislation, it is technically impossible to screen 100 percent of cargo, as it comes in various sizes and shapes. The bill calls for the TSA, within three years of enactment of the legislation, to "establish a system to screen all cargo transported on passenger aircraft or foreign air carrier in air transportation or intrastate air transportation." This "system of screening" will require that "equipment, technology, procedures, personnel, or other methods determined by the TSA provide a level of security comparable to the level of security in effect for passenger checked baggage."

The Homeland Security Appropriations Act of 2005 (P.L. 108-334) had already called for tripling the amount of cargo that is screened or inspected on passenger airplanes; however, the absolute number or percentage of cargo subject to inspection is considered security sensitive. Fiscal year 2006 appropriations language (P.L. 109-90) directed the TSA to take all possible measures including the certification, procurement, and deployment of screening systems to inspect and screen air cargo on passenger aircraft and increase the percentage of cargo inspected beyond the level mandated in the fiscal year 2005 appropriations measure. Further, fiscal year 2007 appropriations language (P.L. 109-295) directed the TSA to work with industry stakeholders to develop standards and protocols to increase the use of explosives detection equipment for screening air cargo.

Opposers and industry representatives to the bill have commented (http://www.airforwarders.org/airmails/020707.html; retrieved 11 Aug 2007):

SUMMARY OF AIRFORWARDER'S ASSOCIATION OBJECTIONS

- *Three years*: We continue to be very concerned about the rapid phase-in required in both bills. Unlike the House bill, there are no year-by-year benchmarks but just a goal of "all cargo in 3 years." The effect, however, will likely be the same — bottlenecks, delays, and expensive upgrades in a very short period of time that may dramatically impact our industry's ability to do business. We have expressed these concerns and will continue to work with the Senate on this provision.
- *System to screen*: This language differs from the "inspection" used in the House bill. We believe that the use of the term "screening" is an improvement and a result of the supply chain's tireless efforts to advance the multilayered risk-based approach. After many conversations with the TSA and Congress, we believe that "screening" embodies the risk-based approach in that it relies on threat assessment rather than "inspection," which we interpret as solely physical or technology-based solutions that treat all cargo at the same level of risk.
- *Equipment, technology, procedures, personnel, or other methods determined by the TSA*: This is far more expansive than just the technology or physical inspection provisions of only a year ago. This is also broader than the House language, in that it includes "other methods." We believe this flexibility given to the TSA will serve our industry well, as the TSA will have the authority to certify certain methods. The TSA's vetting process for new procedures, technology, and equipment have been rigorous to date, and we expect that same level of attention to detail and advocating only policies that are proven to be effective and efficient to continue.
- *Comparable to the level of security in effect for passenger-checked baggage*: We are concerned about this provision as well. The House bill required "equivalent" levels of security —we believe comparable is better in that it begins to outline that baggage and cargo are not the same and should not be treated the same. However, the language is not clear on this matter and needs to be articulated in a way that the TSA cannot interpret as meaning only methods for baggage screening (technology and by hand) are able to achieve a comparable level of security. That would erase the positive gains made in the inclusion of other forms of screening outlined above. We are working on clarifying this with Senate staff.
- *Cost*: The cost is still not explained in the bill. The estimates for the air cargo portion in the House version are around 3.7 billion U.S. dollars over five years—and the House Democratic leadership said that private industry would have to foot the bill. We believe that Congress has agreed to take on the responsibility of homeland security policy and the costs associated with it, and therefore object to user fees, taxes, or additional cost burdens put on the supply chain.)

THE LATEST

At the beginning of the 110th Congress, the House passed H.R. 1, which includes a provision that would require 100 percent screening of cargo placed on passenger aircraft by the end of fiscal year 2009. Specifically, the provision would phase in the percentage of cargo required to be screened, setting these levels at 35 percent by the end of fiscal year 2007, 65 percent by the end of fiscal year 2008, and 100 percent by the end of fiscal year 2009. "The vulnerability of both air and maritime cargo to terrorist attack is well known," said Rep. Ed Markey (D-MA). "Most of the six billion pounds of cargo carried on passenger planes every year is loaded on board without being scanned for liquid, plastic, or conventional explosives. And most of the maritime cargo containers bound for the United States is not scanned for nuclear bombs before being loaded onto ships." Of the 11 million ship-carried cargo containers that arrive at U.S. ports each year, only roughly six percent are randomly inspected, although Customs and Border Protection's Automated Targeting System and other

FIGURE 10.3 The TSA announced a new canine program to enhance explosives detection capabilities in air cargo facilities nationwide. (Source: Transportation Security Administration. www.tsa.gov)

measures are supposed to identify "high-risk" cargo to be singled out for inspection (http://www.hstoday.us/Congress/House%20of%20Representatives/20070109_House_Passes_Landmark_Air_Ship_Cargo_Screening_Legislation.cfm?storyid=5276; retrieved on 11 August 2007).

The TSA has consistently contended that requiring inspection of all cargo on passenger planes could potentially make them more vulnerable to terrorist attack. In his first public comments on a bill approved by the House 9 January 2007, TSA chief Kip Hawley said inspecting all passenger-plane cargo would add "a very small, incremental benefit for security." Hawley said it also could divert airport screeners from other activities such as screening airport employees, inspecting passenger travel documents, and looking for suspicious travelers. The House bill aimed at strengthening domestic security would have required the cargo to get the same screening as luggage by October 2009 (Internet: http://www.usatoday.com/travel/ news/2007−01−17−tsa−cargo−sec urity.x.htm.). In addition to these measures, the TSA has been provided with appropriations to hire more cargo inspectors and canine teams to step up screening and regulatory inspections of air cargo security (see Figure 10.3). The TSA is also planning on deploying a freight assessment system to evaluate cargo risk and target shipments for detailed inspection.

VACUUM CHAMBERS

Vacuum chambers can be employed by airlines and airport authorities to minimize the dangers of barometrically detonated bombs. Before loading the aircraft, air cargo is introduced into a vacuum chamber. The flight sequence is simulated in the chamber, and the cargo is subjected to the varying air pressure expected during a normal flight. Flight details are fed into a computer that activates the chamber. Monitoring can be done locally or at a remote site.

INSPECTION OF HAZARDOUS CARGO

The tragic loss of Valujet Flight 592, 11 May 1996, drew attention to the tremendous growth in the shipment of air cargo. Within weeks of the accident, the FAA formed a task force to review the FAA's hazardous materials and cargo security enforcement programs. A new cargo security and dangerous goods program emerged. It was organized into nine domestic regions and one European region. Inspectors assigned to the program are still located at over 38 field offices in the United States as well as in three international field offices. Directed by a headquarter's staff, agents monitor the regulatory compliance of hazardous materials, shipments, and shippers throughout the

transportation chain by inspecting passenger and "all-cargo" air carriers. They also conduct concurrent cargo security inspections to ensure that all relevant cargo security measures are being applied to all types of cargo.

The FAA had combined its cargo security and hazardous materials inspection activities into a specialized discipline and staff. Authority was eventually granted to hire over 100 specialized cargo inspectors. The program focuses on inspection and testing, trend analysis, and outreach to the shipping community. Inspections are supposed to be more in depth than those now being conducted by the generalized work force. The FAA had also developed a number of courses for newly hired personnel. One course, the Cargo Security Basic Course, is standard for all personnel that are tasked with inspecting cargo. The course was developed to familiarize the newly hired cargo security and dangerous goods inspectors with the regulatory requirements placed on domestic and international shippers, and on air carriers who submit and accept freight for air carriage.

As is often the case, a disaster can prompt significant inquiry into needed safety and security issues. The loss of Valujet Flight 592 also forced officials to recognize the tremendous growth in air cargo shipments and the increase in hazardous materials incidents involving air transportation. The government stepped in and created a commission to investigate the FAA's hazardous materials and cargo security enforcement programs. The screening of cargo on "all cargo" carriers is just as important as air passenger flights. There are fewer humans on board, but since when do we as a society believe that it is fine to negligently kill an aircrew so long as there are no passengers on board?

INTERNATIONAL CARGO STANDARDS

The security plan of the International Civil Aviation Organization (ICAO) is contained in Annex 17. EU Regulation 2320/2002 and ECAC Document 30 which also contain applicable cargo regulations. The security plan addresses all aspects of security, but particularly addresses cargo and mail transported on international passenger flights. Chapter 4 of Annex 17 establishes controls for cargo and mail and recommends that all governments ensure that freight forwarders are also part of a security program. U.S. airlines operating outside the United States have only the security procedures carried out by freight forwarders in countries adopting the ICAO recommendations to rely on. There is no guarantee or even calculated risk that what is loaded in Bombay, Hong Kong, Lagos, or Brussels is safe. U.S. carriers must totally rely on foreign airports and freight forwarders to enforce the requirements of Annex 17. The TSA can advise and suggest but has no real jurisdiction over the operations of foreign airports. To enforce regulations in the United States, they can assess civil penalties and push a particularly egregious situation into the federal courts.

TSA INSPECTION OF AIRPORTS

The FAA has begun to publish a quarterly report of enforcement actions against regulated aviation entities when a civil penalty, suspension, or revocation had been issued. The data is directly compiled from the agency's Enforcement Information System. The text below will review the actions that can be taken by the government against carriers or airports that have committed cargo-related or security violations. Most of the incidents are hazardous-material related, but they still serve to illustrate the inspection criteria and the discrepancies that sometimes are discovered by an inspection.

The government has the authority to issue orders assessing civil penalties of up to $50,000 for violations of its regulations. A single violation can cost an airline up to $11,000 per discrepancy.*

Once a decision has been rendered, decisions to assess a penalty can still be appealed to both the administrative law courts and directly to the administrator. Much negotiation can take place between the regulated entities and the government and usually does. An entity may reach a settlement with

* *Note*: Due to the dangers associated with hazardous materials, there is no $50,000 limitation on assessments for violations of the Hazardous Materials Transportation Safety Act or accompanying regulations.

the administration, and if the adjudication is less than $50,000, no violation is made a part of the entity's enforcement record. Hence, the regulated entities have a real incentive to settle. Any negotiated settlement is a success because the ultimate goal is to seek compliance. Nonnegotiated violations may still be referred to the U.S. Attorney for prosecution in U.S. District Court. It is rare but does happen.

In addition to the assessment of civil penalties, the government has several other alternatives available as deterrents. They can also issue certificates of suspension and revocation. Suspensions of indefinite duration are issued to prevent a certificate holder from exercising the privileges of a certificate, pending demonstration that the certificate holder meets the standards of a certificate holder, including security standards. Certificate revocations are issued when the government determines that a certificate holder is no longer qualified to hold the certificate at all. Fixed-term suspensions are intended to discipline the offender and to deter others from doing the same. For example, on 10 May 2001, the FAA proposed to assess a civil fine of $95,000 against KLM Royal Dutch Airlines for an alleged hazardous materials violation. Supposedly KLM shipped an oxygen generator, which was not declared, nor was the crew informed of the cargo. Last, the generator packing did not meet specifications (FAA Office of Public Affairs, Press Release, 10 May 2001). According to regulations, KLM had 30 days to respond to the FAA and did so. In a similar situation, the FAA on 3 May 2001 proposed to assess a fine of $235,000 against Trans-Brasil Airlines Inc. (FAA Office of Public Affairs, Press Release, 3 May 2001). They also responded as was their right. It must be reiterated that the purpose of the inspection rules and enforcement tools are to prevent the shipment of dangerous or hazardous materials. Just assessing fines is not an adequate deterrent to breaking the rules.

After an initial civil assessment, there is an opportunity for informal procedures to resolve the issues. Correcting the deficiency and resolving the problem is the most important factor. Full litigation of each and every case is just too expensive and does not really address the preeminent goal of the regulations, which is compliance. Realistically, litigation is generally punitive in nature. Consequently, the FAA frequently issues compromise orders and agrees to consent agreements so long as the airline has corrected the deficiency and projects a positive attitude toward future compliance.

CONCLUSION

In October 2000, the FAA conducted a special nationwide assessment of U.S. carrier compliance with legislated cargo security procedures. Unfortunately, inspectors repeatedly found that airlines often failed to comply with requirements specifically related to cargo acceptance, screening of cargo, training of screening personnel, and maintenance of training records for cargo acceptance and screening personnel. Violations took place all across the nation. In accordance with the Sensitive Security Information rule, the government does not release such information for 12 months after the events occur to avoid divulging potential vulnerabilities to terrorists. The area of cargo security continues to be a challenging one and will remain so for many years to come. Hopefully, the current security situation will motivate both administrators and the public to pursue ongoing improvements in cargo-related security.

Additionally, advancements in technology relating to blast containment or blast-resistant containers for use onboard aircraft will not solve the problem of explosives on board. Nor should the possible feasible improvement of containers be ignored because the containers may potentially cost too much. The key is to combine efforts to contain a blast in conjunction with measures to prevent the bomb from reaching the cargo hold in the first place. Regulations pertaining to airmail are another matter of continuing concern. Regardless of the fundamental right of privacy of the mail and an individual's innermost thoughts, the law prohibits putting a bomb in the mail as well. Consequently, cooperation between the airlines and the U.S. Postal Office needs to be ongoing. Another significant and continuing problem is the acceptance of cargo from an unknown shipper. Requirements to maintain an audit trail and to pinpoint the place of responsibility for screening the cargo at the point of acceptance will greatly improve security procedures in this area. However,

the solution must be international and not just domestic. This presents a gigantic diplomatic challenge, but one that must be mastered if both international and domestic air travel is to be protected. Furthermore, attention must also be given to increasing the security of cargo, but not at a cost that makes air cargo noncompetitive with ocean-going cargo.

REFERENCES

FAA Office of Public Affairs, Press Releases, 10 May 2001.
FAA Office of Public Affairs, Press Releases, 3 May 2001.
http://cas.faa.gov/reports/98cargo/98cargo.html, pg. 6.
http://quote. bloomberg. com/apps/news?pid=10000103&sid=a7uf6ljzROg0&refer=us. 14 May 2004.
http://www.airforwarders.org/airmails/020707.html; retrieved 11 Aug 2007.
http://www.faa.gov/ars/ AFS/FARS/far-109.txt, 24 April 2001.
http://www.gao.gov/htext/d03344.html.
http://www.hstoday.us/Congress/House%20of%20Representatives/20070109_House_Passes_Landmark_Air_Ship_Cargo_Screening_Legislation.cfm?storyid=5276; retrieved on 11 August 2007.
http://www.tsa.gov/public/interapp/press_release/press_release.
http://www.tsa.gov /what_we_do/layers/ aircargo/07102006 changes.shtm.
http://www.usatoday.com/travel/ news/2007–01–17–tsa–cargo–sec urity.x.htm.
Vulnerabilities and Potential Improvements for the Air Cargo Security, http://www.gao.gov/ new.items/ d03344.pdf.
Loy, James, "U.S. Plan Urges New Measures for Air Cargo Security," Bureau of International Information Programs, U.S. Dept. of State, 18 Nov 2003. http:usinfo.state.gov.
"Scanning Equipment for Customs Searches is Set for Six Airports," *Wall Street Journal*, 3 Aug 1999.
Schneider, Greg, "Terror Risk Cited on Passenger Jets," *Washington Post*, 10 June 2002, pg. A01.
Screeners Under Fires, http://www. security mangement.com/library/000855.html, pg 3, 11 July 2001.
U.S. Department of Homeland Security, Transportation Security Administration. "TSA Canine Teams Screen U.S. Mail for Explosives - Pilot Program to Expand to Airports Across the Country." Press Release 03-34, May 29, 2003.

11 Security and the Rules of Law — A Slippery Slope

NEWS

13 Nov 2001: President Bush signs a Military Order pertaining to the detention, treatment, and trial of certain noncitizens as part of the war against terrorism. The order makes clear that the President views the crisis that began on the morning of 11 September as an attack "on a scale that has created a state of armed conflict that requires the use of the United States Armed Forces (Military Order, November 13, 2001, Detention, Treatment, and Trial of Certain Non- Citizens in the War Against Terrorism, §1(a), 66 Fed. Reg. 57,833).

13 February 2002: John Walker Lindh, aka Suleyman al-Faris, is taken into custody in Afghanistan. He is charged with: (1) engaging in a conspiracy, while outside the United States to kill nationals of the United States outside of the United States, namely, United States nationals engaged in the ongoing conflict in Afghanistan; (2) providing, attempting to provide, and conspiring to provide material support and resources to designated foreign terrorist organizations, namely, al'Qaeda and Harakat ul-Mujahideen; and (3) engaging in prohibited transactions with the Taliban.

Spring 2002: Some flight attendants are reporting that they are the targets of abusive behavior, including illicit touching by security at the Phoenix and Raleigh-Durham International Airports.

23 April 2005: Trying to distance himself from the terrorist attacks of 11 September 2001, and a potential death sentence, Zacarias Moussaoui describes how he sought to crash a jetliner into the White House. Moussaoui, an al Q'aeda member who was arrested less than a month before the attacks after raising suspicions at a flight school, pleads guilty to all six terrorism conspiracy charges against him.

2008: President Bush says that the House Democrats' version of a terrorist-surveillance bill would undermine the nation's security and that if it reaches his desk, he will veto it. During a press conference at the White House, President Bush tells the House to have the Senate version of the Foreign Intelligence Surveillance Act on his desk before the Easter recess.

INTRODUCTION

Two years after the Algerian terrorist hijacking of a French aircraft, the police were still dealing with the unease related to the anniversaries of the incident. French law enforcement responded with a massive security operation. On a single day in December the police stopped and questioned 6000 people. These French identity checks are similar to U.S. "stop and frisks" and have similar goals. Both are tools used by the police to prevent crime. However, French law is distinctly different from U.S. law, which must conform to the mandates of the Fourth Amendment of the Constitution under such circumstances. French procedures have been highly effective and bear review within the

context of combating terrorism internationally, although many would ague they would not survive judicial scrutiny in the United States.

Under French law, the police are not required to have a reasonable suspicion that criminal activity is about to take place or to establish imminent danger to do a weapons frisk. Additionally, an individual stopped by French police may be detained for up to four hours based solely on police discretion. Such is not the case in the United States, and if applied to airports in the United States would certainly raise the ire of many passengers and constitutional advocates. To understand the intricacies of U.S. law, students must understand that airport security officers and police officers do not have absolute freedom in carrying out their duties, even when a law has clearly been broken.

The balance between the need for effective law enforcement and for the protection of the rights of individuals remains a controversial issue. Many security officials feel that the U.S. courts have gone too far in protecting the rights of accused criminals. On the other side, critics feel strongly that police have been given a dangerous amount of leeway in exercising police powers. Many years ago, in the majority opinion of Mapp versus Ohio, Justice Tom Clark wrote, "Nothing can destroy a government more quickly than its failure to observe its own laws." (376 US 643, 1961 pg. 649). The government contends, however, that due to the magnitude of the danger caused by air piracy that searches of boarding passengers need to be based on either mere or unsupported suspicion.

The courts have faced unique challenges since 11 September 2001 as well. No one has ever stated that being a federal judge is an easy job. However, the jobs of U.S. District Court Judges Leonie M. Brinkeman and T.S. Elliot III took on aspects of particular complexity. They were assigned the cases of John Walker Lindh and Zacarious Moussaoui, respectively. For example, Judge Ellis was faced with the prickly task of balancing Mr. Lindh's Sixth Amendment right of confronting the witnesses against him versus the government's interests in protecting its security personnel and the integrity of the detainee system in Guantanamo Bay. Meanwhile, Judge Brinkeman was forced to deal with the defendant's "in court" request to represent himself. The judge felt it was necessary to issue a four-page written order educating Moussaoui on the proper procedures to file motions under seal and *ex parte*. The judges had precious little precedent upon which to base rulings. However, Moussaoui eventually pled guilty in April 2005 in an effort to distance himself from the 11 September hijackers and to avoid the death penalty.

The legal issues have spurred significant emotional debate. For example, a petition circulated referencing Title 8 of the U. S. Code, Section 1481(a)(3) which states that American citizenship may be lost thusly:

> A person who is a national of the United States whether by birth or naturalization shall lose his nationality by voluntarily performing any of the following acts with the intention of relinquishing United States nationality [by] entering, or serving in, the armed forces of a foreign state if such armed forces are engaged in hostilities against the United States.

The argument has been made that American citizens that fight in the Islamic terrorist cause should lose their citizenship. In fact, groups have vehemently argued that John Walker Lindh, who copped a plea for 20 years of confinement, received too light a sentence. The process of criminally prosecuting Americans and foreigners under the U.S. Constitution has presented some distinctive and contentious issues to the federal bench. A great deal has changed both in the makeup of the courts and public opinion in the last few years regarding all sorts of cases relating to terrorism. New precedent is being decided on a regular basis.

The controversies have extended to Presidential orders, especially the one dealing with military tribunals. Since 2002, hundreds of terrorism suspects have been held at the U.S. detention facility at Guantanamo Bay, Cuba, without charges or trials. The Supreme Court in 2006 in a straightforward decision struck down the military commissions President Bush established to try suspected members of al'Qaeda. The court emphatically rejected President Bush's antiterrorism measure and the broad assertion of executive power on which the president had based it. The majority of the

court simply ruled that that the commissions, which were outlined by Bush in a military order on 13 November 2001, were neither authorized by federal law nor required by military necessity, and ran contrary to the Geneva Conventions.

To start the litigation, Usama bin Laden's former personal chauffeur, Salim Ahmed Hamdan, claimed that his trial by a military commission violated his rights under the Geneva Convention and that President Bush violated the constitutional provision allowing Congress to form tribunals below the Supreme Court. As a result of the Supreme Court decision, no military commission can try Salim Ahmed Hamdan or anyone else, unless the president does one of two things: operates the commissions by the rules of regular military court-martial, or asks Congress for specific permission to proceed differently. "[I]n undertaking to try Hamdan and subject him to criminal punishment, the Executive is bound to comply with the Rule of Law that prevails in this jurisdiction," Justice John Paul Stevens wrote in the majority opinion (*Hamdan v. Rumsfield*, 548 U.S. 557 [2006]). The decision strongly limited the power of the Bush administration to conduct military tribunals for suspected terrorists imprisoned at the U.S. naval base in Guantanamo Bay, Cuba, but did not address the government's right to hold them there. Hamdan has now been tried and convicted but according to some critics, he received a relatively light sentence.

Although the decision addressed only military commissions, legal analysts said its skeptical view of presidential power could be applied to other areas such as warrantless wiretapping, and that its invocation of the Geneva Conventions could pave the way for new legal claims by detainees. Certainly this is not the scenario the President envisioned when he unveiled the military commissions as a tough-minded alternative to the civilian trials that the Clinton administration had used against terrorists. As first outlined in 2001, the commissions did not give defendants a presumption of innocence or guarantee a public trial.

Justice Stephen G. Breyer wrote in his concurring opinion, "Where, as here, no emergency prevents consultation with Congress, judicial insistence upon that consultation does not weaken our Nation's ability to deal with danger. To the contrary, that insistence strengthens the Nation's ability to determine—through democratic means—how best to do so. The Constitution places its faith in those democratic means. Our Court today simply does the same." Joining Stevens and Breyer in the majority were Justices Anthony M. Kennedy, David H. Souter, and Ruth Bader Ginsburg. Closer to the average traveler's daily life, this chapter will examine more specifically the measures taken and extent to which the Constitution and legal precedent regulate the conduct of security officers and the police at airports.

FOURTH AMENDMENT

The Fourth Amendment reads,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Constitution, U.S. Government Printing Office, 1989-249-097).

The Amendment itself needs to be broken down into two critical elements. First, the amendment contains a prohibition against unreasonable searches and seizures, and second is the requirement of probable cause to issue a warrant. Case law has limited the first element to the right to be secure against unreasonable searches and seizures by government agents. The courts have yet to designate airport security officers, acting within specific parameters, as government agents. Consequently, if no search or seizure occurred or if it was done by a private entity, such as airport security, it is not even necessary to determine whether it was reasonable under the Fourth Amendment (*U.S. v. Morgan*, 774 F.2d 1215 [6th Circuit, 1985]). Basically, to a certain extent airport security officials, when not considered agents of the state, are not technically subject to the restrictions of the Fourth

Amendment. If airport security officials are considered to be functioning in the place of state agents, the constitutional protections may again be applicable. Because the FAA required airlines to institute security procedures to screen passengers (14 CFR Sec 108), some courts have reasoned that "the government's involvement in promulgating the FAA guidelines to combat hijacking is so pervasive as to bring any search conducted pursuant to that program within the reach of the Fourth Amendment" *(U.S. v. Ross*, *32* F.3d 1411, 1413 [9th Circuit] quoting *U.S. v. Davis*, 482 F.2d 893, 904 [9th Circuit, 1973]).

However, once it has been determined that a search has been done by the government, the Fourth Amendment requires that the search must either have been supported by a warrant or that it must fit into a few specifically and well-delineated exceptions. Airport searches, if they are determined to be searches in the context of the Fourth Amendment, must fit into one of three established exceptions applicable to the airport security context: the administrative search exception, the stop and frisk exception, or the consent exception. Depending on the circumstances, other exceptions to be discussed include exigent circumstances or a search incident to a lawful arrest based on probable cause.

ADMINISTRATIVE SEARCH EXCEPTION

The Supreme Court has upheld a rather broad range of searches and seizures even when they are conducted without the usual apportionment of probable cause. Collectively, the court cases reflect two kinds of departures from the traditional probable cause requirement. One situation, as in *Terry v. Ohio*, 392 U.S. 1(1968) is to require individualized suspicion or reasonable suspicion less compelling than that needed for arrest. The other kind of exception is to require no reasonable suspicion at all, but instead to require that the search be conducted pursuant to some neutral criteria, which guards against arbitrary selection of those subjected to such procedures and which also serves a public purpose. Those searches have become known as administrative searches.

Administrative searches are justified on the basis that they serve a societal purpose other than the standard criminal law enforcement aim of detecting contraband. An example of an administrative search held to fall within those guidelines is the situation illustrated in *Veronia School District 47J v. Acton*, 115 S.Ct. 2386, 1995. The administrative search exception enables, in this case school officials, to exercise search authority toward select groups of individuals simply because society deems it necessary and appropriate. The case upholds drug testing in schools and notes the importance of limiting the searches to those athletes where the risk of physical harm is particularly high. The court specifically stated that "by choosing to go out for the team voluntarily, student athletes subject themselves to a degree of review even higher than that imposed on students generally" (115 S. Ct. 2386, 1995:2392). This argument lends itself to the theory that passengers choose to fly instead of travel by other modes of transportation.

The Supreme Court is particularly sensitive to the exact nature of the search. In evaluating the appropriateness of these searches they have often focused on the invasiveness of the search. In supporting drug testing of the students, Supreme Court Justice Antonin Scalia stated, "…the student enters an empty locker room accompanied by an adult of the same sex. Each boy produces a sample of urine while remaining fully clothed with his back to the monitor who stands approximately 12 to 15 feet behind the student…no less privacy than in a public restroom" (115 S. Ct. 2386, 1995:2388).

In determining whether a particular search falls within this exception, the courts first evaluate in detail the privacy interests being violated. The first hurdle is to determine whether a search scheme falls into the administrative search exception by balancing the privacy interests sacrificed against the societal purpose or the need for which the search scheme was undertaken. It must still be determined whether the special need could have been met in a less intrusive manner and whether the particular search was really made pursuant to the special need. If it meets all these criteria, then society as a whole has agreed that the threat is worth giving up the Fourth Amendment rights of certain citizens under certain circumstances. In the case of drug testing at schools, the governmen-

FIGURE 11.1 The U.S. Senate passed the U.S. Patriot Act in October 2001. Only one senator opposed it.

tal need to detect and prevent drug usage among athletes outweighs the Fourth Amendment rights of the students.

As regards airports, the issue is whether the government's need to detect and prevent terrorist acts implemented by airline-paid security officers, and soon federal employees, outweighs the Fourth Amendment rights of passengers. So far, the courts have determined that it does. Relying on the rationale of the Terry case, the court balanced the competing interests of law enforcement in the context of the current air piracy problem against the rights of individuals choosing air travel. They decided that airport searches could legally be conducted under less stringent standards than ordinary probable cause.

BALANCING APPROACH

The challenge of airport security officials is to figure out when the courts will conclude that the intrusiveness of the search is equally balanced against the level of the threat from hijacking and is therefore acceptable. The nature of the security interest will change according to the perceived threat level. If the passengers and subsequently the courts believe that the public need for protection against terrorist activity is greater than the preservation of Fourth Amendment requirements; airport searches will likely continue to be deemed appropriate (see Figure 11.1).

Another factor balanced against those special needs of the government is the nature of the privacy intrusion. For example, at airports, "the intrusion is not insubstantial, it is inconvenient and annoying and in some cases it may be embarrassing and at times even incriminating" but it is reasonable (*U.S. v. Skipwith*, 482 F.2d 1272, 1973*).* Skipwith has held in the case of airport searches that once the passenger enters the screening process, they forfeit the right to withdraw. Generally the passenger cannot withdraw simply because the search discloses items they did not want discovered, regardless of a Fourth Amendment challenge. In the context of reasonableness, the Skipwith case involved a man convicted of possession of cocaine. He had presented himself at an Eastern Airlines boarding gate in Tampa, FL. Clearly, the gate was a place at which he knew or should have known

that he was subject to being searched. His only reason for being at the gate was to board the aircraft. An officer approached him because of his suspicious conduct and an apparent bulge in his pants that the officer thought could have been a gun. Cocaine was discovered, and the defendant contested the legitimacy of the search. The court ruled that it had become general knowledge that citizens boarding planes are subject to special scrutiny and to weapons searches. Consequently, they determined that the defendant had little if any expectation of privacy and that the search was reasonable.

However, it is interesting to point out that the privacy issue has many aspects. For example, strip searches at schools, in prisons, and of airline passengers all present a variety of unique and distinct legal issues. All three may be legal under certain circumstances. The difference between them stems from the fact that all three classes of individuals — students, prisoners, and airline passengers — have much different and sometimes higher expectations of privacy than others. Based on these expectations, the level of the perceived threat is crucial in determining what the acceptable levels of the searches will be. Prisoners clearly have a much lower expectation of privacy than an airline passenger does. Consequently, more intrusive passenger screening might not be acceptable if the government's need for ensuring air travel security can be met through less intrusive means. On the other hand, if the threat is high for a specific airport, a specific aircraft, or a whole nation, extra intrusiveness may be quite appropriate. For example, passengers seem more amenable to the very stringent requirements of El Al Airlines, especially when the aircraft is flying directly to and from Israel. Passengers flying from Minneapolis to Honolulu are much less patient with extra security.

LESS INTRUSIVE ALTERNATIVES

The courts generally have upheld the idea that a security search must be limited as is consistent with the administrative need that justifies it *(U.S. v. $124,570 U.S. Currency*, 164 F. 3d 462 [9th Circuit, 1989]). If the same level of security can be maintained with a less intrusive means of search, the less intrusive means must be used. Newer technologies will have to be evaluated in these terms. For instance, to justify a passenger-screening technology that produces an image of the passenger's body beneath their clothes, the privacy of the individual must be protected as much as possible. Future security measures will also need a guarantee that the image data will neither be preserved nor archived.

No matter what the new technology, questions may arise about whether a particular search was appropriately conducted toward the legitimate objective. The human factor can change the appropriateness of any search. Regardless of the approval of the courts to a specific procedure or specific piece of equipment, an individual who steps outside the bounds of the procedure or the intended use of the equipment may still invalidate the search. Training and experience are critical to the effective and legal use of aircraft passenger screening.

The basic administrative search exception that has been extended to airports, however, is specifically limited to the search for objects, which are a threat to the airport or aircraft. Other contraband, including drugs and currency, are technically not the appropriate goal of the search. However, no matter how narrowly a device or procedure is tailored to detecting safety-related concerns, other information will still be obtained in the process. The search procedure in use therefore may yet be acceptable for the confiscation of other contraband, if the additional information is acquired inadvertently. When the information is sought specifically, however, and no concurrent safety rationale is given, the search no longer falls under the exception. A much-discussed topic is the illegal transportation of narcotics. It must be remembered that a plane cannot be easily hijacked by waiving a bag of marijuana at the pilot. Nor will a briefcase filled with cash convince most pilots to divert an aircraft. It raises the question whether airport security needs to be searching for these objects. It also raises the inquiry of the legality of police to pay airport security officers, who are already underpaid, to inform on potential drug smugglers.

The fine point of this debate is whether information on a nonthreat object is obtained in the course of the strict search for threat objects or whether action has been taken in the course of the search to

broaden the scope to include a search for nonthreat but illegal or suspicious objects. For example, invasive searches are authorized only of persons who repeatedly set off metal detector alarms. Security personnel in some cases may even conduct an "intimate search" of such persons until the suspicion is dispelled (*U.S. v. Roman-Marcon*, 832 F. Supp. 24, 1993). In the Roman-Marcon case, the defendant passed through a magnetometer, and, as he passed, the machine set off an alarm. Instead of remaining at the checkpoint for further screening, he kept walking. He was detained by a police officer, patted down, and packages of narcotics were found. However, the search was initiated because of an alarm from a metal detector. Because metal is the prime indication of a weapon, which can be an effective instrument with which to hijack an aircraft, the search fell within the administrative search exception to the Fourth Amendment requirements. Generally, where there is an indication of the presence of metal, the security personnel may frisk the individual.

INDIVIDUAL STOP AND FRISK SEARCHES

A stop and frisk exception to the Fourth Amendment requirement for a search warrant occurs when an officer or another authority has a reasonable suspicion that another person is a threat. In the context of airport passenger screening, reasonable suspicion might be that the subject fits the profile of a typical hijacker, that the screener observed something unusual or that a metal detector set off an alarm. Again, quoting the decision in Terry, a warrantless search was deemed reasonable when "a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger" (392 US 1: 27, 1968). Courts since that time have also analyzed the reasonableness of searches based on profiles. It would seem that current law would allow a stop and frisk search if an individual fits a narrow class of suspicious persons who are part of a "selectee" class search.

However, such procedures are subject to rigorous judicial scrutiny. A case in point occurred in 1997, in Florida. An off-duty police officer, working for the Miami-Dade county police, pulled over a car on the Florida turnpike. The police testified that the car was pulled over because it had changed lanes without properly signaling. In the course of the stop, a fight broke out. At trial, the accused, Aaron Campbell, alleged that the officers had really used a drug courier profile to make the decision to stop him. The judge agreed. ("Jury's Mixed Verdict in Cop Trial," UPI Online, 3 April 1998).

In essence the court determined that the officers had stopped Campbell not because they had a reasonable suspicion that he had broken a law but because they had a "mere suspicion" based on the drug courier profile. Such profiling has adamant supporters on both sides. In a legal stop and frisk, law enforcement officers may briefly detain a person they reasonably believe to be suspicious, and if they believe the person to be armed, proceed to pat down or frisk that person's outer clothing (Hess and Wrobleski, 1997).

Again, it must be remembered this case law is directed at government officers, whether they are local, state, or national and not private security employees such as former contract airport security. When a "passenger" can be stopped and frisked has opened up a whole new series of case law. This too may change in light of the airport screening function becoming the purview of federal employees.

In the famous case of *Terry v. Ohio,* 392 U.S. 1, 1968*,* the Supreme Court ruled that a policeman based on his own instincts and suspicions and on the need to protect himself and others may conduct a limited search for weapons without a warrant or probable cause if there was reason to believe that a crime had been committed. The facts of the case involved a detective named McFadden who had observed two men in downtown Cleveland acting, according to him, suspiciously. According to testimony by the officer, the men would walk past a certain store, look in, and stop at a nearby street corner and confer. They proceeded to meet again at another street corner where an additional man joined the group, one of whom was Terry. The officer detained the group and frisked them. He located two handguns, and they were charged and convicted for carrying concealed weapons.

In other words, *Terry v. Ohio* holds that only a limited search for weapons is allowed in the absence of probable cause where the search is not incident to an arrest. The search can be permissible only if a reasonable, prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger. The rationale, as it pertains to airports and aircraft, is that the slight infringement on individual rights should be balanced against the overwhelming need to stop hijacking.

Overall, the judicial system has refrained from placing restrictions on officers' ability to make stops. The court has basically agreed that officers do have street experience and must be given leeway to use it. In *U.S. v. Cortez*, 449 U.S. 418, (1981), the Court supported an officer's discretion to stop an individual by holding that reasonable suspicion should be based on the "totality of the circumstances," which may include inferences and deductions made by a trained officer. Subsequently, the general climate of danger following the repeated hijackings of U.S. air carrier flights was determined to be reason enough for searching all airline passengers (*U.S. v. Epperson*, 454 F.2d 769 [4th Circuit, 1972]). Section 202 of the Air Transportation Security Act of 1974, 49 USC Sec 1356(a) required a preboarding search of all passengers and their carry-on baggage for weapons and explosives, pursuant to regulations (now TSA 49 CFR Chapter XII, Part 1544). The passing of a human passenger through a magnetometer is just such a search. The invasion of privacy constituted by a measuring of the distortion of magnetic waves around the body is so minimal as to be considered administrative. Stopping and frisking moves the level of intrusion up a notch. The search must be reasonably related in scope to the circumstance that made the original intrusion justified in the first place.

SELECTEE CLASS STOP AND FRISK SEARCH

In contrast to the individualized stop and frisk search, the selectee class category of the stop and frisk search approach requires the identification of small groups of people singled out for additional scrutiny. The suspicion only needs to establish probability, not certainty, and it can be established from the totality of the circumstances (*U.S. v. Sokolow,* 490 U.S. 1, 109 S.Ct. 1581 [1989]). However, to prevent abuse, the attributes in the profile must be relevant to the threat being averted. In the Sokolow case, the defendant was stopped at the Honolulu airport by agents who knew the following: (1) he had paid $2100 for two airplane tickets from a roll of 20-dollar bills; (2) he traveled under the name of someone who did not match the name associated with the telephone number he provided the airline; (3) his original destination was Miami; (4) he stayed in Miami for only 20 hours; (5) he appeared nervous during the trip; and (6) he checked none of his baggage. The court reasoned that these facts amounted to reasonable suspicion, and in the majority opinion they concluded that "reasonable suspicion" was the level of suspicion considerably less than proof of wrongdoing by a preponderance of the evidence.

The court upheld, in essence, the agent's belief that the defendant's behavior was consistent with the Drug Enforcement Agency's drug courier profile, but stated that a court sitting to determine the existence of reasonable suspicion must require the agent to articulate the factors leading to that conclusion, whether they are part of a profile or not. This decision seems to set a precedent for airport-passenger profiling of potential terrorists. Further decisions, however, will be required to settle the issue.

CONSENT EXCEPTION

Another exception to the Fourth Amendment prohibition against unreasonable searches and seizures is evidenced by the rules relating to consensual searches. When passengers freely and voluntarily give consent to a security search, they surrender their privacy interests, and the issue of potential violations of Fourth Amendment rights is moot (*Schneckloth v. Bustamonte*, 412 U.S. 218, 93 S.Ct.

FIGURE 11.2 Security personnel check a passenger's luggage. Passenger rights have become an issue. (Source: Transportation Security Administration, www.tsa.gov)

2014 [1973]). On the other hand, if the travelers had an expectation of privacy, any consent would have to knowingly be waived for the consent exception to come into play (see Figure 11.2).

In the Bustamonte case, a police officer stopped a car containing several men when he observed that one headlight and the license plate light were nonfunctioning. After the driver could not produce a license, the officer asked a passenger who claimed he was the vehicle owner's brother if he could search the car. The passenger replied, "Sure, go ahead." Stolen checks were found under a seat, leading to charges against the car passenger. Bustamonte's motion to suppress the evidence at trial was denied. His conviction was affirmed on appeal, but the Ninth Circuit Court of Appeals set aside the district court's order. The precise question became, what must the state prove to demonstrate that consent was voluntarily given? The court issued a very narrow decision.

They held that when a subject of a search is not in custody and the State attempts to justify a search on the basis of his consent, the Fourth and Fourteenth Amendments require certain conditions be met, namely, that the State demonstrates that the consent was in fact voluntarily given and not the result of duress or coercion, express or implied. Voluntariness is a question of fact to be determined from all the circumstances, and although the subject's knowledge of a right to refuse is a factor to be taken into account, the prosecution is not required to demonstrate such knowledge as a prerequisite to establishing voluntary consent.

As early as 1973, the consent exception to the Fourth Amendment requirement, in the context of airport searches, has been litigated. It was reasoned that if the nature of the established screening process is such that the attendant circumstances will establish nothing more than acquiescence to apparent lawful authority, some authorities have ruled that there is no real consent (*U.S. v. Ruiz-Estrella,* 481 F.2d 723 [2nd Circuit,1973]). Another case went so far as to say that it could hardly be considered a voluntary consent when the passenger's only alternative was to forgo his or her flight (*U.S. v. Albarado*, 495 F. 2d 799, [2nd Circuit, 1974]).

Once again, the central issue revolves around the concept that airline employees, in compliance with government regulations, had conducted these searches. It has already been discussed that some legal authorities contend that these "warrantless", nonarrest searches are legal because private persons administer them. Nonetheless, these searches were conducted because a federal agency has required them. Adding to the mix, federally trained federal employees now conduct the searches. As stated, FAR 108.9 required each certificate holder to "conduct screening under a security program… to prevent or deter the carriage aboard aircraft of any explosive, incendiary, or

deadly or dangerous weapon on or about each individual's person or accessible property and the carriage of any explosive or incendiary in checked baggage." A passenger cannot legally board an aircraft unless the airlines conduct a search of their person and possessions. The Transportation Safety Administration (TSA) rules now govern but essentially require that the same standard of screening applies.

Another case reaching the same conclusion was *U.S. v. Lopez*, 328 F. Supp. 1077 (1971), which was decided before the 100 percent screening rules came into effect in 1973. Regardless, it contains some interesting and applicable language. The government in this case argued that the posting of signs advising that passengers and baggage were subject to search was tantamount to "implied consent."*

The court disagreed and even pointedly commented that consent to a search involves the relinquishment of fundamental constitutional rights and that consent cannot be lightly inferred. In *U.S. v. Lopez*, which involved the seizure of narcotics, the judge wrote, "Nor can the government properly argue that it can condition the exercise of the defendant's constitutional right to travel on the voluntary relinquishment of his Fourth Amendment rights." The court extended its reasoning by providing that airport searches were not justified as searches incident to arrest either. It is also interesting that the judge referred to air travel as some sort of "constitutional right." Of course, a thorough search of the U.S. Constitution fails to reveal such an explicit right.

Two questions regarding the consent exception remain unanswered:

1. What is the point at which passengers give consent?
2. To what precisely are passengers consenting?

As stated, some legal scholars argue that it can hardly be considered voluntary consent when a passenger's alternative to submission is forgoing the flight. The Ninth Circuit Court in *U.S. v. Davis*, 482 F.2nd 893, as early as 1973, also confronted this issue. The Davis judgement did not specifically hold that consent to an additional search could be withdrawn after an inconclusive scan if the passenger agrees not to board the plane. Nor did it determine at what point in the boarding process a passenger might decide not to fly and thereby withdraw implied consent. Basically, the judge simply believed that the defense argument failed because the passenger did voluntarily consent, at least to the initial search.

The law regarding the consensual search of baggage and one's person by police officers has remained fairly constant over the years. More recent case law, as in *U.S. v. Favela*, 247 F.3d 838, 2001, upheld the concept that police can approach and question passengers without the officer's conduct constituting a seizure. The officers had approached the defendant after observing her walk back and forth from a gate to a gift shop at the Kansas City airport. The officers asked if they could search her bag, and she consented. Nothing was discovered. She was requested to pull her shirt tightly around her waist when the officers observed a bulge. One officer asked to touch the bulge, and she consented to the touching as well. She was placed under arrest. A search — incident to arrest — uncovered 1.2 kilograms of methamphetamine. The case was distinguished from *U.S. v. Eustaquio,* 198 R.3d 1068, (8th Circuit 1999), which involved the nonconsensual touching of a bulge in the defendant's clothing, without reasonable suspicion, which was determined to have violated her Fourth Amendment rights. The defendant had argued that the officer lacked the reasonable suspicion necessary to justify a nonconsensual investigative search. The court reasoned that the issue need not be addressed because in this case there was not even a seizure for Fourth Amendment purposes.

Another twist to the voluntariness matter or consent question is the power relationship between the security individual and the passenger, who may be a person of color. That persons of color are

* *Note*: 14 CFR Sec 108.17e (1995) requires notification "posted in a conspicuous place at the screening station and on the x-ray system which notifies passengers…. that they are being inspected."

subjected to a disproportionate amount of police security is hardly in doubt. This fact is especially prevalent in the context of ordinary stops, even when increased security has no objective foundation; it often results in an actual search. As regards traffic stops, Justice Sandra Day O'Conner stated in a dissenting opinion that "As the recent debate over racial profiling demonstrates all too clearly, a relatively minor traffic infraction may often serve as an excuse for stopping and harassing an individual" (*Atwater v. Lago Vista*, 121 S.Ct. 1536:1567, 2001). Such traffic stops can be analogized to stops in airports. Demonstrating whether or not a particular airport security or police officer has acted on race-based motivation is problematic at best. So much racial bias is subtle, difficult to prove, and can even be subconscious. The concept was highlighted when after 11 September, two Rabbis praying in an aircraft were removed from an aircraft to be searched, presumably when a passenger presumed they were speaking Arabic and acting suspicious.

Once the passenger is singled out for whatever reason, he or she is often asked to consent to a search. Many courts are leaning toward requiring a law enforcement officer to have at least an articulable suspicion before even asking for consent to search. The officer often intimidates people, especially those of color. They do not completely understand their right to just say no. Even if the police do have some suspicion, the inherently coercive nature of the police citizen encounter, especially in airports, and the difficulty in proving free and voluntary consent may require additional safeguards. One court in Hawaii has even suggested a Miranda-like warning such as advising the individual of the following (*State v. Kearns*, 867 P.2nd 903 [1994]):

- The individual is free to leave and need not give consent.
- If consent is given, any contraband found during the search will be used to prosecute.
- Consent may be with drawn at any time.

The courts will certainly continue to evaluate whether passengers have truly consented to searches in airports and that the consent they give is voluntary. In the aftermath of 11 September, passengers seemed particularly willing to consent to be searched. This attitude may well already be fading. The government maintains, however, that ever since the 11 September 2001, attacks, airport security needs to be ratcheted up across the United States, and female passengers are not exempt from thorough checks. By all accounts, there's every reason to be cautious. In 2004, two Russian planes crashed almost simultaneously shortly after taking off from a Moscow airport, killing at least 90 people on board. Investigators suspect that two women linked to the Chechen conflict had smuggled high-grade explosives on board. And in the Middle East, some Palestinian women have taken advantage of their traditional flowing robes to hide explosives-laden belts for suicide missions.

OTHER EXCEPTIONS TO FOURTH AMENDMENT REQUIREMENTS

Border Searches

At a national border, a border search is a superficial search or inspection conducted without a warrant or probable cause of persons, vehicles, and property entering the United States. The Supreme Court in *Martinez-Fuerte*, 428 US 543 (1976) upheld border searches as inherently reasonable under the Constitution. Any person entering the United States is subject to search for the simple reason that they are entering the sovereign territory of the United States. The border area is defined as any place that is the functional equivalent of the border, whether it is the first airport where the plane lands or at any established inspection station near a border. Additionally, a U.S. Customs official is allowed to stop, search, and examine any person on whom an officer suspect is in possession of any type of contraband whatsoever (*U.S. v. Ramsey*, 431 U.S. 606, 97 S.Ct. 1972 [1977]).

Specifically, in the Ramsey case, the court upheld a customs inspection of mail entering the United States, which by regulation does not extend to reading the correspondence. The mail can be searched for prohibited items, including explosives and weapons. In the Ramsey case, the court stressed:

- That the search was constitutional under the long-standing rule generally applicable to border searches; namely, such searches are considered to be reasonable by the single fact that the person or item in question had entered into the United States from outside
- That the lower court was wrong in concluding a warrant would be needed as to mail

The lower court in the Ramsey case had excluded the evidence because it did not meet the "exigent circumstances test" for permitting searching without warrants. The Supreme Court, however, reversed the decision and determined that the border search exception is not based on the doctrine of exigent circumstances at all. As for nonroutine border inspections, the standards are quite different. Lower courts have generally held that a "real suspicion" is needed for a strip search and a "clear indication" of the presence of some sort of contraband for a body cavity search to be acceptable. The U.S. Customs Agency had formerly often been criticized for abusing this investigative tool.

Exigent Circumstances

Searches under exigent circumstances also constitute an exception and are conducted to prevent physical harm to officers or other persons, and the fruits thereof are perfectly admissible (*U.S. v. Sarkissian*, 841 F.2nd 959 [9th Circuit, 1988]). Certain situations may clearly justify a search of something without triggering the Fourth Amendment. According to the Legal Counsel Division of the Federal Bureau of Investigation (FBI), there are three threats that provide that justification (Sauls, 1987). They include clear dangers to life, of escape, and the removal or destruction of evidence. The requirement for searches under exigent circumstances was first recognized by the U.S. Supreme Court in *Warden v. Hayden*, 387 US 284 (1967).

The court approved the search of a residence conducted without a warrant that followed a report that an armed robber had fled into a specific building. The courts, using very interesting language, extended the idea even further in *Mincey v. Arizona*, 437 US 385 (1978). The Supreme Court held that "the Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others (437 US 385, 1978:392). Emergency searches therefore, seem to be permissible when conducted by the police without a warrant on the basis of some immediate and overriding need, such as police safety. Employing this logic, airport police officers, airport security officers, and the public are certainly gravely endangered if a fellow passenger has a gun or an explosive device. How that device becomes apparent to the authorities is what is at issue. In essence, it is apparent when it is reasonable for the officer to assume that a threat exists.

REASONABLENESS

Much has been written about the concept of reasonableness. Law enforcement personnel and security professionals use searches and seizures to locate and collect evidence needed to convict individuals suspected of crimes and to control the access to aircraft. Each of these searches must be reasonable. Courts, lawyers, police, and security officials have agonized over the precise meaning of this term. In *Mapp v. Ohio,* 367 US 643, (1961), the Supreme Court found that the police did not exercise reasonable judgment in their enthusiastic seizure of alleged pornographic materials without a warrant. On the other hand, the same actions, with a valid warrant, would probably have resulted in a conviction upheld by the courts.*

In airports, the reasonableness of a search must be weighed against the level of the threat. High-threat situations, such as existed during the Persian Gulf War and post 11 September, change the

* *Note*: *Mapp v. Ohio* also held that the prohibitions of the Fourth Amendment were fully applicable to the states under the Amendment's due process clause; evidence obtained by illegal searches by state or federal officers was admissible in state court.

degree of acceptable intrusiveness of airport searches. However, there are limits to intrusiveness. In *U.S. v. Afanador*, 567 F2d. 1325 (5th Circuit 1978), customs officials, acting on an informer's tip, stopped two airline attendants in Miami after arriving from Colombia, a known drug source country. Despite finding no contraband in their luggage, the agents insisted on a strip search, even though the informant's tip had only pertained to one individual. The court decided that the strip search of the second flight attendant was just too intrusive based on the totality of the circumstances.

Another case involved a Drug Enforcement Agency (DEA) agent who stopped a traveler in the Atlanta airport. The passenger had arrived from Fort Lauderdale, FL, a city the agent considered a principal source of cocaine. The suspect apparently arrived early when law enforcement activity is diminished and appeared to be concealing the fact he was traveling with someone else, plus he only possessed some carry-on luggage. In *Reid v. Georgia*, 448 US 438, 100 S. Ct. 2752 (1980), the Supreme Court held that "the agent could not, as a matter of law, reasonably suspect the petitioner of criminal activity on the basis of these observed circumstances" (448 US 438, 100 S. Ct. 2752, 1980:441). The court went on to speculate that their experience with drug agents makes them wonder if there exists any city in the world that a DEA agent would not characterize as a known source of narcotics. These cases support the contention that courts will set limits on police and airport searches when they believe the authorities have simply gone too far.

PROBABLE CAUSE

This concept of reasonableness is linked to probable cause, and probable cause is another term that has been meticulously dissected and reconstructed by the courts. In essence, the Supreme Court has ruled that any arrest or seizure is unreasonable unless it is supported by probable cause (*Michigan v. Summers*, 452 US 692 [1981]). Additionally, the burden of probable cause requires more than mere suspicion. The officer must know of facts and circumstances that would reasonably lead to "the belief that an offense has been or is being committed" (*Brinegar v. U.S.*, 338 US 160 [1949]).

If no probable cause existed when a police officer took a certain action, it cannot be retroactively applied. Information to support probable cause can be acquired in a number of ways. First, personal observation permits police officers to use their personal training, experience, expertise. and instinct to infer probable cause from situations that may or may not be obviously criminal. Second, information collected from witnesses, victims, and informants, so long as it is reliable, can be used to support probable cause. Third, physical evidence, such as a gun or knife, in plain view, such as inside an x-ray machine, may provide officers with sufficient credence to support probable cause. Last, probable cause clearly exists where the police actually see a person committing the crime by concealing some sort of weapon or contraband.

On top of all this, case law has held that a judicial determination of probable cause must be made within 48 hours after the arrest, even if this period is over a weekend (*County of Riverside v. McLaughlin*, 1991; Del Carmen, 1987). Adopting the conclusions of the courts as to what exactly constitutes probable cause is often difficult to apply in an airport setting. Airport security officers, whether police or private, are expected to make split-second decisions on probable cause. This is required regardless of the fact that the courts will dissect the decisions with a fine tooth comb, using all the time in the world needed to do so. When an officer has overstepped what the courts consider reasonable, they are quick to implement the exclusionary rule.

THE EXCLUSIONARY RULE

The judiciary's most effective tool in regulating the activity of law enforcement officers is the exclusionary rule, which prohibits the use of illegally seized evidence in court. According to the rule, any evidence obtained by an unreasonable search or seizure is inadmissible against a defendant at trial (*U.S. v. Leon*, 468 US 897 [1984]). Furthermore, any physical or verbal evidence police

acquire by using illegally obtained evidence is known as the fruit of the poisonous tree and is also inadmissible.

The exclusionary rule forces the police to gather evidence properly. If they abuse the mandates of the Fourth Amendment, they are unlikely to get a conviction. Critics of the rule argue that it permits guilty people to go free because of simple carelessness or innocent errors. Consequently, the courts have carved out several exceptions to the rule.

The Legal Authority of Private Persons to Search

The exclusionary rule applies to all evidence presented in federal court as per the decision in *Weeks v. U.S.*, *232* US 383 (1914). The case held that where federal officers have made an "unreasonable" and consequently illegal search and seizure, the evidence obtained is not admissible in a federal court proceeding. However, in *Wolf v. Colorado*, 338 US 25 (1949) the Weeks case ruling was not to be applied to illegally seized federal evidence offered in a state court. Consequently, the first of many "illegal state searches" was admissible. As evidenced by the case of *Lustig v. U.S.*, 338 US 74 *(*1949), the courts also were inclined to admit illegally seized evidence by state officers in federal court. The court had, for some reason, not readily accepted today that "the crux of that doctrine is that a search is a search by a federal official if he had a hand in it; it is not a search by a federal official if evidence secured by state authorities is turned over to the authorities on a silver platter" (338 US 74:79).

For approximately 50 years after the original Weeks case ruling, state courts continued to allow illegally obtained evidence, and federal courts could admit evidence that had illegally been obtained by state officers. This practice came to be known as the silver platter doctrine because each conviction was handed to the prosecution on a silver platter. The only times when the procedure was discouraged was when police actions were so extreme that they shocked the conscience of the court.

For many years, however, the silver platter doctrine was acceptable law. In essence, a search by a federal official, even if the officer had a hand in collecting the evidence, did not technically constitute a search by a federal official. If the evidence secured by the state authorities was turned over to the authorities "on a silver platter," it was still admissible. The Supreme Court in the decision in *Mapp v. Ohio* (1961) finally eliminated this procedure. Whereas the Supreme Court had previously been hesitant to apply the Fourth Amendment in state courts, the Mapp case signaled a new willingness to apply the Fourth Amendment to both federal and state law enforcement officers.

Earlier in *Elkins v. U.S.*, 364 US 206 (1960), the Supreme Court had laid the foundation that evidence illegally obtained by state officers and subsequently provided to federal agents would not be admissible in federal court as per the due process clause of the Fourteenth Amendment. This was further refined in the Mapp case, where the court reasoned that the prohibitions of the Fourth Amendment were fully applicable to the States under the Amendment's due process clause, making illegal searches equally inadmissible in any court.

The court was first convinced where, as mentioned, police actions were so extreme that they shocked the conscience of the court. The standard was created in *Rochin v. California,* 342 US 165 (1952). In the Rochin case, the police entered the home of Mr. Rochin, without a warrant, and testified that they saw him place what they suspected to be narcotics in his mouth. They transported him to a hospital and had his stomach pumped. Some morphine was recovered, and he was subsequently convicted of possession of illegal drugs. The Supreme Court overturned his conviction. They concluded that the police officers had gone too far and had violated the defendant's constitutional right for protection against unreasonable searches. First, the courts had made a huge distinction between state officers and federal officers. Today, they make a distinction between officers of a government entity and private security officers. It remains to be seen whether that differentiation will survive, especially when the "private security officers" are federal employees.

It should be noted at this point that as regards airport searches, which are in essence still considered private citizen searches, the courts first recognized and analyzed the issue in a landmark case

as early as the 1920s in *Burdeau v. McDowell*, 245 U.S. 465, 41 S.Ct. 574 (1921). The court specifically held that searches by private persons are separate and distinct from searches conducted under state authority. The Fourth Amendment was intended as a restraint on the activities of sovereign authority, and it was not intended to be a limitation on anyone other than governmental agencies. Individuals have other means of redress against those who may have illegally taken private property as part of an administrative search. This particular reasoning was re-inforced again 40 years later. They can sue using the law of torts as a remedy.

In *People v. Superior Court of Los Angeles*, 449 v. P.2nd 230, 74 Cal Reporter 294 (1974). The court in California reiterated that there are no state standards for "search and seizure" by a private citizen who is not acting as an agent of the state or other governmental unit. The Court subsequently reasoned that "therefore acquisition of property by a private citizen from another person cannot be deemed reasonable or unreasonable." Exactly who today is considered a government agent or is acting in essence or in the shoes of a government agent is still to be adequately defined by the courts, again becoming more and more complicated by the assumption of such duties by the TSA.

EXCEPTIONS TO THE EXCLUSIONARY RULE

Supporters of the exclusionary rule maintain that it is necessary to keep the police in line and as a deterrent to the police overstepping their authority. Critics have reasoned that the costs to society of losing critical evidence are higher than the benefits of deterring police misconduct. As a result, the courts eventually began to carve out exceptions to the exclusionary rule, which assisted the criminal justice system in convicting individuals even though their Fourth Amendment rights were technically violated. The rationale was based on the perceived need to get a handle on criminal activity, regardless of simple mistakes or if the police would have acquired the evidence eventually anyhow. The shift in perception was also the result of more conservative, law-and-order-type judges being appointed to the Supreme Court. The shift once again reinforces the concept that the criminal justice system adjusts to public opinion.

INEVITABLE DISCOVERY

The "inevitable discovery" exception was first created in the case of *Nix v. Williams,* 467 US 431 (1984). A ten-year-old child, Pamela Powers, disappeared on Christmas Eve 1968. The police's primary suspect was a religious fanatic named Robert Williams. The police eventually tricked the accused into revealing where he had buried the child using his own religious fanaticism against him. The police pressured the defendant to reveal the location of the body so she could ostensibly have a "religious funeral." The Court in *Brewer v. Williams*, 430 US 387 (1977) initially ruled that the evidence, in this case the body of Pamela Powers, was inadmissible because the accused attorney was not present during the interrogation wherein the accused revealed the location of the body. Later in the Nix case the Court reversed itself and decided that the evidence was admissible because the body would have been inevitably found by legal means. In essence, in *Nix v. Williams*, the judges decided that although the government should not be put in a better position because of its illegal conduct; it should not be totally barred from the use of such evidence in cases either.

In *U.S. v. Hernandez-Cano,* 808 F.2nd 779, (11th Circuit Georgia, 1987), the courts applied the inevitable discovery rule to airport search situations. The defendant was proceeding through baggage screening when the x-ray revealed a large dark mass. At first, the defendant agreed to have the bag further inspected, but the airport security officer extracted a large wrapped object out of the bag. The passenger eventually objected to any further inspection. A verbal exchange took place after which the defendant agreed to give the security officer a peak at what was inside the wrapped parcel. The airport security officer later testified he thought he observed a white powder. The defendant refused to submit to a more thorough inspection, and airport security personnel decided to

summon a law enforcement officer. The police officer advised the defendant that if he refused further access to the parcel that he could not pass beyond the security checkpoint.

Consequently, the defendant retrieved the baggage with the parcel inside it and returned to the ticket counter. He advised the agent that he wished to transfer an item from his carry on to the checked baggage. The airline complied. However, when returning to the checkpoint he advised the security agent that the bundle had been thrown away, offering the explanation the bag had contained some laundry. Security proceeded to confer with the counter airline agent and was made aware of the fact that the defendant had added "something" to his checked baggage. On the theory that the agent did not know whether the bundle contained drugs or a bomb, the agent put a hold on loading the baggage. The agent also discussed the situation with the pilot and decided to open the luggage by use of a luggage passkey. Meanwhile the officer had followed the agent to the baggage area and had been peering over the agent's shoulder. When he observed the parcel of "alleged white powder," he reached in and grabbed the bundle. The parcel was later determined to hold cocaine.

Regardless of the lack of a warrant, the court in the Hernandez case agrees that although the officer's warrantless search was not justified, it stated, "We hold that the inevitable discovery exception should have been applied." In an interesting note, the court described its reasoning. Under the inevitable discovery exception to the exclusionary rule, evidence is admissible that otherwise would be excludable if it inevitably would have been discovered by lawful means had the illegal conduct not occurred.

The court believed that had the police officer not reached into the bag and retrieved the parcel, that the agent inevitably would have done so. Consequently, so long as the prosecution can introduce sufficient evidence to show that the information would ultimately have legally been obtained by lawful means, it is still admissible. In essence, an inevitable discovery finding is based on objective evidence concerning the scope of the ongoing investigation, which can be objectively verified or impeached.

The ultimate or inevitable discovery exception is closely related in purpose to the harmless-error rule. The rule serves a very useful purpose insofar as it blocks setting aside convictions for small errors or defects that have little if any likelihood of having changed the result of the trial. On the other hand, these exemptions can provide the police with an incentive to avoid the warrant requirement. The police could seek to find the most expeditious method of obtaining evidence, without regard to its illegality, knowing that so long as they could have acquired the evidence legally, the evidence will still be held to be admissible. The courts, therefore, have been required to evaluate, after–the-fact, many of the judgment calls made by officers in the field.

GOOD FAITH EXCEPTION

Later in *U.S. v. Leon*, 468 U.S. 897, (1984), Supreme Court Justice Byron R. White described the "good faith exception" to the exclusionary rule. In 1981, a confidential informant of unproven reliability informed an officer of the Burbank Police Department that two persons known to him were selling large quantities of cocaine and methaqualone from their residence. The informant also indicated that he had personally witnessed a sale of methaqualone by one individual at the same residence five months earlier. He also described a shoebox containing large quantities of cash and indicated that drugs were usually stored at the residence.

The police launched a serious investigation of the residence. Cars parked at the residence were determined to belong to Armando Sanchez and Patsy Stewart. Sanchez had a previous conviction for drug possession, and Patsy had no criminal record. During the investigation, officers noted a vehicle belonging to Ricardo Del Costello, a known dealer arrive at the residence. The driver, later determined to be Alberto Leon, entered the house and left soon after with a small paper bag. Further investigation revealed that Leon was living in an address in Burbank as well.

Based on the observations mentioned and some others, two police officers summarized their findings in an affidavit and prepared an application for a search warrant for the addresses mentioned and a third. The warrants were executed, and large quantities of drugs were seized. The suspects

were indicted and charged but made a motion to exclude the evidence collected during the search. The court concluded that the affidavit was insufficient to establish probable cause, but the court made clear that the officer had acted in good faith. The defense had argued that the drugs be suppressed on the grounds that the warrant had not been issued on probable cause.

The court rejected the government's suggestion that the Fourth Amendment exclusionary rule should not apply where evidence is seized in reasonable, good faith reliance on a search warrant. The U.S. Supreme Court disagreed and overturned the decision. The court held "…the officer's reliance on the magistrates' determination of probable cause was objectively reasonable, and application of the extreme sanction of exclusion is inappropriate."

One scholar has countered the idea that police officers may use this exception to circumvent the law. He states that the deterrent to the rule's effectiveness "lies in the impetus it has provided to police training programs that make officers aware of the limits imposed by the Fourth Amendment and emphasize the need to operate within those limits." An objective good-faith exception is not likely to result in the elimination of such programs, which are now viewed as an important aspect of police professionalism. Neither is it likely to alter the tenor of those programs; the possibility that illegally obtained evidence may be admitted in borderline cases is unlikely to encourage police instructors to pay less attention to Fourth Amendment limitations" (*U.S. v. Leon*, footnote 20).

Thus, the good faith exception to the exclusionary rule was created. The concept has been repeatedly upheld in such cases as *Illinois v. Krull*, 480 US 340 (1987) and *Arizona v. Evans*, 514 US 1 (1995) involving instances where the police either objectively or reasonably relied on information or where a clerical error was made.

POLICE PARTICIPATION

The cases of *Burdeau v. McDonnell* and *People v. Superior Court of Los Angeles* had concluded that a search by a private security officer was not a search conducted by state officials and need not be determined to be either reasonable or unreasonable. However, the courts were not totally blind to the creative nature of many law enforcement officials. Police officers soon realized that private security officers could legally search someone without necessarily observing the stringent requirements of the constitutional parameters placed on law enforcement by the courts. Consequently, the courts came to rule on a case wherein the police officer was literally standing behind the private security officer and directing the search. The courts were quick to recognize these attempts at legitimizing an illegal search were outside the protection of the above two cases.

In the case of *Corngold v. U.S.,* 367 U.S. F.2nd 1 (1966), the actions of several ingenious customs agents were put to the test. The case involved the admissibility of evidence discovered by opening packages for inspection; shipped from Los Angeles to New York under alleged false description of the contents in the shipping documents. Customs officers had originally tested the suspect package with a scintillator, advising the airline workers that the scintillator detects the radiation from watches. The customs agents unequivocally requested that the airline agent open the package. The court ultimately held that "it would be difficult to justify any conclusion other than that the carrier employee participated in the search solely to serve the purpose of the government. There was nothing else in the record which would indicate that the package was in fact opened for any purpose of the carrier." (367 US F2nd 1:10). The watches did not pose a threat to the aircraft, and the customs agents were aware of that fact. They were concerned with the shipment of illegally manufactured watches, not any danger to the airport or aircraft.

The Corngold case set the precedent that the fruits of a search conducted solely in aid of enforcement of a federal statute are inadmissible when the search fails to meet the Fourth Amendment requirements. The airline agents had merely been the pawns of the government agents. Clearly, the discovery of illegally manufactured and shipped watches does not pose a threat to the security of the airport or the aircraft. Airline officials often make much the same argument regarding the

transportation of illegal drugs. As stated, the airlines consistently and vehemently have argued throughout the growth of the air transportation industry that they are not law enforcement agents and should not be forced to conduct themselves as such.

The court in *Taglavore* v. U.S., 334 U.S. 699, 68 S.Ct. 1229 (1948) further reasoned that, "law enforcement agents must secure and use search warrants wherever reasonably practicable." The court directly commented that "The violation of a constitutional right by subterfuge cannot be justified, and the circumstances of this case leave no other inference than that this is what was done."

However, the courts did not completely close the door on airline personnel assisting in the discovery of contraband and the subsequent successful prosecution of smugglers. The Corngold court also reasoned that:

> We would of course agree that if a carrier, while inspecting packages for its own purpose pursuant to a provision in the contract of carriage, discovers contraband and notifies the customs agents of that fact, and the agents then secure a warrant on the basis of this information and conduct a search, the search is entirely proper. This is precisely the procedure which the Fourth Amendment contemplates (367 U.S. F.2nd 231 [1966]).

Such a set of circumstances exemplifies the perfect legal cooperation between airline security and law enforcement. The airlines quite properly search and discover. If the contraband is illegal but not dangerous, the information they possess can be used to substantiate the issuance of a warrant. There will always be a blurring of the boundaries between public sector and private sector employees as well as a difference between individual and institutional responsibilities. The key is to find the correct balance and maintain it.

NONVIOLENT THREATS?

Generally, security is concerned with detecting weapons, explosives, and other dangerous materials. When security personnel do suspect such a risk, they usually call in the appropriate government agency or military personnel to handle the risks of a bomb or other dangerous device. This type of search is easily distinguishable from the normal "suspect" search due to the potential threat to the public. Arguably it could be held to be a private search because the carrier initiated it. Additionally, it could be considered a lawful police search under the exigent searches exemption to the Fourth Amendment rules.

However, the search for other "nonviolent threats" has also occupied the courts. In *U.S. v. Pryba*, 312 F. Supp. 466 (1970), a United Airlines supervisor had authorized a package to be opened because of "peculiar circumstances" surrounding receipt of the shipment. Basically, the "peculiar circumstances" consisted of the fact that the shipper was nervous; he evaded questions on the actual contents of the package and admitted that the return address on the package was nonexistent. It must be remembered that this incident took place in 1970. The airline employee was arguably just being cautious because the airlines were being held to the standard of exercising due diligence in uncovering explosives. After opening the package without a warrant, the contents turned out to be films of alleged hard-core pornography, which were turned over to the Federal Bureau of Investigation (FBI). The search was considered legal.

Other examples of closer judicial scrutiny were exhibited in *Wolflow v. U.S.*, 391 F.2nd 61 (1968) where police participation at the request of the carrier was at issue once again in a case of the "nonviolent" contents of certain luggage checked for carriage. The ticket agent accepted two "overweight" suitcases for a flight scheduled to fly between Los Angeles and Las Vegas. The agent testified that he held them off the flight based solely on the excessive weight of the two suitcases. The agent's superior, for whatever reason, called a Los Angeles policeman to witness the opening of the bags. The contents revealed 3500 watch movements that the airline turned over to customs agents.

This 1968 case upheld the admissibility of the fruits of the search as falling within the exemption created by *Burdeau v. McDowell*, 256 U.S. 465, 41 S.Ct. 574 (1921). However, it is unclear how the weight of baggage actually accepted for shipment is suspicious in and of itself.

Earlier the courts had bolstered once again the concept that law enforcement agents must secure a warrant whenever reasonable. The judges categorically restated the basic idea of unreasonable searches when they said, "It is a cardinal rule that, in seizing goods and articles, law enforcement agents must secure and use search warrants whenever reasonably practicable." This rule rests upon the desirability of having the magistrate rather than police officers determine when search and seizures are permissible and what limitations should be placed upon such activities. *Trupiano v. U.S.*, 68 S.Ct. 1229, 334 U.S. 699 (1948). Overall, airline agents now leave the contraband exposed so that law enforcement can visibly see the contraband and are not forced to reopen the luggage, which would necessitate the acquisition of a warrant.

Therefore, the courts have sought to rule on searches wherein the airline agent locates contraband and summons the police. Is the police activity, with respect to the same object a separate search subject to Fourth Amendment constraints? In *U.S. v. Jacobsen*, 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2nd 85 (1984), Federal Express employees opened a damaged box. They discovered newspapers covering a tube. After the tube was cut open they observed plastic bags of white powder. They immediately summoned the federal authorities. However, prior to the federal agent's arrival, the airline employees had put the plastic bags back into the tube, and the tube and newspapers back into the box. They did keep the box open. A federal officer reopened the box and exposed the smaller bags of white powder. He field-tested the contents on the spot and determined the white powder to be cocaine.

Justice Stevens concluded that the agent's actions were not a significant expansion of the earlier private search and concluded that subsequently no warrant was required. He stated, "Respondents could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to their offices for the express purpose of viewing its contents. The agent's viewing of what a private party had freely made available for their inspection did not violate the law. It remains in dispute whether the suggestion that the owner of the container had no legitimate expectation of privacy in its contents and that government agents in opening that container without a warrant on the strength of information provided by a private party would not violate the law.

The subject of joint operations between private security, the airlines, and law enforcement personnel remain blurred and are generally decided on a case-by-case basis. In a very early case during prohibition, *Byars v. U.S.*, 47 S.Ct. 248 (1927), a federal agent who had been invited to accompany a state officer participated in a search that turned up counterfeit strip stamps of the kind used on whiskey bottled in bond. The court once again set the precedent that such joint operations dictate the need to strictly follow Fourth Amendment protections and held the contents of the baggage, therefore, inadmissible.

In summary, in the Burdeau case, the exclusionary rule was characterized "as a restraint upon the activities of sovereign authority and not a limitation upon other than governmental agencies" (256 U.S. 465:1921), and on this basis courts have declined to exclude evidence in criminal cases when obtained by private persons. However, the Fourth Amendment becomes applicable when this private officer or citizen is acting as an instrument of government agents. Whether a private individual has been encouraged to cross the line is determined by a "totality of the circumstances" test. Circumstances to consider include the motive of the private security officer or airline agent, any compensation or other benefit the private individual receives from the government, and the advice, direction, and participation of the government agent. This test would therefore apply to airline security officers who receive a bonus for discovering certain kinds of the contraband and who may be receiving bribes from law enforcement to inform them of suspicious activity.

It is significant to point out that certain circumstances can jeopardize an individual's status as a private airport security guard or simply a private citizen. Of particular concern is the moonlighting

of off-duty police officers. In *People v. Tarantino,* 45 Cal. 2nd 590, 290 P.2nd 505 (1955), the court resolved that a police officer working during his off-duty hours as a security guard is still a deputized police officer. In the Tarantino case, the court concluded that the Burdeau case was inapplicable. They distinguished the case by recognizing that an officer employed by the district attorney and paid with public funds as part of his regular daytime employment obtained the evidence.

AIRPORT ADMINISTRATIVE SCREENING SEARCHES AT AIRPORTS

As repeatedly mentioned, the concept of police participation in private searches takes on a whole new aspect when combined with the idea of searches conducted by federal officers. Much has been written about the idea that airport security officers are not agents of the state and that they are in essence private citizens. However, they would never be stationed at airports searching baggage unless mandated by federal regulation. The government and the airlines consider the threat real and have regulated the equipment used in the searches and have made it obligatory that airport operators and airline carriers maintain and implement stringent search procedures precluding the introduction of dangerous weapons and materials onto airplanes and into airplane terminals.

FAR 108.9 required each certificate holder to conduct screening under a security program. They were to prevent or deter, by appropriate procedures approved by the Federal Aviation Authority (FAA), the carriage aboard airplanes of any explosive, incendiary, or a deadly or dangerous weapon on or about each individual's person or accessible property and the carriage of any explosive or incendiary in checked baggage. An assistant attorney general of the United States testified before Congress in 1973 that even though private employees of airlines are doing the search, it is indisputable that they are ordered to do so by the Federal government. This issue is again amplified by the transfer of private security jobs to federal employees.

Cases prior to the mandatory 100 percent screening of all passengers and baggage requirement explain the concept. In *U.S. v. Lopez*, 328 F. Supp.1077 (1971) discussed earlier, the courts were critical of airline employee abuse in airport searches. The case involved a narcotics seizure and turned on the issue of consent. Government attorneys contended that because airport officials had posted signs advising passengers that they and their baggage were subject to search that they could search on that basis alone. The idea of "implied consent" is not a new one but is based on some stringent requirements.

The Lopez case was one of the first airport search cases to raise the issue of consent by prior written notification. The idea simply of posting signs advising that passengers and baggage were subject to search was tantamount to "implied consent" neglects to recognize that the passenger is not free to leave if contraband is suspected or that access to air transportation is effectively denied. Everyone knows that to actually reach the aircraft or gate concourse each passenger, visitor, crew member, or vendor must submit to a search of their person and effects. Early cases were extremely critical of the concept. Most courts have consistently held that consent to a search involves the relinquishment of fundamental constitutional rights and that this consent should not be lightly inferred. In fact, in *U.S. v. Meulener*, 351 F. Supp. 1284 (1974), a passenger opened a suitcase only after he was ordered to do so by the marshal at a time when he was not free to leave or to avoid the search. The court therefore concluded that under these particular circumstances, the search was inherently coercive.

U.S. v. Blalock, 255 F.Supp.268 (1966), another earlier case, discussed the requirement of an "intelligent consent," which implies that the subject of the search must have been aware of his or her rights. The logical extension of this reasoning was that for an intelligent consent to be present, it could only embrace the waiver of a known right. In other words, if the individual is not aware of the fact they have a right; it is difficult to conclude that they knowingly waived it. Remember again that this case was decided prior to the 100 percent screening requirement. Secondly, note that the Lopez case also did not support the contention that airport searches were justified on the basis that they are searches incident to arrest. In traditional legal language, simply because a search discovers

evidence of a violation of a law does not render the search justifiable. The end does not justify the means. A police search conducted in violation of the Constitution is not made lawful just because they find something illegal.

Returning to the discussion relating to *Terry v. Ohio*, legal scholars have also sought to use the concept of probable cause to warrant an airport search. The Terry case was the first case to recognize the need for police officers to search individuals for the sheer need of protecting themselves and in the interest of public safety. The Terry court reasoned, "A police officer may in appropriate circumstances and in an appropriate manner approach a person for purposes of investigating possible criminal behavior even though there is no probable cause to make an arrest." The court, however, made it perfectly clear that the police officer's conduct must be limited in scope and be reasonable. So what constitutes the probable cause? Officers have used everything from alerting the magnetometer to an individual fitting a specific profile.

The Terry court also commented on whether or not mere government observation constitutes a search regulated by the Fourth Amendment. They concluded the decision rests on whether or not the defendant had a legitimate expectation of privacy in the place or thing searched (*Terry v. Ohio,* 392 U.S.1, 1968:9). Based on the above reasoning, it appears there is no search if the government observation reveals information only relating to illegal activity. This kind of rationale has also been used to substantiate the legality of canine searches.

U.S. v. Place, 462 U.S. 696, 707 decided in 1983, contained the language that the warrantless use of a canine did not violate the Fourth Amendment, because the sniff of a dog only discloses the presence or absence of drugs or explosive residue. The dog cannot reveal a plethora of unlimited information about the items or person searched. The logic is based on the concept that a defendant has no legitimate expectation of privacy for drugs, explosives, or other contraband. Some legal analysts have extended this logic to reach a conclusion that more sophisticated and precision-oriented search equipment at airports may be free of the Fourth Amendment concerns of the past. The Place court concluded that the canine search was not very intrusive and also did not expose the person to much embarrassment or inconvenience.

The courts have relied heavily on determining just how intrusive the search is. There are competing values at play. Certainly, the courts have recognized the need to maintain public safety. As the courts and the public further understand the continuing need for stringent security measures, the more likely the courts will be to justify the newer less intrusive means of airport searches. As early as 1971, in *Barrett v. Kunzig*, 331 F. Supp. 266 (1971), the judges supported the government's substantial interest in conducting a cursory inspection at federal buildings, determining that the intrusion outweighed the personal inconvenience suffered by the individual. Such searches have now become commonplace. Further supporting the idea that "some" government observation does not even rise to the level of a search, the court commented. The term search has been used by plaintiffs. To the extent that term is applied to more than a casual visual inspection, it has no meaning and is without foundation in this record (331 F.Supp. 272 [1971]).

The courts have applied the above reasoning to magnetometers at airports. They once again weighed the minimal invasion of personal privacy and the reasonableness of the security search in the light of the known risks. As early as 1972, the court in *U.S. v. Epperson,* 454 F.2d 769 (1972*)* simply and concisely analyzed the legality of a search by use of a magnetometer. The growing threat to combat terrorism was self-evident. Consequently, the court expressed the view that "the danger is so well known, the government interest so overwhelming, and the invasion of privacy so minimal that the warrant requirement is excused by exigent national circumstances." The court was quick to recognize that the public viewed the searches as a welcome reassurance of safety to passengers traveling domestically and abroad. Specifically the court stated,

> The reasonableness of any search must be determined by balancing the governmental increases in searching against the invasion of privacy, which the search entails….It is clear to us that to innocent passengers the use of the magnetometer to detect metal on those boarding is not a resented intrusion on

> privacy, but, instead, a welcome reassurance of safety. Such a search is more than reasonable; it is a compelling necessity to protect essential air commerce and the lives of passengers (454 F.2nd 772:1972).

The court considered the use of magnetometers perfectly legal right from their initial operation. It is worthwhile to point out that the Constitution does not forbid all searches, just those that are unreasonable. The same reasoning applied to magnetometers was soon applied to x-ray machines searching carry-on baggage at airports. X-ray machines are minimally intrusive of privacy and are also minimally embarrassing, if at all, to passengers. This is true at least as to the machines currently in use.

Soon thereafter the court in *U.S. v. Henry*, 615 F.2d 1223 (9th Circuit) 1980, differentiated between the x-ray scan and the magnetometer search. The judges resolved that the x-ray scan is a more intrusive search than the magnetometer and that both were subject to Fourth Amendment controls. At the time they also recognized that if the passenger wants, he or she could have decided to avoid the x-raying of their carry-on baggage by merely consigning any baggage they did not want searched to the baggage compartment. The magnetometer does not provide such an option in that passengers cannot ship themselves via the baggage compartment. It is simply a different set of circumstances when the only way to avoid search is not to fly. With the advent of 100 percent screening of checked baggage, this rationale became moot.

PASSENGER'S RIGHT TO TERMINATE A SEARCH

According to many legal analysts, passengers are deemed to have given consent when they place their bags on the conveyer belt for luggage screening (*U.S. v. Pulido-Baquerizo,* 800 F.2nd 899 [1986]). The judge's decision includes the language that "Those passengers placing luggage on an x-ray machine's conveyer belt for airline travel at a secured boarding area gave implied consent to a visual inspection and limited hand search of their luggage even if the x-ray scan is inconclusive in determining whether the luggage contains weapons or other dangerous objects" (800 F.2nd 902:1986).

From a security officer's perspective, if passengers were allowed to withdraw after setting off the security system, the deterrent effect of the security system would be undermined. It may even be reasonable to argue that there is no guarantee that they might not return and be more successful later. The greater threat may even be the very fact that because a safe exit is available; it would be diminishing the risk and in essence encourages attempts.

The alternative question is more difficult to answer. Implicit consent derives much of its justification from the fact that it is a privacy invasion that free society is willing to tolerate as long as the scope of the search is limited to discovering weapons or explosives and is limited in a manner that produces negligible social stigma. It appears the law is still somewhat unsettled. In *U.S. v. DeAngelo*, 584 F.2d 496 (4th Circuit, 1979) a traveler submitted his briefcase for search. The security officer noticed an opaque object that could not readily be identified. The traveler was advised that his bag would have to be manually searched. The passenger protested the further search of his briefcase and said he would prefer not to take the flight. He was not afforded that option, and narcotics were ultimately found.

The court believed that the circumstances were sufficiently suspicious to cause a reasonably prudent man to conclude the defendant might endanger security officers and passengers. Later, in the opinion the judge specifically stated that "allowing him to withdraw his luggage when the x-ray raised the suspicions of the security officers would frustrate the regulation's purpose of deterring hijacking." The De Angelo case was decided before the case *U.S. v. Pulido Baqerizo*, where the court extended the earlier decision. The opinion added the concept that placing luggage on the x-ray machine conveyor belt automatically provides implied consent not only to scan, but also to conduct a manual search if deemed by security personnel to be necessary.

The idea that potential passengers may avoid the search by electing not to fly is somewhat losing favor. Even though there certainly exists no constitutional right to fly, there has been some softening of the hard-core position that passengers have indeed consented to searches to fly but only when the search is directly related to the safety of the flying public. As stated before, marijuana or counterfeit money do not have the ability to bring an aircraft down or provide the means to hijack it.

In the course of litigating these issues, some passengers and later defendants have more vigorously sought to avoid being searched. In the case *U.S. v. Herzburn*, 723 F.2d 773 (11th Circuit, 1984) clearly involved a more determined and forceful attempt by a passenger to terminate the search. The defendant had placed a shoulder bag on the conveyor belt, and the examiner observed a large dark mass on the bottom of the bag. The defendant insisted he did not want the bag searched further, but the airport security officer reached into the bag. At this point, the defendant exclaimed, "I don't want to fly," grabbed the bag and retreated to the nearest exit. Later the bag was searched after a dog was alerted, and authorities obtained a warrant. The court opinion referred to the Skipwith case discussed earlier and restated that an unimpeded exit would diminish the risk to skyjackers and increase attempts.

ALTERNATE VIEWPOINT

Not all courts have supported the decision contained in the Skipwith case. The court in *U.S. v. Albarado,* 495 F.2d 799 (2d Circuit), 1974, took a diametrically opposed position. They reasoned that the prospective passenger may refuse to submit to a frisk and instead forfeit his ability to travel by air because this serves the purpose of the whole search procedure, which is not to catch criminals, but rather to keep armed hijackers from getting on airplanes. As previously mentioned several times, airlines are loathe to act as law enforcement officers. They did not and still do not believe that they are responsible for the confiscation of all forms of contraband. Conversely, the Federal Aviation Regulations only required them to search for potentially dangerous weapons and materials.

Courts in the past have also wrestled with a similar issue. Remember in the Meulener case, the court determined that the defendant's Fourth Amendment rights were indeed violated. They concluded that when he was not told at the time the search was initiated that he had a right to refuse to submit to the search provided he did not board the airplane, he had not knowingly waived his rights and consented to the search. The cases appear to mix the concepts of implied consent and just how far the passenger has agreed to be searched without the need for some other substantial government need. Some defense attorneys continue to argue the language contained in Meulener, that the government interest that justifies a physical search of the person or hand baggage of a passenger in the process of boarding is lacking in cases where the prospective passenger declines to board the plane.

Attorney's holding the opposite view have honed in on some additional language in the case of *U.S. v. Davis*, 482 F 2d. 893 (9th Circuit) 1973. In this case, the court used a different justification for the searches. They supported the searches on the basis of an "administrative" search theory. They alternatively rationalized that the essential purpose of the scheme is not to detect weapons or explosives or to apprehend those who carry them but to deter persons carrying such material from seeking to board at all.

Future case law will need to engage in a balancing test to determine if and when a passenger can actually revoke his or her consent, if consent is the most accepted justification for making airport searches consistent with the Fourth Amendment. Some common sense must also be thrown into the mix. Everyone knows at this point in time that they will not be boarded unless they submit and consent to a security check at the entrance of a sterile concourse. Common sense dictates that the alternatives presented to a potential passenger approaching the screening area are so self-evident that his or her election to attempt to board necessarily manifests acquiescence in the initiation of the screening process. In other words, it is unlikely anyone in the 21st century arrives at an airport unaware that they will be searched. They still have plenty of alternatives before they reach the airport. Additionally,

they can check their luggage, or they can leave. When they do place their luggage on the conveyor belt or walk through the magnetometer, some would argue they have clearly consented.

Additionally the courts will also have to contend with whether airport searches are simply administrative searches and therefore exempt from all Fourth Amendment restrictions. The courts will have to determine whether the airport administrative search incorporates a screening process that is limited sufficiently in its intrusiveness as to be consistent with the requirement that the administrative need justifies the search. Courts will also surely consider whether the risk of successful hijacking is not necessarily enhanced by allowing a potential passenger to avoid a search on a particular occasion by electing not to fly because the potential hijacker or terrorist will just be searched on the next attempt.

One additional case deserves some collateral discussion and mention. The case of *U.S. v. Henry*, 615 F2nd. 1223 (9th Circuit, 1980) involves some unique security considerations. In this particular instance, a passenger first offered his briefcase to the ticket agent to check it. In the process he asked for the briefcase back and allegedly nervously went to the men's room. Apparently the passenger was wearing an ill-fitting wig and extra clothing, which invoked some extra suspicion. After getting the briefcase back from the agent and seeking to resubmit it, the agent advised the defendant he could no longer check baggage. This was a subterfuge to get the defendant to submit it to screening by x-ray. In some interesting language the court opined "that under the totality of the circumstances Henry, freely and voluntarily consented to the search." Additionally, they reasoned, "In determining whether Henry freely and voluntarily consented to the search we believe the crucial factor is whether Henry could have freely withdrawn the briefcase and avoided the search." Defendants are likely to litigate these issues extensively in the future.

THE WAR ON DRUGS

Continually, airline officials have attempted to reiterate the fact that the airlines are not in the law enforcement business. They repeatedly argue that the carrier's only legal obligation is to locate weapons. On occasion the courts, in frustration, have gone further. Certainly, procedures for handling attempts to smuggle contraband, when discovered by the airlines, need to be addressed. Criminal activity cannot just be overlooked. Difficult issues arise, however, in determining just how far the airlines need to go to fulfill their duty to every citizen to maintain a safe and lawful atmosphere at airports and aboard aircraft. These difficult situations are passed along by the airlines to the security officials who are expected to understand and interpret the law in every situation and to conduct themselves accordingly in every instance. Of course, constant correct decision-making constitutes a tall order in that attorneys and judges alike struggle with these issues.

In 1973, the federal courts were becoming distressed over the amounts of illegal drugs being smuggled into the United States on commercial carriers. Consequently, in a U.S. District Court in Brooklyn, New York, a judge ordered the U.S. attorney to seize a Braniff DC8. The aircraft, which had carried three persons smuggling drugs from South America was technically used in the illegal transportation of controlled substances. The federal government had already passed laws to combat the increasing influx of drugs into the United States by statutes that provided for the actual confiscation of vehicles used in transporting narcotics. This well-known law, on the other hand, had previously not been enforced against commercial carriers. The seizure in this instance did get the attention of the airlines.

This particular federal action prompted carriers to reexamine corporate policy regarding contraband items. The original legislation, permitting federal agents to confiscate boats and small aircraft, was passed in 1986. It also imposes stiff penalties on owners and operators of aircraft found to be involved in smuggling or in other fraudulent activities. The legislation was intended to take away the smugglers' means of transporting the illegal goods as well as the tangible results of extremely profitable drug business. However, airlines had not considered themselves subject to this law.

They based their interpretation of the law on theories argued in other case law. Some state courts had reasoned that a common carrier aircraft should not be seized in connection with drugs unless they had been negligent in locating the contraband. Generally, the cases were in agreement that the carrier was not responsible for drugs found on passengers, in their luggage, or in the cargo found to be properly manifested, unless the carrier had knowledge of the violation or was "grossly negligent" in the preventing or discovering it. Other judges concluded that the aircraft may not be seized and forfeited unless neither the owner, pilot, nor any other employee knew or through the exercise of the "highest degree of diligence" could have known that the contraband was aboard.

It is well-accepted law that no carrier is required to embark upon a full-scale law enforcement effort to discover contraband. The carrier must take steps to ensure that proscribed articles are not knowingly transported. Extraordinary measures to identify contraband items are not required, but just what constitutes reasonable measures will continue to be litigated. Airlines are not often able to analyze and psychically know what courts will determine to be sufficient effort to locate contraband on an air carrier. Judges are usually willing to permit searches in the name of airport security, citing a special need that benefits all of the traveling public. Extending police power to search, simply for drugs, has not been authorized and will not likely be authorized in the future.

PASSENGER RIGHTS

Additionally, airport security officials that go beyond what the courts consider reasonable searches are subject to 42 USC Section 1983. The legislation passed in 1976 authorizes a person deprived of any constitutional right as a result of state action to bring civil suit against the person who deprived him or her of that right. Even though neither the airlines nor airport security officials have yet to be considered to be engaged in "state action," they have repeatedly been sued for allegedly violating a passenger's constitutional rights.

Clearly, not ignoring contraband is much different from actively searching for it. As discussed previously, the issues are once again fogged when the airlines refuse to cooperate. Sometimes law enforcement officers have continued to pursue passenger screening with airline employees as paid informants, without the knowledge of the carrier. When airport security personnel literally have a police officer standing over their shoulder and are encouraged to engage in a search that the officer would not be permitted to effectuate, the courts will raise a red flag and exclude any evidence of contraband found. Airline security officials or the TSA, must not encourage employees to engage in this activity, and when discovered it must be stopped. Otherwise, the airlines and contract security officials will be ratifying the conduct of the informants, and the courts will not look kindly on the activity. Such conduct could result in the carrier being sued.

One of the most recent cases in this area tried to answer the question, can law enforcement authorities use airport security inspections to look for contraband that is unrelated to safety? The U.S. Court of Appeals for the Ninth Circuit in *U.S. v. $125,570 Currency*, 873 F 2nd 1240 (9th Circuit 1989) analyzed the actions of Bonnie Boswella, a flight terminal security officer at the Seattle International Airport when she noticed a dark mass in a brief case. On 5 January 1987, Wayne G. Campbell put his locked briefcase on the airport x-ray scanner. After noticing the dark mass, Officer Boswella asked Campbell to open the briefcase. At first he was reluctant but agreed to open it in a private area behind a screen. Karen Kangas, another airport security officer, searched through the briefcase and located a huge sum of money. After inquiring as to his destination, security released him. Ms. Kangas called Steve Symms, a U.S. Customs Service Officer and informed him about the briefcase and its contents. In addition, Customs was provided with a description of Mr. Campbell. Consequently, for their efforts, they received a reward of $250 for locating currency over $10,000. Later, Mr. Campbell arrived in Los Angeles where two DEA agents met him. During questioning he admitted that he had about $130,000 in his briefcase, but that the money belonged to a friend of his who had hired him to ransom a stolen painting.

The two DEA agents confiscated the briefcase. They advised Mr. Campbell he was free to go, but he decided to accompany the agents to the DEA office. At the office, the agents asked Campbell to open the briefcase. He was told that if he refused, they would simply obtain a search warrant and open it in any case. Mr. Campbell, therefore opened the briefcase and a significant amount of money was discovered as well as a lot of cigarette rolling papers and a receipt from a Seattle hotel. On the following day, a drug detection dog signaled an alert when brought into contact with the money; indicating that drugs had come into contact with the currency. As per administrative procedures, the United States filed a civil forfeiture action pursuant to the currency. In response, Mr. Campbell filed a claim to suppress the evidence uncovered by the search. The District Court denied the motion to suppress and ruled the currency was rightfully subject to forfeiture, which decision was later appealed to the 9th Circuit Court of Appeals.

The judge, Alex Koziniske, was concerned with two issues. He considered the idea that the flight terminal security officers were looking more carefully for currency in carry-on baggage because of the potential $250 reward rather than concentrating on searching for items relating to air safety. The second issue the judge considered was whether Mr. Campbell had in actuality voluntarily consented to the search at the airport because his expectation of privacy was waived only as it related to the search for weapons or explosives. The judge ruled that the search at the airport had not been conducted within the narrowly construed objectives permitting airport searches solely to ensure airline and airport security. The judge reversed the lower court and vacated the order of forfeiture. Basically, the judge had reasoned that the Air Transportation Act of 1974 requiring all passengers and carry-on property to be screened by security does not extend an exception to the Fourth Amendment to search for contraband or currency.*

In conclusion, it should be noted that a law enforcement officer may walk up to a person in an airport, or any public place for that matter, and ask questions. The officer need have no evidence or even suspicion of wrongdoing. A "hunch" is enough. The interesting questions involve what the officer may do if the individual refuses to answer or walks away. The law carefully distinguishes "encounters" from "seizures." An encounter is a simple interaction between a law enforcement officer and an individual (e.g., "Excuse me; I'd like to ask you a couple of questions…"). No evidence of wrongdoing is required. Encounters occur "if a reasonable person would feel free to decline the officer's requests or otherwise terminate the encounter" (*Florida v. Bostick,* 501 U.S. 429, 115 L.Ed. 2d 389, 111 S.Ct. 2382 [1991]). Put differently, so long as a reasonable person would feel free to walk away without answering the officer's questions, no Fourth Amendment "event" has occurred that might result in the suppression of evidence. To illustrate, an officer may ask to see a person's ticket and identification, ask questions about their travel plans, and request to search their belongings, including luggage, without the slightest scintilla of evidence of wrongdoing (*U.S. v. Odum*, 72 F.3d 1279 [7th Cir. 1995]).

NEW LAW IN THE AREA OF SEARCHES

In a departure from recent rulings supportive of police in drug interdiction efforts the *U.S. Supreme Court in Indianapolis v. Redmond*, 531 U.S. 32, 121 S.Ct. 497, 2000, has held that the use of

---

* *Notes*: Law 1990s

U.S. v. Scales (903 F.2nd 765 (1990) Tenth Circuit.

Law enforcement authorities with reasonable suspicion that a piece of luggage contains narcotics may detain luggage briefly to investigate the circumstances. Seizure of the suitcase exceeded law enforcement's authority when suitcase was seized for approximately seven hours before a drug-sniffing dog alerted them to the case.

U.S. v. Riley (927 F.2nd 1045 (1991) Eighth Circuit.

Police only need reasonable suspicion, not probable cause, to separate a narcotics defendant's suitcase from others at an airport and subject it to a dog sniff.

U.S. v. Hooper (935 F. 2nd 484 (1991) Second Circuit.

Briefly detaining a defendant and his suitcase, and exposing the luggage to a narcotics detection dog, if conducted diligently, only requires reasonable suspicion.

roadblocks designated to uncover ordinary criminal activities like drug trafficking are unconstitutional. The decision stems from a situation where police stopped a motorist at a roadblock in a high drug crime area. The man was arrested after police discovered drugs in the car. The motorist challenged the arrest, arguing that there was no probable cause for the search.

In the decision, the court distinguished between roadblocks used to deter drunken driving and illegal immigration from those used to check for random criminal activity. Whereas the previous roadblocks carry implications for public safety and immigration, the latter searches were reasoned to amount to an unreasonable search under the Fourth Amendment. Specifically, Justice Sandra Day O'Conner stated, "We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing." The case evidenced the scrutiny by the court in distinguishing between searches that serve a public safety purpose, like airport searches, and searches specifically conducted to detect criminal activity unequivocally unrelated to public safety.

Earlier caught in a fire of controversy over "racial profiling," the U.S. Customs Service began imposing limits in 1999 on its screening of airline passengers to intercept illicit drug shipments. They have implemented rules that prohibit agents from detaining airline travelers suspected of drug smuggling for more than four hours without specific approval of a federal magistrate. The policy guidelines also require customs officers to notify an attorney or friend of the passenger, if asked, if the passenger is detained for longer than two hours. In cases, where no drugs are discovered, the agents must also assist the passenger in resuming their journey.

The high technology crime landscape is another area of expanding law. Experts were closely watching a racketeering case against Nicodemo S. Scarfo. FBI agents used a warrant to break into his place of business and put either a program or some sort of "electronic bug" into his computer. According to Scarfo's lawyer, the procedure enabled law enforcement to capture every keystroke made on a user's computer (*U.S. v. Scarfo*, 263 F.3rd 80, [3rd Circuit, 2001]). They used a system called TEMPEST. Using this software, the FBI has the means to recreate the picture on a computer screen from its electromagnetic energy. Another program, called DCS 1000 enables investigators to follow a suspect's Web browsing and e-mail.

In the federal court case in New Jersey, Mr. Scarfo was using a publicly available software program named Pretty Good Privacy (PGP), which is a free-encryption program that is usable for e-mail and files. The FBI wanted the password to those files ostensibly so they could collect information on gambling and loan-sharking operations. The government argues that what they did does not rise to the level of a wiretap. Mark Rausch, former head of the Department of Justice's computer crime section, has said, "You really need to understand at what point it captured things, and how it got it back to the government, to figure out what the Fourth Amendment concerns are" (Associated Press, 2001). The defendant's motion to suppress this evidence was denied (*U.S. v. Scarfo*, 180 F.Supp 2nd 572; 2001). The case was affirmed in 2002.

Permitting law enforcement to peek into computers is the wave of the future. Providing such a tool to airport security would enable them to snoop into the computers of passengers and possibly detect information on potential terrorist activity. However, civil libertarians and the courts will likely heavily scrutinize this kind of exploratory investigation. Additionally, the courts have ruled concerning the concept of profiling in airports and searches. The Supreme Court has expressly approved the use of "probabilistic" profiles in the airport setting to identify potential drug couriers or terrorists. Generally, individuals may be searched based on their identification through the use of a profile because the profile provides the officers with reasonable suspicion to stop a suspect. Profiles are valid as long as they leave no room for subjective interpretation and are not applied in a discriminatory fashion.

NEW TECHNOLOGIES AND THE LAW

Sometimes, new technologies change everything. The use by drug enforcement officials and law enforcement in general of forward-looking infrared devices, or FLIR, is one of those innovations.

Law enforcement has used the equipment, often mounted on helicopters, not only to assist ground law enforcement during dangerous chases, but also to establish evidence of indoor marijuana cultivation. The device detects differences in the surface temperature of objects, and because marijuana needs high-intensity grow lights to successfully grow indoors, FLIR can detect the huge amount of heat radiated.

The constitutionality for use of the FLIR has been upheld on several occasions. The circuit court in the case of *U.S. v. Pinson*, 24 F3d 1056 (8th Circuit, 1994) believed that the defendant had no legitimate expectation of privacy in the heat emanating from his house. The court took into account the fact that the only information acquired by the FLIR was data. The 8th Circuit developed a two-pronged test for determining what constitutes an expectation of privacy. A legitimate expectation of privacy is considered to exist where "…the individual manifests a subjective expectation of privacy in the object of the challenged search and society is willing to recognize that subjective expectation as reasonable." The Supreme Court, however, ruled that special heat-seeking devices require a warrant when seeking to find home-grown marijuana plants; changing the legal landscape completely.

The courts have analogized the expectation of privacy argument to the use of canines and also the placement of garbage left on the curb. These situations have been thought not to have a reasonable expectation of privacy attached to them. In the case of the garbage, it is left out to be taken away. In the case of the dogs, the court compared the dogs to the FLIR, by claiming that the dogs merely sniffed the odor emanating from the bags. The court also specifically stated that "none of the interests which form the basis for the need for the protection of a residence, namely the intimacy, personal autonomy, and privacy associated with a home, are threatened by thermal imagery." Consequently, the use of the FLIR could easily be utilized for airfield security without much concern about constitutional challenge.

As is common in the law, other courts have disagreed. The Fifth Circuit court in *U.S. v. Ishmael*, 843 F. Supp. 205, affirmed 48 F.3d 850 (1995) reached an opposite conclusion. They reasoned that the FLIR cannot tell the difference between legal heat and heat used to grow marijuana. For that matter, even the excessive heat radiated from grow lights could be being used to grow basil or a host of other legal plants. They therefore reached the conclusion that the FLIR is more intrusive than a dog. Additionally, the dog's sense of smell is clearly not as technologically precise as the FLIR, which can detect miniscule heat graduations. Reviewers of both arguments have tended to continue to support the concept that dog-sniffing, FLIR, and garbage searches are all fair game for law enforcement as investigative techniques. The dogs and the FLIR especially both involve sense-enhancing equipment. The degree of that detectability is really not an issue.

The first thermal imaging case was considered in 1991. In *U.S. v. Penny-Feeney*, 84 Calif. L. Rev. 1437, the defendant and her husband were growing marijuana in her garage. She was arrested due to a search warrant issued after police measured the heat emissions from her home from a helicopter equipped with a thermal imaging device. The Supreme Court affirmed the conviction on the grounds that no search had occurred because the defendant had not attempted to disguise the heat levels emanating from her garage, and thus did not display a subjective expectation of privacy. The Court likened the emanation of heat waste to the concept of placing one's bagged trash on the sidewalk for collection, theoretically available for anyone to examine. The Court also compared the emission of heat to the emission of odors, in the context that drug-sniffing dogs can detect odor emissions through smell without performing an invasive search (Laba, 1996).

Another emerging technology that may have much in common with thermal imaging is passive millimeter wave imaging. This method utilizes a special type of camera, "which emits passive millimeter waves through an individual's clothes, as well as through most building materials, to detect concealed weapons." It is similar in concept to the metal detectors or magnetometers used to detect weapons at airports, although it is more portable and can be used from a distance, rendering it capable of very invasive monitoring. One possible trend in search and seizure may be toward increased restrictions in photography of individuals in public locations. California and Louisiana have both recently passed legislation aimed at "peeping toms" or "video voyeurs," individuals who

videotape or photograph others in locations such as public dressing rooms or restrooms in varying stages of nudity. Other states, such as New Jersey, have also passed laws prohibiting surreptitious video recording under certain circumstances (Rotherburg, 2000).

Other technological innovations have presented additional court reviewable topics. U.S. Customs officials at six U.S. airports are currently using the Body Search x-ray to examine drug-smuggling suspects. The system basically sees through clothes. Specifically, passengers who cause customs officials to become suspicious are required to choose between a patdown search or to stand in front of the machine that arguably renders an image of the suspect naked.

Customs officials "…had hoped that the new technology would help quiet a controversy over the agency's searches, which civil libertarians contend focus too much on minority passengers. A hands-off approach, customs officials reasoned, would seem less intrusive" (Allen, 2000). However, the technology is so good it reveals just about everything. In other words, airport security officials might be able to view a little more than the average citizen is personally inclined to show to a stranger. This modesty has nothing to do with the carriage of weapons. Pulsed radar scanners, which pretty much produce an image of an individual's naked body, are clearly intrusive.

In another area, the increased popularity of the Internet has generated changes in the law. Different Internet applications provide opportunities for electronic monitoring and search, one of the most controversial being the monitoring of e-mail. As previously discussed in the Scarfo case, one subject of frequent debate is the issue of whether e-mail messages should be able to be encrypted to a level indecipherable by the government. Currently PGP software can legally encrypt messages that cannot be cracked by the government. The government is wary of this standard, due to the fact that it might conceivably endanger national security by preventing the interception of messages from criminals.

Satellite technology is also important for the future of search and seizure law. One use of satellite technology might be to take aerial photographs. Another satellite use that may become important in terms of electronic monitoring is the global positioning system (GPS), which uses the signals of orbiting satellites monitored by the U.S. Air Force to calculate the position of articles on earth equipped with GPS receivers. Intelligent Vehicle Highway Systems (IVHS) is yet another application of GPS. This system would place GPS receivers in passenger vehicles, which could then be used to locate and monitor the vehicles and prevent individuals from driving under dangerous conditions.

The Republican administration under President George W. Bush might also be a factor in increasing restrictions on electronic monitoring. It is worth noting that the majority opinion in *Kyllo v. U.S.*, 2001 U.S. LEXIS 4487*,* that a warrantless wiretap search is not permissible, was authored by Supreme Court Justice Antonin Scalia, a conservative Republican. It is a distinct possibility that these factors may lead to further decisions restricting the use of technology in search and seizure. Conceivably, future decisions in the regulation of other new technologies might move away from the photographic model, toward the model of the restrictions on wiretapping and thermal imaging, providing the maximum protection against search and seizure reasonable under the law of the privacy (*Kyllo v. U.S.*. 2001 U.S. LEXIS 4487. No. 99-8508. U.S. Supreme Court. 2001. Online. Lexis-Nexis Academic Universe. 10 August 2001.)

In summary, the courts currently do not require a physical intrusion to determine that a search has taken place. However, how much of an intrusion, what degree of expectation of privacy is involved, and reasonableness of the search will all play into any future court analysis. The problem evolving is that as technology improves, it becomes easier to characterize information as exposed because technology can now expose it. By systematic practice, expectations of passengers have been conditioned to expect some sort of search. Just how intrusive a search is permissible is still the question to be litigated fully.

CONCLUSION

Admittedly, the law is a complicated matrix of sometime conflicting legislation, policies and opinions. However, every security official, whether a state agency or privately employed individual, should have a basic understanding of the Fourth Amendment and how it applies to airport searches. Because the Fourth Amendment is currently only applicable when a state agent is conducting the search, private security must be careful not to wander into discretionary authority that rightfully belongs to the police. Whether contract airport security personnel continue to fall into the nonstate agent category has so far generally been decided in the negative. However, the distinction between private and public "policing" is blurring, and it will remain to be seen if this decision persists. The water becomes even murkier when the airport security officer is an off-duty police officer or a federal employee.

The Fourth Amendment also only protects passengers against unreasonable searches and seizures, not all searches. Additionally, just what is considered reasonable is often defined in terms of how serious the threat is conceived to be. During the Persian Gulf War, the threat was accepted as being significantly higher than normal, and the public and the courts were willing to adjust the expectations of privacy. This acceptance was clearly expanded again after 11 September. Another issue pertains to how much privacy a passenger expects to receive at an airport. They expect to be searched for dangerous weapons and explosives because that is the public policy function of the search. Therefore, it may be perfectly acceptable to have a passenger screened by a metal detector and his or her carry-on luggage scanned. Having the passenger literally undress in front of an x-ray machine may result in a different conclusion. The courts, consequently, will likely continue to evaluate the extent of the permissible intrusion. Advances in technology will likely strain the courts' patience with the airline wish for speed versus the level of intrusion.

There are outright exceptions to the Fourth Amendment including administrative searches, border searches, and consent searches. Generally, the judiciary has concluded that passengers do consent to airport searches but also seem to accept that they are administrative in nature and serve a distinct public need. If the courts believe that security has gone too far, the exclusionary rule may come into play. It is meant to keep the state, via its police function, at an appropriate distance from individual rights. If the state chooses arbitrarily to overstep its bounds, the rule will deny them the success of a conviction against the perpetrator of the alleged crime. According to many criminologists, the rule has proved an effective deterrent, but the rule has also undergone much criticism. It is difficult to account for just how many police officers or federal agents restrained their conduct fearing the implications of the exclusionary rule. Consequently, some exceptions have been carved out. Most importantly; the good faith exception, inevitably discovery exception, and the exigent circumstance exception are the most frequently utilized. Whatever the ultimate decision of the courts regarding a particular search or procedure, the public's attitude toward the search will play a large part in determining its acceptability.

The reasonableness and extent of that attitude from the public can become strained even in today's tense environment. The perception that it is unreasonable to search "little old ladies" whereas "suspicious characters" are permitted to board unhindered will continue to pose a challenge to security officials. Additionally, any legal search can quickly become illegal when security goes outside the boundaries of reasonableness. The allegation of the selection of only "good-looking" flight attendants for patdown searches at Sky Harbor Airport in Phoenix is a good example. Most people do not mind being searched to feel more secure when they fly. However, when the searches provide neither security nor a sense of security, they lose their public safety purpose and the support of the traveling public.

REFERENCES

Allen, Michael, "Are These x-rays Too Revealing?" Targeting Drug Smugglers. Airport Screening Device Sees Right Through Clothes," *Wall Street Journal*, Thursday, 2 March 2000, pp. B1, B4.

Associated Press, "FBI's Electronic Snooping Headed for Court Test," Star Tribune, Minneapolis, MN, Sunday, 29 July 2001, pg. A13.

Hess, Karen M. and Henry M. Wrobleski, *Police Operations Theory and Practice*, St. Paul, MN, West Publishing Co., 1997, pg.122.

"Jury's Mixed Verdict in Cop Trial," *UPI Online*, 3 April 1998.

Laba, Jonathan Todd, "If You Can't Stand the Heat, Get Out of the Drug Business: Thermal Imagers, Emerging Technologies, and the Fourth Amendment." *California Law Review* October 1996: 84 Calif. L. Rev. 1437. Online. Lexis-Nexis Academic Universe. 10 August 2001.

Rolando V. Del Carmen, "Criminal Procedure for Law Enforcement Personnel," Monterey, CA., Brooks/Cole Publishing CO., 1987, pg. 63.

Rotherburg, Lance E., "Re-thinking Privacy: Peeping Toms, Video Voyeurs, and Failure of the Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space." *The American University Law Review* June 2000: 49 Am. U.L. Rev. 1127. Online. Lexis-Nexis Academic Universe. 10 August 2001.

Sauls, John Gales, "Emergency Searches of Premises," Part I, *FBI Law Enforcement Bulletin*, March 1987, pg. 23.

U.S. Constitution, U.S. Government Printing Office, 1989-249-097.

12 Foreign Airport Security
Comparison of U.S. Law and Foreign Domestic Law — Lessons Learned

NEWS

1987/1988: The U.S. Department of Justice files suit (*PLO v. U.S.*, 695 F. Supp. 1456, 1987) in federal district court seeking to close the PLO's observer mission in New York City. Four members of the IRA successfully challenge the British Anti-Terrorism law in the European Court of Justice.

1988: An Italian court sentences Abu Nidal to life imprisonment for his role in the 1985 massacre at the Rome airport in 1985. He is tried "in absentia." He is found dead in Iraq in August 2002.

20 October 2000: A French Appeals Court rules that Libyan leader Muammar Khaddafi can be prosecuted for the bombing of a French DC-10 airliner over Niger in 1989 in which 170 people died.

February 2001: A Saudi Court sentences an army officer to 70 lashes for using his mobile phone on a domestic flight, despite warnings from the crew to desist from using it.

15 July 2005: One of the bombers in London's Metro attacks makes a direct phone call to a suspected recruiter for an extremist group in New York. Authorities reveal records that show Mohammed Sidique Khan, the eldest of the bombers and now believed to be the field commander of the attacks, called a person who is associated with the Islamic Center, a mosque in Queens, NY. Yet, a member of that mosque claims they had no knowledge of the phone call.

INTRODUCTION

Certainly the quality and quantity of security in foreign airports varies from country to country. Title V of the International Security and Development Act of 1985 authorizes the U.S. Secretary of Transportation to determine that an airport maintains effective security measures. Basically, if a condition exists that threatens the safety or security of passengers, aircraft, or crew traveling to or from a foreign airport, the Secretary of State is supposed to be notified. The Transportation Security Administration (TSA) assesses, in conjunction with local host government authorities, the security of airports that are served by U.S. carriers or served by foreign carriers flying directly to the United States. Assessments are based on the provisions of International Standards and Recommended Practices of Annex 17 of the Chicago Convention supplemented by European Union Document 30.

The Federal Aviation Administration (FAA) annually evaluated many of the airports worldwide, usually around 200 in any given year. The United States has no jurisdiction to mandate that foreign

airport managers comply with U.S. regulations or suggestions. Many foreign airports simply refuse to accept U.S. standards or ICAO Annex 17 requirements, and others do not have the financial resources to implement any well-intentioned efforts. An example of the difficulty can be shown by a particularly complex choice for some policymakers. One airport in a third world country explained they had no x-ray equipment or scanning devices because their government was currently saving money to get a proper x-ray machine for the hospital. Aircraft from these impoverished nations still fly into the larger and more industrialized nations' airports and present significant security challenges. The United States has taken a hard stand against terrorism and has legislated laws to support that proactive stand. The level of precautions taken at U.S., European, and other industrialized countries' airports are not the universal norm, and even those standards have not prevented terrorist attacks. The government attempts to assess foreign airports along several criteria. Ground security is one of them.

GROUND SECURITY

Adequate security on the ground has increased in importance over the years. It is clear that hijack attempts or incidents had been moving from the actual aircraft to the more open terminal. Despite the 11 September 2001 hijackings, the terminal remains a high-threat area. The killing of 25 people and wounding of another 76 at Tel Aviv's Lod Airport on 31 May 1972 was one of the first indications that passengers on the ground were easy targets of machinegun-wielding terrorists. Additional attacks in the Rome and Athens airports in December 1973 and the Rome and Vienna killings in December 1985 finally woke the world up to the increased need for sufficient ground security. The incident at Los Angeles International Airport over the July 4th weekend 2002 reminded the public once again of this particular threat. Unfortunately, it is often the wrenching pictures on television and in newspapers that awake the general public to the need to spend the funds to provide satisfactory protection. It is also significant to point out that the above airport incidents in Rome, Vienna, and Tel Aviv were the result of terrorists spraying automatic weapons fire in the terminal while passengers were checking in. Consequently, efforts to screen passengers and their carry-on baggage would not have avoided the consequences of the attacks.

Some airports, due to the fact that they have been previous targets, have implemented improved and demanding security procedures. At the Frankfurt International Airport, for example, security appears tight even to the most casual observer. Armed guards patrol the entire airport, and their presence is obvious to any passenger arriving to initially check in. Additionally, only passengers with tickets are permitted outside of the main check-in area. At arrival, no curbside checking is available. All passengers must check in at the counter to receive a boarding pass. Once through the first screening, passengers must also clear immigration and customs where their identities can be again checked and verified. These added procedures, required for international travel, all have secondary security benefits. However, individual airlines have added even more security. In Frankfurt, Delta Airlines rechecks carry-on baggage at the gate and reverifies passenger identities on other international flights before proceeding to the aircraft.

Some other overseas airports also take security quite seriously. At Narita Airport outside Tokyo, Japan, armored personnel carriers are stationed around the entire facility; indicating to everyone that they mean business. Singapore, Sydney, and Seoul also have taken special efforts to make their airports safe. The same cannot be said for Manila, Lagos, and many others. Athens airport had repeatedly come under severe criticism for the ineffectiveness of its security processes. Ever since the hijacking of Trans World Airlines Flight 847 in June 1985, Athens officials have attempted to upgrade their security. Travel advisories have been published and lifted over the last 20 years; however, laxity was still prevalent. In October 1986, the Greek government received a $5 million loan for security improvements, after which perimeter fences were upgraded and armored cars were stationed at exits. However, the Greek government had still not given the needs of Athens Hellenikon Airport much priority in their budgeting process, regardless of the thousands and thousands of

international passengers transiting this particular European airport. The new airport, which opened in March 2001, was still plagued with problems, especially concerning the access roads to the airport (Athens Sparta Airport Not Ready to be Opened 2001). Experts continued to criticize the Athens airport management and concerns as the Olympics approached; however, the games went off without a security hitch. In fact, since the advent of the Olympic Games in 2004, the Athens airport has made a remarkable turnaround. Their increased efforts have established a much safer and secure airport. The U.S. government regularly publishes their assessment of airports serving U.S. aircraft and aircraft servicing U.S. ports of entry.

AMERICAN ASSESSMENTS

On 8 August 1985, Public Law 99-83, the Foreign Security Act was signed into law. Title V, Part B amended Section 1115 of the Federal Aviation Act of 1958. It directed the Secretary of Transportation to assess the effectiveness of security measures at all foreign airports. The legislation covered all airports being served by U.S. air carriers, those foreign airports from which foreign air carriers serve the United States, those foreign airports that pose a high risk of introducing danger to international travel, and other airports as the Secretary should assess. The Act also obligated the Secretary of Transportation to take appropriate action with respect to airports that do not maintain and administer effective safety or security measures. The Secretary subsequently delegated the FAA the responsibility to implement the provisions of Public Law 99-83. The International Aviation Safety Assessment Program (IASA program) was developed via public policy in August of 1992 (14 CFR Part 129, as amended 2000). It focuses on a country's ability, not the individual air carrier, to adhere to international standards and recommended practices for aircraft operations and maintenance established by the United Nation's technical agency for aviation, ICAO.

Foreign airport assessments continue to be handled by the former Civil Aviation Security section of the FAA, which is now a part of the TSA. The Office of Inspections within the FAA will also continue to assist with some functions and review the effectiveness of all TSA programs. There are only two choices for inspectors when assessing airports overseas. The foreign airport either complies with ICAO standards or does not. A Category 1 airport exists when a country's civil aviation authority has been assessed and has been found to license and oversee air carriers in accordance with ICAO aviation safety standards. On the other hand, Category 2 airports do not. A determination is made whether the airport does not provide safety oversight of its air carrier operations in accordance with ICAO standards. The government recognizes the following deficiencies (http://www.faa.gov/avr/iasa/iasadef5.htm pg. 1):

- The country lacks laws or regulations necessary to support the certification and oversight of air carriers in accordance with minimum international standards.
- The country's Civil Aviation Authority (CAA) lacks the technical expertise, resources, and organization to license or oversee air carrier operations.
- The country's CAA does not have adequately trained and qualified technical personnel.
- The country's CAA does not provide adequate inspector guidance to ensure enforcement of, and compliance with, minimum international standards.
- The country's CAA has insufficient documentation and records of certification and inadequate continuing oversight and surveillance of air carrier operations. Each airport's overall safety and security procedures are reviewed. Trained inspectors make determinations whether the in-place programs are efficient and fully supported by the local CAA. Safety and security programs in name only do not withstand scrutiny.

As stated, the assessment program became official policy in August 1992. It was published in the Federal Register, Vol. 57, No. 164, 24 Aug 1992. The purpose of the overall program was to ensure that all foreign carriers that operate to and from the United States are competent to do so. After a

trial period, the formal rules were formulated and implemented. Any foreign air carrier desiring to conduct air operations into the United States needs to file an application with the U.S. Department of Transportation (DOT). The foreign carriers apply for a foreign carrier permit in accordance with the Federal Aviation Act, 49 U.S.C. 41302, Parts 211 and 302. The Code of Federal Regulations (CFR) implements and codifies the rules in 14 CFR 211, 302. Additionally, 14 CFR Part 129 specifies that the carrier must meet the safety standards prescribed in the Chicago Convention, Annex 6. Before the DOT actually issues the permit, the government evaluates the candidate's capability to provide safety and continuing oversight for its international carriers. Assessment teams are regularly sent to the CAA of the applicant country, and evaluations are forwarded to the DOT for review and action.

To effectuate their responsibilities, the government conducts periodic inspections of the applicable airports. Assessments are made and threats are analyzed in conjunction with the Department of State. U.S. authority is limited by the fact that the foreign airport authorities must be willing to cooperate. The United States really only acquires some specific jurisdiction over foreign carriers on the last leg of their flight directly to the United States. All other evaluations are done on a cooperative basis. Over 300 airports are routinely evaluated and meet the criteria established by the government for a safe airport. Obviously, due to limited resources of funds and personnel, not every airport that should be periodically assessed can be as often as the government would prefer. See http://www.faa.gov/safety/ programs_initiative /oversight/iasa/media /iasaws.xls. for 2008 assessments.

Security at foreign airports is governed by Title 49 of the U.S. Code, Section 44907, which requires the Secretary of Homeland Security, through the TSA, to conduct security assessments at foreign airports. If the Secretary of Homeland Security determines that security at an airport is not effective, he is required to notify the foreign government of the findings and recommend corrective action. Specifically, the Secretary must: (a) publish the identity of the foreign airport in the Federal Register, (b) post the identity of such airport at all U.S. airports that regularly provide scheduled air carrier operations, and (c) notify the news media of the identity of the airport (49 U.S.C. 44907[d]). In addition, the statute requires all air carriers providing service between the United States and the airport to provide written notice of the determination, either on or with the ticket, to all passengers purchasing transportation between the United States and the airport (49 U.S.C. 44907[d] [1] [B]. TSA representatives regularly assist airport authorities at foreign airports in bringing the airport up to international standards.

The TSA evaluates the security of foreign airports and air carriers that service the United States regularly. Of the 128 foreign airports that TSA assessed during fiscal year 2005, TSA determined that about 36 percent complied with all applicable security standards, whereas about 64 percent did not comply with at least one standard. At that time, the security deficiencies identified at two foreign airports (Bandara Ngurah Rai International Airport, Denespar, Bali, Indonesia and Port Au Prince Airport in Haiti) were so ineffective that the Secretary of Homeland Security notified the public. Of the 529 overseas air carrier inspections conducted during fiscal year 2005, about 71 percent did not have any security violations, and 29 percent had at least one security violation. The TSA has the authority to take the following enforcement actions: warning letters, correction letters, or monetary fines violations.

DIVERSION AIRPORTS

Stansted Airport is London's third largest airport (see Figure 12.1). It is little known to the international traveler because most passengers normally arrive at the gateway airports of Heathrow, outside London, and Gatwick, South of London. Located slightly east of London, Stansted Airport has become the choice of airport security officials dealing with a hijacked aircraft. In an effort to handle a developing hijacking incident without disrupting the major airports, authorities have attempted to hornswoggle the terrorist demanding that an aircraft be flown to one of the two larger airports, by diverting it to Stansted. In combating a hijacking, it is an obvious and valuable tool to be able to

FIGURE 12.1 Stanstead is London's third international gateway and one of the fastest growing airports in Europe. The airport currently handles more than 14 million passengers and plans to grow to a capacity of 25 million passengers by 2010. It is also an exceptional diversion airport manned by trained and coordinated ant-terrorist security teams.

direct the hijacked aircraft to the airport of choice of the security officials as opposed to the hijackers. Despite the perceptions 11 September has created, few hijackers are expert aviators.

Stansted was first used to receive a hijacked aircraft in 1975, when a BAC 111 was hijacked on an internal flight between Manchester and London. The pilot, as part of a prebriefed alternative in case of a hijacking, managed to divert to Stansted instead of Heathrow. The hijacker had demanded money and wanted to be flown to France. Not being a pilot, the hijacker was convinced that the aircraft had actually been flown to France when in reality it was still in England. Many lessons were learned from this initial effort to be in more control of an ongoing hijacking situation.

For example, it became imperative that airline personnel and ground security needed to be able to quickly coordinate their responses. Security officials began to work out the number of police on hand to deal with a specific emergency and to create rendezvous points for emergency services. As a result of lessons learned, communications between pilots and ground personnel security were greatly improved, and designated command posts were firmly incorporated into procedures.

The importance of training all personnel and maintaining a high level of response capability was reinforced during a second hijacking. The hijacked aircraft, originating in central Africa in 1982 aboard an Air Tanzania Boeing 727, eventually made its way to Stansted after traveling a circuitous route throughout Europe. In this particular situation, a fully coordinated response team awaited the aircraft. The team consisted of a combined police and military operation with the elite British Special Air Service (SAS) standing by to mount a hostage rescue operation if negotiations failed. In

protracted negotiations including the Tanzanian High Commissioner, the crisis was settled peaceably approximately 24 hours after it began.

By 1996, the hijacking team was ready and waiting for a Sudan Airways A310 Airbus originating in Khartoum that had been hijacked by Iraqi terrorists. They had demanded that the plane be flown to Italy, but due to insufficient fuel the plane was forced to land in Cyprus. After becoming airborne again, the pilot was prepared to fly the aircraft to Stansted, and a well-prepared team settled the crisis peacefully and professionally. Such prearranged diversion airports and supporting teams should become standard procedure. Not only does a well-trained and prepared team meet and greet the hijacked aircraft, but also the entire situation is centered away from other standard airport facilities precluding the need to stop air operations and take other precautionary measures.

LEGAL REMEDIES

International treaty efforts to combat terrorism have already been discussed. The U.S. domestically legislated approach has not necessarily been adopted by other nations. In other words, other nations have legislated quite different domestic legal tools to address the problem. It is worthwhile to explore the U.S. legislation as well as some of these different methods. Some have arguably been more successful than others. Additionally, the ever-increasing threat from nuclear, biological, or chemical terrorism has heightened the attention the public has given to law enforcement and general criminal justice efforts.

On the eve of the bombing of the federal building in Oklahoma City, Congress sent a compromise version of antiterrorism legislation, The Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) to President Clinton for signature. He signed it into law. As discussed, just how to define terrorism and who exactly should be considered a terrorist has created much controversy. In the last eight years the federal government has once again become focused on terrorism, both domestic and international. Prior to 11 September, this renewed attention was already the result of an increased threat from nuclear proliferation, ethnic cleansing, and continued religious wars. Many nations unfortunately have been brutally forced to refocus on the shady world of terrorism. No country is immune.

The AEDPA was formally adopted on 24 April 1996. In addition, the United States is party to over 100 extradition treaties (Janis, 1993, pg. 348). Overall, "extradition treaties provide that a state is obligated to extradite persons to another state when the other state shows that the person is sought for trial for a crime allegedly committed within the jurisdiction of that state for punishment for a crime committed in that state after conviction and flight from that state." (Restatement of Foreign Relations Law of the United States, 1987, Pg.475.) However, extradition has historically been subject to several exceptions including the concept of when the offense is shown to be political in nature. Terrorists have used this exception to their advantage. Persons accused of terrorism have claimed that they are engaged in political activities and fall within the exception. The tradition has survived many challenges and remains in effect due to the strong inclination of several nations to provide refugees political asylum.

How the treaties define political offense is open to interpretation. In essence, the requirements of the exception include the following:

1. That the conflict for which the accused claims support is ongoing
2. That the act in question is part of the conflict
3. That the accused is a member of an organization of defined structure and command
4. That the accused is acting on orders from someone within the organization

Because the Irish Republican Army (IRA) claims to fall within this definition, naturally, the British have failed to recognize it. The United States and Britain amended their extradition treaty accordingly. In 1985, the Supplemental Extradition Treaty went into effect (Janis, 1993, pg. 349).

The new version excludes several offenses from the "political exception" parameters. Specifically, the law permits extradition in cases of politically motivated crimes of murder, manslaughter, kidnapping, hostage taking, and the manufacture of explosives and use thereof. It effectively discounts the political offense exception. As is usually the case, powerful nations can interpret international law when it suits them. The British have taken a hard stand against the IRA, and during the Reagan administration every effort was made to support them, hence the new extradition treaty.

Even after passage of the AEDPA, the Clinton administration sought stronger legislation against terrorism. In July 1996, the administration reintroduced two measures previously removed from the AEDPA. The administration sought expanded federal roving wiretap authority and the required use of taggants in explosives (Atlas, 1996; Airline Security Crackdown is Stalled on the Runway: Despite Federal Rhetoric Little Has Been Accomplished, 1996). Simultaneously, Vice President Al Gore was heading the commission to review all aspects of aviation safety and security. After the commission published its findings, the Aviation Security and Antiterrorism Act of 1996 was passed. Unfortunately, the House version, under pressure from the National Rifle Association and the American Civil Liberties Union, dropped the wiretap and taggant provisions. The British and others have been much more successful in enacting stronger antiterrorism legislation.

LEGISLATION AFTER 11 SEPTEMBER 2001

The Aviation and Transportation Security Act established a new TSA within the DOT responsible for security for all modes of transportation and headed by a new under secretary. The bill provided that the federal government would assume responsibility for all passenger and baggage screening at commercial airports in the United States as soon as possible. Within a 12-month period, the TSA hired, trained, and deployed federal screeners, federal security managers, federal security personnel, and federal law enforcement officers. In addition, five airports were allowed to participate in a pilot program to experiment with private contracting. After two years in the program, all airports will be allowed the option of having the federal government contract with private firms to provide aviation security services if the Secretary of Transportation determines that this will provide an equal or greater level of security. The law is supposed to require the Administration to adopt new stricter standards for screeners. All screeners are to be U.S. citizens. It also requires the Federal government to conduct background checks on all individuals with access to secure areas within an airport. The measure allows for expedited procedures to be used to get important security directives in place, including a provision that 100 percent of checked baggage be screened by explosive detection equipment. It also requires the deployment of Federal Air Marshals. Furthermore, it also directs the new under secretary, in consultation with the FAA, to take action to strengthen cockpit doors and now provides for pilots to carry firearms to defend their aircraft.

In conjunction, the legislation mandates a fee to be charged to cover the cost of providing the aviation security services. The fee will be based on the number of times a passenger boards a plane during the course of travel, but will be capped at $5.00 per one-way trip. Any additional funds needed will be authorized to be appropriated or may come from a fee imposed directly on the airlines. The intent of Congress was also to establish an aviation oversight board composed of representatives from other agencies (DOT, Department of Defense, Department of Justice, Department of Treasury, and the CIA, the National Security Council, and Homeland Security) of the federal government to share intelligence information and oversee the actions of the new under secretary. The Aviation and Transportation Security Act or S. 1447 Sec 118 authorized funding and provided flexibility in the use of the Airport Improvement Program (AIP) and Passenger Facility Charges (PFC) funds to help airports pay for the increased security costs. The bill (S.1447) was signed into law 19 November 2001 as legislation passed by the 107th Congress. The bill, as previously discussed at length, authorized appropriations for fiscal years 2002 through 2005 for aviation security activities. It also authorized appropriations for fiscal year 2002 to the Secretary to make grants to or other agreements with air carriers (including intrastate air carriers) to do the following:

1. Fortify cockpit doors to deny access from the cabin to the pilots in the cockpit;
2. Provide for the use of video monitors or other devices to alert the cockpit crew to activity in the passenger cabin
3. Ensure continuous operation of the aircraft transponder in the event of an emergency
4. Provide for the use of other innovative technologies to enhance aircraft security.

Another piece of legislation, H.R. 3210 created a temporary industry risk-spreading program to ensure the continued availability of commercial property and casualty insurance. The bill became law on 26 November 2002 as Public Law No: 107-297. The intent was to establish a means for insurance companies to reinsure for terrorism-related risks to limit immediate market disruptions, encourage economic stabilization, and facilitate a transition to a viable market for private terrorism risk insurance. According to the legislative history, in the event of a terrorist attack, the Secretary of the Treasury will determine when losses from one or more acts of terrorism result in insurance claims industry wide of over 1 billion and up to 20 billion U.S. dollars during the coverage period of the measure. This provision is modeled in part on existing state insurance programs for solvency guarantee funds and catastrophic disaster pools. After such a determination, the Treasury will pay 90 percent of the claims (with 10 percent of losses retained by the insurers) on the first dollar of the coverage. The Secretary of the Treasury must thereafter assess all commercial property and casualty insurers to recoup the costs of the Treasury payments. If losses in the coverage period are less than $1 billion industrywide, the bill provides company-specific trigger levels for cost sharing with a per company deductible to protect smaller insurance companies. If losses exceed $20 billion industrywide, the Treasury will pay 90 percent of all claims up to financial assistance of $100 billion over the covered period. The legislation gives the Secretary the power to recoup these payments through surcharges on commercial property and casualty policy premiums on a weighing of economic conditions and other factors. These provisions expired at the end of 2002, although the Secretary extended the program through 2005, and it has been again revalidated.

Additionally, H.R. 3004, the Financial Antiterrorism Act of 2001, was to provide the United States with new tools to combat the financing of terrorism and other financial crimes. The measure contained provisions to strengthen law enforcement authorities, as well as to enhance public-private cooperation between government and industry in disrupting terrorist funding. Specifically, the measure contained the following:

1. Made it a crime to smuggle over $10,000 into or out of the United States and to transport more than $10,000 in criminal proceeds across state lines
2. Gave the Justice Department new prosecutorial tools to combat terrorist-related and other money laundering through U.S. financial institutions
3. Provided statutory authorization for the Financial Crimes Enforcement Network (FinCEN), which analyzes reports filed by financial institutions on currency transactions and suspicious financial activity
4. Set up a unit in FinCEN directed at oversight and analysis of hawalas and other underground black-market banking systems
5. Made it a crime to knowingly falsify one's identity in opening an account at a financial institution and directed the Treasury Department to develop regulations to guide financial institutions in identifying account holders
6. Directed the Treasury Department to establish a secure Web site to receive electronic filings of Suspicious Activity Reports (SARs) and provided financial institutions with alerts and other information regarding patterns of terrorist or other suspicious activity that warrant enhanced scrutiny
7. Required the Treasury Department to report quarterly to industry on how SARs are used to assist law enforcement in combating terrorism and other crimes

8. Authorized intelligence agency access to reports filed by financial institutions and expanded government access to consumer financial records and credit histories
9. Created a public-private task force on terrorist financing
10. Set a 31 December 2001 deadline for proposed regulations on SARs reporting requirements for broker-dealers and authorized the Treasury Department to require SARs of commodity futures traders
11. Authorized the Secretary of the Treasury to impose "special measures" if a foreign country, financial institution, transaction, or account is deemed to be a "primary money laundering concern"
12. Prohibited U.S. financial institutions from providing banking services to "shell" banks that have no physical presence in any country nor any affiliation with a financial institution
13. Required greater due diligence for certain correspondent and private banking accounts
14. Authorized the Treasury Department to regulate concentration accounts
15. Required financial institutions to have antimoney-laundering programs
16. Authorized the President to impose certain sanctions (including limiting access to the U.S. financial system) against foreign governments that refuse to cooperate in law enforcement efforts against terrorism and money laundering
17. Updated U.S. anticounterfeiting laws. Unfortunately, the bill never became law and was only passed by the House. Such measures will likely be reconsidered after the 2008 election.

ANTITERRORISM LEGISLATION IN THE UNITED KINGDOM

Because of continued violence in Northern Ireland, the British considered a criminal justice means of handling the prolonged situation. In 1972, Lord Chief Justice Diplock was sent to Northern Ireland to review the processes in place and to make recommendations. He investigated how to use criminal law to combat terrorism. His recommendations were implemented, and they became some of the most controversial antiterrorism policies in the world.

The police and the courts were given increased powers, some would say excessive. Security forces were given the power to arrest and jail individuals suspected of being terrorists without a warrant or a trial. Courts, in conjunction, were given the power to hold secret trials and collect testimony without any opportunity to cross-examine. A special type of martial law to supplement the procedures, the Special Powers Act (1922), was first enacted by a semiautonomous Irish parliament and renewed each year until 1933 when it became a permanent part of the legal code in Northern Ireland. After the Diplock report, the Emergency Powers Act was passed; taking only a slightly different approach. It remained in existence from 1973 to 1995. This law united the police, the military, correctional departments, and the courts into a cohesive antiterrorist unit. This act was not legislated in an "Irish parliament" but came directly from Britain. According to one scholar, the purpose of the act was to shift the burden of proof from the state to the defendant and to shift more control away from the judicial branch of government and channel it toward the executive branch (Finn, 1987).

The United Kingdom Prevention of Terrorism Act of 1984 granted some extraordinary powers to the executive branch. They were granted the powers of arrest, detention, and exclusion. They also "proscribed" membership in the IRA and the Irish National Liberation Army (INLA). The Act made contributions to acts of terrorism and withholding information about acts of terrorism outright criminal offenses, and expanded the powers of police in carrying out searches of travelers. Internment became an administrative process. The suspect could be held for 28 days unless a police official decided there was reason for further detention. No criminal charges had to be filed because the individual was not under arrest. It came under serious review in 1985 and again in 1993 after the Anglo-Irish Peace accord. The law was extensively criticized, not just for its sweeping violations of civil liberties, but many argued it was totally ineffective as well.

In 1988, the European Court of Human Rights found the amended law to be in violation of the European Convention on Human Rights. The act still allowed individuals, suspected of terrorism, to be held for seven days without any sort of court appearance. Opponents of the law alleged that the seven-day holding provision is simply a means of harassment and is used in efforts to intimidate and obtain information. According to these same opponents, thousands of people were affected by it each year, and only a tiny percent were ever charged with anything. The exclusion provisions of the law enable the U.K. Secretary of State to issue exclusion orders against British citizens and non-citizens from entering the United Kingdom. The authorities were seeking to limit IRA flexibility in moving around the United Kingdom. It is clear that such provisions would not likely survive judicial review in the United States because of long-standing freedom of movement expectations.

Another distinct difference between U.S. and British law was the fact that wiretapping was not illegal in Britain until 1985. Under pressure from the rest of the European community, the British passed the Interception of Communications Act of 1985 that limited the government's indiscriminate tapping of telephones and interfering with the mail. It is relevant to acknowledge the fact that the United Kingdom is one of the few democratic nations that does not have a written constitution or a Bill of Rights that guarantees the rights of individuals.

The United States and the United Kingdom have taken different paths to reach the same end. Both hope to control the proliferation of terrorism. The major difference in their approach is simply that the British do not have a supreme written constitution and an established Bill of Rights. Also, because of the absence of separation of powers between a judicial, legislative, and executive branch, the functions of drafting and implementing laws are somewhat merged. Consequently, there is no real judicial review of British anti-terrorism legislation. Hence, the scrutiny which has cropped up originated in the European Court of Justice.

The United States has also historically approached the problem from a criminal code perspective. When people died in terrorist acts, the crime of murder was committed. The terrorist acts were forced to fit within the already existing criminal code. Later under AEDPA, the approach was changed somewhat, singling out terrorists as people unworthy of certain civil liberties. The Bush Administration has expanded this concept even further. Some would argue that the new approach is inappropriate because it impinges on basic civil liberties and is therefore not worth any advantage it may give law enforcement in stopping terrorism.

POST 2005 LONDON BOMBINGS

The British Parliament passed the Terrorism Act after being introduced on 12 October 2005 by the Labour government. The act creates new offenses related to terrorism and amends existing ones. Arguably, the act was drafted in the aftermath of the 7 July 2005 London bombings (see Figure 12.2), and some of its provisions have proven to be highly controversial. According to the British government, the Terrorism Act contains a comprehensive package of measures designed to ensure that the police, intelligence agencies, and courts have all the tools they require to tackle terrorism and bring perpetrators to justice. The act received Royal Assent on 30 March 2006. This government formally asserts that the law was not a direct response to the July attacks on London in that they had been planning the changes for quite some time.

The legislative history of the act claims it specifically seeks to make it more difficult for extremists to abuse the freedoms enjoyed in democratic Britain, by acts which encourage others to commit terrorist acts. The act creates a number of new offenses. It is now a criminal offense to commit:

- Acts preparatory to terrorism: This aims to capture those planning serious acts of terrorism.
- Encouragement to terrorism: This makes it a criminal offense to directly or indirectly incite or encourage others to commit acts of terrorism. This will include the glorification of terrorism, where this may be understood as encouraging the emulation of terrorism.

FIGURE 12.2 The British reacted quickly after the July 2006 London bombings.

- Dissemination of terrorist publications: This will cover the sale, loan, or other dissemination of terrorist publications. This will include those publications that encourage terrorism, and those that provide assistance to terrorists.
- Terrorist training offenses: This makes sure that anyone who gives or receives training in terrorist techniques can be prosecuted. The Act also criminalizes attendance at a place of terrorist training.

The act also makes amendments to existing legislation, including the following (Internet: http://www.legislation.gov.uk/acts/acts2006/pdf/ukpga_ 20060011 en.pdf):

- Introducing warrants to enable the police to search any property owned or controlled by a terrorist suspect
- Extending terrorism stop and search powers to cover bays and estuaries
- Extending police powers to detain suspects after arrest for up to 28 days (though periods of more than two days must be approved by a judicial authority)
- Improved search powers at ports
- Increased flexibility of the proscription regime, including the power to proscribe groups that glorify terrorism

The new legislation has proved to be quite controversial. The law now unmistakably makes it illegal to glorify terrorism and distribute terrorist publications. In conjunction, the Terrorism Act 2006 allows groups or organizations to be banned for those offenses and encompasses anyone who gives or receives training. The act also designates nuclear sites as areas where trespass can become a terrorist offense. Even before the law was passed, members of Parliament worried it would curb free speech and rejected the plans five times before voting them through in March 2006. There was particular controversy over the creation of the new offense of the "glorification" of terror, i.e., people who "praise or celebrate" terrorism in a way that makes others think they should emulate such attacks. The then-Home Secretary, Charles Clarke, said people should not, for example, be allowed to glorify the 7 July attacks, or the bombers themselves, as it could encourage impressionable young men to think they should commit similar atrocities. Some argued this would mean the Irish Taoiseach could be prosecuted in the United Kingdom for celebrating the Easter Rising. They also point out such laws could have led to people being arrested in the 1980s for supporting Nelson Mandela's fight against apartheid in South Africa. The government has adamantly rejected such

claims. The law also bans two radical Muslim groups - Hizb ut-Tahrir (HT) and Al Muhajiroun, formerly run by radical cleric Omar Bakri Mohammed.

CANADA'S WAR WITH THE FLQ

Canada decided on yet another approach. The Canadian government concluded the best way to handle terrorism was both swift and limited in scale. Canada was forced to deal with a violent native terrorist group. The Front du Liberation du Quebec sought an independent Quebec and was willing to create anarchy and commit murder and kidnapping to accomplish it. The era culminated in the kidnapping of James Cross, a British diplomat, and Pierre Laporte, Minister of Labor in the Quebec provincial government.

Then Prime Minister, Pierre Elliot Trudeau, who had been so eloquently outspoken about terrorism at the Bonn Conference, invoked the Canadian War Measures Act in 1970. The law empowered him to call in the Army when the prime minister felt it necessary.*

At the time of the kidnappings, Prime Minister Trudeau agreed to negotiate with the terrorists. In return for the release of Cross, the terrorists were permitted to fly to Cuba. Laporte, however, had already been murdered. As the British had learned years before when British citizens were held captive, bargaining with terrorists is often antiproductive. The Canadians vowed to never negotiate again. After the kidnappings, Trudeau wanted to rid Canada of the FLQ by whatever means necessary.

He inundated Montreal with troops after the Royal Canadian Mounted Police concentrated on locating the terrorists. Suspending some of the normal Canadian protections against unreasonable search and seizures, the police used their new broad powers to arrest and search about 300 suspects (Dobson and Apyne, 1982). Trudeau's troop saturation of Montreal took nine weeks but successfully tracked down those responsible for Laporte's death. When it was over, the troops disappeared from the streets, the police went back to normal democratic search and seizure protocols, and the government sought to address some of the issues which contributed to terrorism in the first place. Canada, at the time, chose to focus on a specific group for a specific period of time. The United States, on the other hand, must deal with a multitude of international and domestic threats.

GERMANY

When the German antiterrorism laws were first enacted, many considered them to be fairly moderate considering the seemingly overwhelming problems the authorities were having with the Baader-Meinhof gang and later the Red Army Faction. Germany decided to enact what came to be known as the "contact ban" and the "propagation of violence laws." The contact ban law was intended to restrict the flow of communication between imprisoned terrorists and their comrades on the outside of Germany's prisons. The German authorities believed that the attorneys visiting the imprisoned members of terrorist organizations were passing information back and forth. Consequently, the German correctional authorities suspended the right of prisoners to confidentially discuss their cases. "To many experts on German law, this made it appear that a fundamental principle of due process was being sacrificed without any appreciable benefit" (Report on Domestic and International Terrorism 1981).

The provocation of violence law stirred up a bit of controversy. The law was used against student protestors as well as those engaged in terrorism. For example, it made it very easy for the police to infiltrate a student demonstration and arrest anyone they thought might be planning to riot or resist. It gave them almost blanket authority to arrest whom they saw fit, without any restraint, under the pretense that any situation was prone to violence.

Terrorism has been severely curtailed in Germany not only because of these laws, but also the "declassified" files of the former East German "Stasi" or secret police. When those files were

* *Note*: The Posse Comitatus Act prevents this alternative in the United States.

opened after the reunification of Germany, many terrorists formerly financed and protected by the East Germans lost the cloak of protection. The secret police were no longer able to circumvent the police efforts of the West Germans to track them down. As mentioned previously, on occasion some German antiterrorism units have allegedly gone too far.

ITALY

When Aldo Moro was kidnapped and killed, Interior Minister Virginio Rognoni, assumed the office. At the time, the Italian Red Brigades were at their peak. "Statistics issued by the Interior Ministry indicated that in 1978 there were 2498 terrorist attacks in Italy. Between 1968 and 1982, 403 people were killed in terrorist incidents, and another 1347 were injured" (Combs, 1999). In response, the Prime Minister unleashed a Carabinieri general named Carlo Alberto Della Chiesa. He created an antiterrorism unit, which was supported by legislation with teeth. The Italian laws, like some of their European counterparts, strengthened the maximum sentences for convicted terrorists, suspended search and seizure laws, and legislated terrorism as a crime.

The Italian authorities also made use of the fact that the population was tired of terrorism. Even the terrorists began to think that their efforts were gaining little. In 1982, a law that promised "repentant" terrorists lighter sentences if they confessed was passed. One of the most famous "Penniti" was Patriz Peci. He was a commander of a Red Brigade from Turin, Italy, who provided the police with some important intelligence. Italy balanced strict police enforcement measures with the ability to confess and be somewhat forgiven. The mix worked, and Italy is currently relatively free of terrorism.

PROFILING

As discussed, critics are inclined to denounce the practice of profiling. The basic concept behind a profiling system is to use trained security agents to detect patterns and behaviors that warrant closer scrutiny of certain passengers and their baggage. The system is not designed to detect weapons or explosives. It is designed to detect the person who is carrying such devices. A terrorist is absolutely convinced that the cause, whatever it is, has been betrayed and that he or she has been victimized. The cause can be based on ethnic, religious, economic, or ideological convictions. Because they feel exploited by forces usually more powerful than their group, they feel they can victimize others. Their psychological characteristics do not easily transform themselves into physical attributes. However, many terrorist groups are anti-Western. Consequently, many members of racial minorities repeatedly complain that they are unfairly singled out for questioning and searches.

Using similar techniques, the U.S. Customs Service also uses computer profiling and plainclothes and uniformed officers to prevent contraband from entering the country. That agency, in particular, has been heavily inundated with complaints, that its officers select a disproportionate number of blacks for strip searches. The agency has been sued often, but just a short while ago it has been sued by the American Civil Liberties Union (ACLU) representing a 33-year-old advertising agent returning from a vacation in Jamaica. As a result, Raymond Kelly, Customs Commissioner, has since instituted a sensitivity training regimen for officers that conduct these types of searches (Carr and O'Brein, 2001).

Similarly, the FAA had implemented a computerized profiling system to help identify potential hijackers. The details of the system have not been disclosed. It was, therefore, relatively impossible to precisely determine whether the profiles in use involved illegal conduct or not. However, David Harris, a law professor at the University of Toledo, had said that the system scans for: passengers' destinations, how they paid for the fare, and when they booked their reservations ("Profiling at Airports Warranted, say officials who screen people," 2001). The Computer Assisted Passenger Screening, or CAPS, system was, as previously discussed, supposed to rely solely on information that passengers already provide to air carriers for reasons unrelated to security. It was never

intended to depend on gathering any additional information from the traveler, nor was it connected to any law enforcement or intelligence database as sometimes alleged. The government had also repeatedly and emphatically denied that race, ethnicity, gender, or religion play a role in the process. They frequently stated that "it has to do with people's travel patterns and how well they're known in the system" (Interview with FAA Officer James Paget, 1998). It is difficult to ignore that a person's personal, ideological, and psychological characteristics do not play an important role in "profiling" them. After the Trans World Airlines 800 disaster in mid-1996, it was alleged by some that the FAA issued an internal confidential memo to select all individuals who were Iranian or carrying an Iranian passport to be singled out for special scrutiny (ACLU Against Airport Profiling, Internet: http://www.antidiscrimination.org/airlineprofileform.htm 2001). In response, the ACLU has created a form for people to fill out who believed they had been discriminated against. Literally hundreds of complaints were filed at the time.

In reality, abuse of such collected information would be almost inevitable. It puts every person in the situation that a "virtual" identity overshadows our corporeal selves. It also raises the issue that those individuals who are determined enough to construct a bomb and carry it onboard an aircraft, are almost certainly intelligent enough to avoid behavior likely to single themselves out for special scrutiny. Regardless, the Gore Commission was responsible for reviewing airline passenger safety and making recommendations on how to improve the system. The Commission wholeheartedly embraced profiling of terrorists specifically used in conjunction with some other controls.

In the Final Report to President Clinton, the Commission had stated, "the threat of terrorism is changing… it is no longer just an overseas threat from foreign terrorists. People and places in the United States have joined the list of targets, and Americans have joined the ranks of terrorists." The Commission recognized the need for sophisticated technology for detecting the presence of explosives in checked baggage. However, because those machines were expensive and not readily available for use in many airports, the report also recommended that the FAA implement programs for bag matching and passenger profiling by 31 December 1997 to enhance overall airport security. Additionally, the commission recommended that the FAA should develop the automated system for passenger profiling over the legal objections of the ACLU and many Arab-American groups.

In mid-1996 the FAA, using a grant with Northwest Airlines introduced the first automated passenger profiling system. In April 1997, the FAA and Northwest completed programming changes to a prototype CAPS system. It uses information directly acquired from the airline reservation system. If the system decides that someone is high risk, that person becomes subject to more stringent security review as per the discretion of the viewer. The system could also randomly select individuals for specific scrutiny. The system was not supposed to maintain a permanent database, and the airline was required to delete all information shortly after a flight lands. However, the profiles used in the system were not based on data about actual terrorists. The FAA developed the criteria based on "consultations with a large number of security and terrorism experts, who gave their assessments of the likely patterns of behavior of individuals intending to attack civil aviation" (Fainberg, 1998). The parameters themselves were therefore open to criticism.

In the mid-1970s, the FAA began using manual passenger screening to combat hijacking and to prevent explosives or incendiary devices from being placed aboard aircraft on international flights. This kind of screening relies on an employee of an air carrier to use personal judgment on whether a passenger meets the profile of a terrorist. Even though the factors used in conducting the manual screening are not suppose to be biased, there is always a distinct chance that the employee may be either consciously or unconsciously biased. There can be a thin line between profiling and discrimination.

Indeed, profiling has failed in the past. For example, the German S.S. profile for the potential bomber of the Hindenburg made Jewish and dissident passengers the preferred suspects. The alleged culprit turned out to be a German patriot. Prejudice, whether it is overt or less consciously implemented, does play some part in "profiling." Profiling should augment technological safeguards such as high technology bomb detectors, trace explosive detectors, and bomb-sniffing dogs and not

considered to be an independent tool. In and of themselves, profiling systems would be incapable of protecting airports from a terrorist attack.

The specific format of future airport programs remains uncertain. The system was designed to remove some human subjectivity by eliminating the choices of the personnel who identify persons targeted for heightened security. As stated previously, after each passenger's name is entered into the computer, the system makes an independent determination and flashes red or green. The passenger is totally unaware of the event. The process is focusing on checked baggage and other travel-related information. If the person's bags appear suspicious, they should be opened or scanned. The level or intensity of the search would depend on the level of suspicion. The choice to initially scrutinize the baggage is made by the computer, but the field officer must decide whether to halt or continue the search process through any additional steps. They view the images on the scanner and have complete discretion to choose the subsequent intensity of the search. Theoretically, they could just have a hunch or maybe they decide to seek other contraband not dangerous to flight. For it to work, the terrorist must be unaware of its criteria. Additionally, terrorists are likely to continue to seek innovative ways to place bombs on aircraft without having to carry them onboard themselves. The Department of Justice had repeatedly recommended that the FAA conduct periodic reviews of the CAPS system, require domestic airlines to obtain approval before adding to or enhancing the system, and require airlines to train employees responsible for the passenger screening system to respect individual civil liberties.

On 19 April 1999, the FAA proposed new regulations pertaining to security profiling (Federal Register: 19 April 1999). The FAA proposed that each certificate holder be required under Section 108.5 to adopt and implement an FAA-approved security program to screen checked baggage or conduct passenger bag matching for scheduled passenger operations.*

The proposal mandated that the screening of checked baggage on domestic flights may be accomplished by screening the checked baggage of every passenger with explosive detection equipment (EDS), by 100 percent positive bag matching (PPBM), or by utilizing the government-approved CAPS system. Unfortunately, the improvements were not implemented in a timely manner. The FAA argued that CAPS was based on the same concept as the manual screening system, which was designed to exclude from extra security measures, the vast majority of passengers. It supported the system and supported its decision, despite allegations it is discriminatory or that a potential terrorist could circumvent the system. To further justify the merits of the system, in addition to selecting persons pursuant to the profiling standards, it randomly selected a limited number of passengers for heightened security measures. The FAA determined that this random selection in which each passenger has a chance of being a selectee had a valid deterrent effect. However, alternatively it is arguable that the chance of the system selecting a terrorist by means of random selection was about as likely as winning the powerball lottery. CAPS was eventually amended into CAPPS and CAPPS II.

The federal government continues to battle privacy advocates, airlines, and members of Congress critical of its plans for an improved screening system that uses fliers' personal information to determine whether they pose terrorist risks. To every charge that the system would be too intrusive, the TSA issued assurances that it was building in safeguards. In 2004, the General Accounting Office (GAO) reported that the CAPPS II system could make passengers' financial and other personal information vulnerable to government misuse and computer hackers. The GAO's conclusions show where more government attention is needed to ensure that any new screening system will do a better job of flagging suspected terrorists without compromising privacy rights guaranteed under federal law.

The screening system does identify many innocent passengers as security risks and diverts government attention from those posing greater threats. The GAO concluded:

- The TSA has not yet determined the accuracy of commercial and government databases it plans to use to screen passengers. Inaccurate data could flag innocent fliers as risks.

* *Note*: The regulations are to apply to aircraft configured to seat more than 60 passengers.

- The TSA has exempted its system from some of the federal privacy strictures that ban government use of personal information without an individual's knowledge. That raises concerns about what data might be collected and how it could be used.
- The TSA has not developed a process for fliers to correct errors that might result in their being stopped from boarding planes.

A TSA official has told Congress that the agency agrees with much of the GAO report. The TSA has assured it critics that an independent review board that includes consumer, airline, and privacy representatives will be named to ensure privacy is protected (GAO-04-385).

INTERNATIONAL VIEWS OF PROFILING

Much of the hijacking had been taking place in the Middle East, and the Israeli Airline, El Al, was said to have the best security in the world. Security officials for El Al have made profiling of passengers, a necessity since 1968 (*Security Management*, 1992). Dan Issacharoff, ex head of El Al said the El Al security system emphasizes the identification of people who would be a threat, rather than the detection of objects that could be used to hijack or destroy the airplane. Their system recognizes five types of passengers. The five types of people are labeled: naïve passenger, partly naïve passenger, framed terrorist, terrorist, and suicide terrorist. They have developed procedures to specifically deal with each of those types of individuals. The procedures in other countries vary, depending on the perceived threat in the geographic region where the airport is located.

SAFEE

The Security of Aircraft in the Future European Environment (SAFEE) represents the first coordinated international effort to create an airplane system capable of thwarting hijackings and terrorist attacks by analysis of the hijacker. Eleven European countries and Israel are involved in pursuing the technology. Much of it is in advanced stages of development, although systems for accurately analyzing facial expressions remain problematic. The director of the $50 million program, Daniel Gaultier, describes the system as being developed largely in secret by the European Commission and 31 aircraft, avionics, computer and security companies, and university research centers The concept is considered in terms of "a last defense against attack" in a post–11 September world. In the interim, human rights officials have expressed concerns about passenger privacy, pilot groups are fearful of computers usurping command of the aircraft, and airline manufacturers ponder about the eventual price tag (Internet: http://www.washingtonpost.com/wp–dyn/content/ article/2007/ 01/15/AR2007011501048.html).

BOMB SNIFFING DOGS

Dogs have a great sense of smell. Their noses are about 100,000 to a million times more sensitive than a human's nose, and a well-trained dog can detect up to 20 different kinds of explosives. Furthermore, the legality of their use is well established and does not seem to be significantly limited by the Fourth Amendment. In the case of United States versus Place, 462 U.S. 696 (1983), the Supreme Court held that the warrantless use of a canine did not violate the Fourth Amendment because the dog disclosed only the presence or absence of narcotics and nothing more. The opinion reasoned that the dog was less intrusive than a typical search, and the limited disclosure exposed the property owner to a minimum amount of inconvenience.

Canines are also less expensive than other means of explosive detection. Dogs cost about $6000 to train, and a piece of equipment can cost more than a million dollars. According to the Web site *Tech.mit.edu,* "…the Bureau of Alcohol, Tobacco ,and Firearms is developing a plan to train and provide bomb-sniffing dogs for up to 50 of the nation's largest airports in a proposed new step toward tightening security for air travelers" (Techmit.edu, 2002). The White House Commission

on Aviation Safety and Security had recommended in 1996 that the number of bomb-sniffing dogs and handlers needed to be increased. Consequently, Congress provided $8.9 million for reimbursements to airports that used the dogs. In response, by the end of 1998, there were about 150 teams working at 40 airports. Dogs have historically only been used at airports if the threat of a bomb was eminent.

Bomb-sniffing dogs are not without their problems, which include short attention spans, false alarms, sickness, and distraction of female dogs in heat. Therefore, the FAA and the Bureau of Alcohol, Tobacco, and Firearms (ATF) teamed up to conduct a joint research pilot project to determine the best method to train these dogs and their handlers. Testing was done at Dulles International Airport and Ronald Reagan Airport in Washington, D.C. To pass the certification test used by the ATF, the dogs have to receive a score of 100 percent accuracy. They must convince the handlers that they can successfully detect at least 20 known explosive compounds, which enables them to identify over 19,000 varied explosive combinations. Their training system is based on a food reward program. The method rewards the dog for detecting a compound. To reinforce the conditioning, they are never fed without some exposure to an explosive's odor. This keeps the dogs highly motivated to sniff out the explosive because food is always available if they do.

The ATF and the U.S. Department of State have provided dogs and training to numerous airport authorities around the world. The program was successfully used by the Australians before the 2000 Olympic Games and has been in operation at high-threat airports for a number of years. Dogs are compact, mobile, and capable of working in a variety of environments including confined spaces. More importantly, in the airport environment they can reduce the manpower needed to screen huge quantities of cargo.

CONCLUSION

Most countries have taken a "legal" or "criminal" approach to prosecuting terrorists. They assess the results of an attack and pursue a public legal remedy based on the specific misconduct already deemed criminal in a standard penal code context. Murder, kidnapping, and assault by terrorists are treated exactly the same as murder, kidnapping, and assault by any other type of criminal. Other sovereign nations have chosen to create the offense of terrorism. They have legislated laws, which apply directly to the antiterrorism effort. Some have been in place for quite a long time as in Northern Ireland and the Middle East. Others like those enacted in Canada have been short-lived. In Great Britain they have also been toughened and enhanced. The United States is adjusting its efforts in the fight against terrorism by moving away from the use of state and federal penal codes and have moved to an allout effort to pass the necessary legislation to more aggressively combat terrorism by the use of specific contextual and procedural laws. As in all other criminal cases, the U.S. legislation is subject to review by the judiciary and is bound by the fundamental civil rights dictated in the Constitution. Other countries are not held by those same constraints.

Many nations have tried many remedies to control terrorist activity. New technologies become available with increasing speed to assist authorities in providing security at airports and onboard aircraft. However, all these available technologies used by security personnel or antihijacking and rescue squads must be viewed in perspective and in the proper focus. Technology is not the bottom line. The human effort behind the security demands scrutiny as well. The current political sentiment has justified massive budget expenditures to militaries, police forces, and other agencies. Such actions also have challenged constitutional personal rights to travel, to privacy, and equal protection under the laws. It is clearly within every nation's best interests to harness the concern for airline safety. The key is to do so within acceptable democratic norms.

Each airline determines what procedures are appropriate for its own operation. In the recent past, however, the airlines have all come to realize that the threat is very real. Additionally, that very real threat has made it clear that security is cheap in comparison to the costs of a major security breech. The airlines have been forced to think the unthinkable, namely that the cockpit is not secure, the

terminal is not secure, and the aircraft is not secure unless proper procedures and equipment are used to make them secure.

In accordance with the concept of awareness of the threat, the airlines need to take one step further and recognize that quick stopgap measures will prove to be insufficient. Furthermore, more of the unthinkable thoughts need to be addressed. Those unthinkable thoughts; including the threat of nuclear, biological, or chemical attack, will continue to plague the airlines and airports. New procedures and policies must be developed to meet these threats. The ebola virus released in one aircraft and transported thousands of miles across an ocean can potentially kill millions of people.

REFERENCES

ACLU Against Airport Profiling, http: //www.antidiscrimination.org/airlineprofileform.htm., Pg. 1, 21 August 2001.

Airline Security Crackdown is Stalled on the Runway: Despite Federal Rhetoric Little Has Been Accomplished, *Los Angeles Times*, 19 August 1996, B4.

Athens Sparta Airport Not Ready to be Opened, *IATA Press Release*, 9 February 2001, Internet: http://www.iata. org/pr/pr01febb.html., 10 July 2001.

Atlas, Terry, "GOP Balks over Wiretaps, Tagging Explosives; US Allies OK Counterterrorism Initiatives," *Chicago Tribune*, 31 July 1996, pg. 3.

Carr, Martha and O'Brien, Keith, "Profiling at Airports Warranted, Say Officers Who Screen People," *Star Tribune*, 4 February 2001, pg. G-2.

Combs, Cindy*, Terrorism in the 21st Century,* 2nd Edition, Prentice-Hall, NJ, 1999, pg. 185.

Dobson, Christopher, and Apyne, Ronald, *Counterattack, The West's Battle Against Terrorists*, New York, Facts on File, 1982, pg. 113.

Fainberg, Anthony, "Aviation Security in the United States: Current and Future Trends," 25 *Transportation Law Journal*, 1998, pg. 200.

Federal Register: 19 April 1999, Volume 64, Number 74, Pg. 19219-19240; Federal Register On-line via GPO access, wais.access.gpo.gov.

Finn, John E., "Public Support for Emergency Legislation in Northern Ireland: A Preliminary Analysis," *Terrorism,* 1987 pp. 113–124.

http://www.faa.gov/avr/iasa/iasadef5.htm pg. 1.

http://www.faa.gov/safety/ programs_initiative /oversight/iasa/media /iasaws.xls.

http://www.legislation.gov.uk/acts/acts2006/pdf/ukpga_ 20060011 en.pdf.

Interview with FAA Officer James Paget, Gore Commission participant, 6 Nov 1998, Michael Higgins, Looking the Part, *A.B.A. Journal*, pg. 52.

http://www.washingtonpost.com/wp–dyn/content/ article/2007/ 01/15/AR2007011501048.html.

Techmit.edu, 2 October 2002.

Janis, Mark, *Introduction to International Law*, 2ed., 1993, pg. 348.

Janis, Mark, *Introduction to International Law*, 2ed., 1993, pg. 349.

Profiling at Airports Warranted, say officials who screen people, *Star Tribune*, Sunday February 4, 2001, pg. G2.

Report on Domestic and International Terrorism, Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, First Session April 1981, Washington, D.C., Government Printing Office, pp. 6–23.

Restatement of Foreign Relations Law of the United States, 1987, pg.475.

Security Management, May 1992, Vol. 36, No.5, pg. 26.

13 Technological Improvements
Some Intrusive, Some Not

NEWS

27 April 2001: Perkin-Elmer Instruments announces a $6.2 billion contract award for the development of ARGUS, a certified automated explosive detection system.

9 May 2002: Airbus, the European jet manufacturer, considers a set of tiny, concealed cameras above the passenger seats. The pilot would be able to be a spy in the sky to spot a potential hijacker.

17 June 2002: The U.S. Department of Transportation makes public a new rule that foreign airlines must install new flight deck doors on aircraft serving the United States by 9 April 2003. Temporary locking devices are authorized until that date.

19 April 2005: "We agree with the IG's conclusion that significant improvements in performance will only be possible with the introduction of new technology. That said, we will continue to seek incremental gains in screener performance through training, testing, and management practices" (Transportation Security Administration [TSA] response to the "Follow-Up Audit of Passenger and Baggage Screening Procedures at Domestic Airports" Inspector General Repor**t)**.

29 July 2005: The TSA announces that it has deployed an explosives detection trace portal at the passenger security checkpoint in the A/B concourse of Palm Beach (FL) International Airport.

August 2006: The Bush Administration proposes $4 billion for Homeland Security research and development, mainly directed against weapons of mass destruction, including nuclear and radiological devices.

INTRODUCTION

With the need for safety increasing in the airline industry by leaps and bounds, new technology is constantly and rapidly being developed. With technological change also comes concern from the public about health and intrusion-related factors. When purchasing new high technology equipment, the security manager must be aware of the availability of more and more sophisticated equipment as well as the public's reaction to it. The most sophisticated and effective technology in the world is unacceptable if the traveler will avoid travel to avoid the equipment.

Improved x-ray imaging, microwave holography, and acoustic detection are just a few of the many technologies recently put into service for detecting weapons and other contraband. All these systems can be utilized in many formats such as wand-type metal detectors, x-ray imagers, and microwave radar imagers.

Other rapidly expanding advancements will certainly tend to improve security at airports. The costs will be correspondingly high. Under former law, each airline passenger paid a three-dollar passenger facility charge (PFC) for the use of the airport facilities and the costs associated with

airport maintenance (14 CFR 158; 1998). Many believe that the charge should have been increased to five dollars to provide for increased funds for security measures (FAA Reauthorization Bill 106th Congress 201, 1999). In light of 11 September and the new Airport Security Act passed in November 2001, the fees are even higher. The Bush Administration plan proposed an increase in the fee to $5.50 for a one-way ticket and a fee of $8 for trips requiring several boardings. The White House expected the fee increase to generate $1.5 billion in new revenue.

However, nothing will replace a human being's overall situational awareness. Regardless of massive and critical improvements in technology to be used at airports, if a human operator cannot properly utilize the new technology it is useless. Additionally, as stated above, with technological change also comes concerns from the public.

In 1996, The National Research Council published a study on the future implementation of new passenger screening technologies. One of the primary tasks of the research was to assess aspects of each method that might generate concerns over health risks and to consider ways to maintain effectiveness while increasing public acceptance. In the 1970s, the first introduction of equipment that x-rayed baggage was met with alarm from some segments of society. The initial alarm was due, in part, to a lack of information. However, it is likely that the introduction into air terminals of more powerful and intrusive systems of both baggage and personal screening may evoke a similar prompt response. The key to avoiding a negative public reaction will depend on efforts to educate the public prior to their use.

As repeated many times in this book, the responsibility for aviation security was shared between the Federal Aviation Authority (FAA), the airlines, and the airport operators and now by the TSA and the new Department of Homeland Security. The government sets guidelines, establishes procedures, and relies on the intelligence community for information on threats to aviation. In addition, the government sponsors the development of new security technology, such as explosive detection equipment, and it also oversees the implementation of such equipment. Generally, airlines were responsible for screening checked baggage, carry-on bags, passengers, and cargo, whereas airports were responsible for the security of the airport facilities. Even though the FAA set the standards and approved the equipment, it generally remained the responsibility of the airport and air carriers to obtain and finance new equipment. Everything has changed.

GORE COMMISSION

A catalyst for taking important steps in aviation security was the July 1996 crash of Trans World Aairlines Flight 800. As stated previously, the crash prompted the August 1996 creation of the White House Commission on Aviation Safety and Security (the Gore Commission). A further result of the Gore Commission was Congressional approval of 198 million U.S. dollars for aviation security initiatives. As part of the $198 million, $144.2 million of it was for the deployment of advanced security technologies, $18 million to hire 300 additional FAA security personnel, $8.9 million for additional canine teams (see Figure 13.1), $5.5 million for airport vulnerability assessments, and $21 million for aviation security research and operational testing.

One piece of new equipment that was a direct development of the Gore Commission, was the CTX-5000SP™. The machine was developed to improve the capability of explosive trace detection equipment. The equipment is supposed to increase security by safely collecting, analyzing and identifying trace amounts of many different types of explosives. These analyzers, previously produced by Perkin-Elmer Instruments, and Invision, now have high detection probabilities with low false-alarm rates and allowed for rapid baggage screening; however, initially they did not. Employing transmission x-ray data, the system acquires an overall map of objects in luggage and uses strategic computerized axial tomography to identify objects that may be explosives. An explosive detection system (EDS) is automated, using red and green lights to indicate the presence or absence of a threat. When a potential threat is detected, the operator is alerted and can use the instrument's threat resolution features to validate the threat.

FIGURE 13.1 A police dog sniffs the baggage of a traveler. Trained dogs continue to represent a vital tool within the overall security toolbox at airports around the world. (Source: Transportation Security Administration. www.tsa.gov)

The complexity of the installation and the number of entities involved slowed deployment of the initially purchased CTX-5000SP's™. At some airports the CTX-5000 SP's™ were installed in locations not conducive to efficient and effective security operations. Another contributing factor to delays and nonuse had been the initial inexperience of the integration contractors; airline indecision on site surveys, and delays experienced due to airport permits, approvals, and construction. In contrast, because of smaller size and portability, implementation of trace detection devices for screening carry-on baggage has been smoother.

The industry has found those integrating new explosives detection systems, with day-to-day operations was more complex than first imagined. Making this task more difficult is the fact that each airport is unique, and airline-operating philosophies differed as well. The success of industry and government efforts is dependent on the development of an effective security plan that includes the cooperation and commitment of all facets of the aviation security community. The events of 11 September have speeded up the process.

The White House had urged the FAA to purchase and deploy the latest technology for detecting explosives. In 1997, the FAA purchased 54 CTX5000SP™ to scan checked baggage. Initially, they were installed in Atlanta, San Francisco, Chicago, New York, and Manila. As it turns out, the CTX 5000SP's™ performance in airports differed from its performance during certification testing. Expert analysis indicated that FAA-certified CTX 5000 SP's™ deployed at airports were experiencing high false alarm rates and slow baggage processing speeds. From the operational data reviewed, the false alarm rates were up to 169 percent higher than the standard established during certification testing. Test bags used for certifying false alarm rates in the laboratory environment were not fully representative of passenger baggage. Many of the items, such as food that cause false alarms, were not included in the bags used for certification tests. Also, the certification testing procedure for determining the machine's baggage processing rate does not take into account "alarm resolution." Resolution is the time it takes for an operator to determine if an alarm is real. Without improvements in performance, the early EDSs were unable to facilitate the goal to ultimately screen 100 percent of checked baggage. This goal would take several years to complete.

Furthermore, the analysis indicates air carriers had initially underutilized the EDS. For example, daily usage rates on 10 of 11 units installed and operating during the review were significantly less than the certified processing speed of about 225 bags per hour. At five locations, 10 CTX 5000 SP's™ were screening fewer than 200 bags per day. The machine has a tremendous throughput capability, but some airlines formally ran as few as four bags an hour through the 1-million-dollar

machines, according to the *Chicago Tribune* (The Associated Press, 1999). At the time the goal was to run 2 to 20 percent of all checked baggage through the machines, depending on the threat at a particular airport. It has been reported that nationally the machines actually screened less than one percent. This was in part due to complaints by the airlines that more extensive use would disrupt flight schedules. The scan is relatively quick; however, if the machine sets off alarms, the process takes longer. The machines also sometimes give off a false alarm, frustrating the scanner, the airlines, and ultimately the passengers.

Human factor issues associated with the new equipment deployment can also not be underestimated. The government agrees that screeners are absolutely critical in improving security. The CTX 5000SP™ was a very complex piece of equipment that has taken countless man-hours to design and implement into the everyday workings of an ever-increasing busy airport environment. Additionally, with every new piece of equipment such as the 9000 series comes the ever-increasing expense related to training, as well as an enormous amount of money for future development and upkeep. Without such maintenance and training expenses, operators will be unable to use the equipment effectively. According to the manufacturer, GE Invision, the CTX 9000 DSi system is now the world's fastest operational TSA-certified automated EDS. The company emphasizes the 1-meter-wide conveyor that coordinates with airport baggage handling systems and requires minimal space for built-in installation.

HOMELAND SECURITY: SCIENCE AND TECHNOLOGY DIRECTORATE

Critics claim that the department has been plagued with poor leadership, weak financial management, and inadequate technology since it was established in 2003. One thing is clearly substantiated. There have been significant turnovers, reorganizations, and raids on the directorate's budget. Insiders point to the fact that the Bush Administration's overriding focus has been on nuclear and biological threats, which has subsequently delayed research on weapons aimed at aviation. The distinction was well publicized after a plot to blow up U.S.-bound airliners from London was made public on 10 August 2006.

ANTIMISSILE DEFENSE SYSTEMS

In January 2007, a Federal Express (FedEx) flight took off from Los Angeles International Airport equipped with the Guardian antimissile system. The FedEx flight marked the start of operational testing and evaluation of the laser system designed to defend against shoulder-fired antiaircraft missiles during takeoffs and landings. Adapted from military technology, Guardian is designed to detect a missile launch and then direct a laser to the seeker system on the head of the missile and disrupt its guidance signals. The laser is not visible. During the current test phase, which was scheduled to conclude in March 2008, nine MD–10s equipped with the Guardian system will be in commercial service, all the aircraft currently being tested on cargo freight aircraft. The ultimate goal is to defend passenger airliners. The testing is part of the Counter–Man Portable Air Defense Systems program of the Department of Homeland Security, or DHS (Internet: http://www.signonsandiego.com/news/business/20070116–1146–c–airlineranti–missile.html).

In addition, the DHS tested drones flying at 65,000 feet above the nation's most active airports in efforts to protect aircraft from being shot down by shoulder-fired missiles. The project named "Project Chloe" was established to test drones over Patuxent River Naval Air Station outside Washington, D.C. The drones were to be fitted with missile warning systems and antimissile lasers that could send planebound missiles veering off course. The drone was to pick up the ultraviolet (UV) plume from a missile's rocket booster and trigger an antimissile laser, which could be shot from the drone or from a ground site.

Officials have directly addressed the possibility that terrorists could use shoulder-fired missiles to bring down an airliner. Two U.S. senators, Barbara Boxer (D-CA) and Charles Schumer (D-NY),

originally wanted to equip all 6800 commercial airplanes in the U.S. fleet with antimissile equipment. The cost would have exceeded 10 billion U.S. dollars. The U.S. government has requested high technology companies to explore the development of such antimissile defense systems. However, several experts have reasoned that equipping passenger planes with defenses against missile attacks would be very complex and still not totally effective. Specifically, one opponent has said, "The best thing to do is to create an environment where an attack does not happen or consequences for that would be very severe, and not to complicate the airplanes" (Web Investor Conference, 2003). He went on to comment that adding defensive equipment to evade missile attacks would require dramatic changes to current airline systems, and those defenses probably would not work against modern weapons. Military aircraft, which are more maneuverable than commercial aircraft, use flares, chaff, and sometimes electronic means to ward off attacks. Commercial aircraft do not possess such maneuverability, and fitting commercial airplanes would be expensive to say the least.

In August 2003, the United States sent aviation security experts to Iraq, Europe, and Asia amid renewed fears that terrorists would use shoulder-fired missiles or rocket-propelled grenade launchers (RPGs) to shoot down passenger jets. The list of airports investigated included Basra and Baghdad in Iraq and Manila in the Philippines, among others in Europe and Asia. In Manila, the Philippine National Police Aviation Security Group confirmed that the DHS sent a member of the FAA and two others from the TSA to check on security gaps at the international airport. The TSA has commented publicly that they are visiting countries that want to work with them. The inspections began in early summer 2003, but announcement of the visits did not take place until August out of concern that the information might prompt terrorists to attack before more stringent security was in place.

For example, at Ninoy Aquino Airport in Manila, on the advice of U.S. experts, authorities leveled an area full of trees near the airport's 100 hectare compound periphery and also planned on moving squatter colonies formerly near one of the runways (Runway 06-24) to a more safe distance. Experts are concerned about the possibility of terrorists using either the U.S.-made Stinger or the Russian-made SA-7. It is well known that Afghan groups close to al'Qaeda possessed such weapons during the Afghan War in the 1980s. Aviation officials know very well that the weapons can also be purchased on the black market for as little at 5000 U.S. dollars a piece. Technical specifications of the weapons indicate they can hit a jet from 5 kilometers away and can reach altitudes of between 10,000 and 18,000 feet, depending on the series. Most only weigh approximately 30 pounds.

More recently, U.S. airports have been conducting exercises aimed at improving defenses against a possible surface-to-air missile attack. During March and April 2004, airports were asked to participate in tabletop exercises to openly discuss the issues involved. The scenarios ranged from handling a suspicious person observing takeoff and landings to an actual shootdown of an aircraft. A TSA spokeswoman has stated that the exercises are intended to heighten readiness. These exercises are part of the overall threat mitigation program to assess U.S. airport vulnerability to a missile attack.

Attention became focused on shoulder-based missiles when two SA-7s narrowly missed an Israeli charter flight taking off from Mombasa, Kenya in November 2002, and after another missile narrowly missed a U.S. military jet taking off from Prince Sultan Air Base in Saudi Arabia in May 2003. In July 2003, in Iraq, a U.S. C-130 military transport plane also came under fire from a surface-to-air missile as it was landing in Baghdad. More recently, a missile hit a DHL cargo plane taking off from the Baghdad airport and was forced to return to the airport, wing ablaze, in late November 2003. The plane, an Airbus A-300 with a crew of three and operated by the European-based delivery service DHL, was apparently hit with an SA-7. Attacks against aircraft have been often repeated. Insurgents have shot down five U.S. helicopters using shoulder-fired weapons and RPGs, killing 40 U.S. servicemen.

A U.S. Congressional Report, issued in 2003, indicated that the worldwide inventory of portable surface-to-air missiles likely exceeds half a million weapons and could be as high as 700,000 weapons. Certainly, hundreds if not thousands of Soviet-style missiles are available in the international arms market, which are capable of hitting a low-flying aircraft or any other transportation component. The Israelis had budgeted 1.3 million U.S. dollars to test an antimissile system for commercial

aircraft and stated publicly they hoped to have the system operational within a short period. They have followed through, and Israel's national airline was the first to take measures to safeguard passengers against missile attacks from the ground. In June 2004, El Al began equipping all its planes with an antimissile system called "Flight Guard." When a plane comes under attack, the system responds by firing flares designed to confuse a heat-seeking missile and divert it away from the original target. The Israelis have incurred some difficulties in implementing the program.

The system was implemented because of the previously mentioned incident 18 months before in Mombasa, Kenya, when an Israeli charter jet came under attack just after takeoff. In November 2002, two shoulder-fired, heat-seeking missiles narrowly missed the Boeing 757, which was carrying over 250 passengers. Israeli officials believe they present the next big risk to the airline industry. "So the Israeli government took the decision not to wait for another case to happen and to equip all its aircraft with countermeasures" (Arik Ben-Ari, 2004).

The planes are equipped with a Doppler radar system made up of four antennas at the front, two on the sides, and four at the back of the plane capable of giving 360 degrees of radar coverage around the aircraft. Within seconds of a missile being detected, an onboard computer releases flares, firing at different angles to act as a diversion. The system is completely automated, meaning there is no involvement from the pilot or copilot. The reason for this is a missile attack could happen so fast that the incident could be over before the pilots could have time to react. "The time that passes is one or two seconds. With this time frame the pilot of such a big aircraft can do nothing. He cannot maneuver...he cannot even react to the alert, so everything has to be automatic," says one test pilot. The pilot will only be alerted that the plane was under attack once the threat is over. Already "Flight Guard" is being used by Israeli helicopters and fighter jets in combat. This technology was originally developed for the Israeli Air Force several decades ago.

The manufacturers are waiting on FAA approval before it is available for commercial airline use in the United States. But with a $1 million price tag per plane and thousands of aircraft, for many airlines the cost of the system could be a major obstacle, especially those already in financial distress. "Today, I haven't seen an assessment of general threat to the whole of civil aviation to say that all aircraft should be equipped," Dennis Phipps, the Director of Asgard Security Management Services and the former head of security for British Airways, told CNN in 2004. "You have to assess the threat to decide what countermeasures are necessary. The important thing is the shoulder-fired missile has definite limitations. For this type of missile, the aircraft is only vulnerable when the aircraft is flying under 15,000 feet and when it is coming in on a designated flight path," Phipps said. "The threat we are looking at is can a terrorist get there and get within an area near an airport that is being used? And that is something that is being assessed." British Airways has also confirmed they are considering fitting aircraft with antimissile systems and have begun negotiations with Boeing and Airbus about adapting existing technology to commercial aircraft.

After publication of a Congressional Report, Chairman of the House of Representatives Aviation Subcommittee had called for outfitting the nearly 7000 U.S. commercial aircraft with antimissile technology. Such an effort, as stated, would be incredibly expensive and is estimated to possibly cost 1 million U.S. dollars per aircraft. The feasibility of such an effort is clearly questionable. As stated, antimissile equipment could include decoy flares, infrared jamming devices, and high-powered lasers, but effectiveness is questionable in the commercial venue. Regardless, the U.S. House Transportation Aviation Subcommittee gave unanimous approval to a bill that would have required airport vulnerability assessments and fast-track certification of missile defense systems to protect air carrier operations.

As an additional indication that the threat is being taken seriously, the DHS created a special office to deal directly with the missile threat. They also requested that Congress provide 2 million U.S. dollars to establish the first year's budget. The department had additionally notified eight government contractors that they were finalists for potentially huge contracts to develop a prototype for an electronic antimissile system for commercial jets (Shenon, 2003). By the end of September 2003, the Senate had approved $60 million to develop the necessary technology. The latest proposal has

called for spending $100 million over two years. The new strategy is to focus on the use of existing technology such as infrared jamming that redirects heat-seeking rockets away from the engines. Some U.S. Air Force and Navy aircraft are at present so equipped.

Congress has since somewhat reconsidered the U.S. position. They now recognize some of the serious problems associated with installing such equipment. Rep. John Mica (R-FL) once championed immediate action. He later authored legislation, submitted in April 2004, asking for a quick federal review of the technology and asking the Administration to coordinate with foreign governments to limit the number of missiles available on the black market. The Congressman had participated in a visit to a California company working on antimissile technology for the military. He learned that the laser technology is energy intensive and also that installation and maintenance costs are quite high. Any additional equipment eventually used on commercial aircraft also will need FAA approval, which could constitute another lengthy process.

The SA-7, or a variant of the weapon, is currently being produced under license in countries like China, Egypt, North Korea and the former Yugoslavia. They can be bought for approximately $5000 and according to *Jane's Defense Weekly* several thousands are in circulation all over the world. Hezbollah is believed to have acquired some and on 8 May 2001, Israeli authorities confiscated four SA-7's being smuggled on the Lebanese flagship Santorini. Hezbollah is also thought to have acquired Stingers from the Afghani Mujahideen and well as Chinese made QW-1s.

It should be noted that some attacks are falsely attributed to shoulder-launched missiles but instead have been initiated by use of an RPG. RPGs have a range of approximately 984 feet or 300 meters and can do significant damage to low-flying aircraft. A perfect example is the destruction of a U.S. Blackhawk helicopter in Somalia in October 1993. Antimissile technology would be less effective against these weapons. Incidents involving these weapons are often reported as ManPad attacks. However, the proliferation of shoulder-fired missiles presents the more serious threat.

MICROWAVE HOLOGRAPHIC IMAGING

Microwave holographic imaging is a portal-type device that scans individuals using microwave energy. Some of its drawbacks will cause airlines to resist purchasing them. They include an inability to search for weapons or contraband in body cavities, the person being scanned must stop and be scanned, and the portal is for some people claustrophobic.

On the other hand, the system provides a means to see through optically opaque mediums. In an ordinary system the microwave field is scattered from a stationary object. The object is illuminated from a stationary transmitter, which is mapped over a prescribed hologram recording aperture by means of a detector that is scanned over the aperture. The simplest machines need a fixed reference beam to interfere with the object wave that creates a wave-field pattern that can be measured by an internal sensitive detector. More sophisticated pieces of equipment use phase-locked receivers with local oscillators, which act as synthetic internal reference beams. Sometimes, in detectors using low-intensity applications, the detected wave field is considerably disturbed, giving false or disturbed readings. This can be overcome by using modulated scattering techniques including mechanically, electrically, and optically modulated signals. Equipment used today for discovering metallic objects generally employs a scatterer in the form of a selected high-speed photodiode that is modulated optically via a plastic fiber, collecting and performing image reconstruction digitally.

Summing up some complicated scientific language, this type of technique for obtaining two-dimensional microwave holographic images of objects uses a light-modulated scatterer that can produce highly distinct images of metal objects. The technology would exhibit an extremely dissimilar image, making it very simple for the scanner to recognize a potentially dangerous object. Microwave holographic imaging has the potential to provide crystal clear images that a screener could hardly miss. However, currently, having each passenger step into a closed portal is not conducive to airport use.

TRIGGERED SPARK GAP

In a case of dual-use technology, the use is productive and entirely beneficial and useful; a piece of technology can also be used in a sinister manner. A "triggered spark gap" serves as the ignition switch of sorts in a machine that uses electrical shock waves to break up kidney stones. However, a terrorist can use the device to detonate a nuclear bomb. They are defined as devices that can switch megawatts of power in a few microseconds, with jitters of less than a nanosecond. These devices make use of the very low impedance of an arc once the arc is established. Two electrodes are separated by sufficient distance that the gap does not spontaneously break down. The breakdown is initiated by a variety of means: UV irradiation from another spark or a laser, an overvoltage pulse, or reducing the gas pressure in the gap (http://home.earthlink.net/~jimlux/hv/hvtrigsg.htm). They are small and look a lot like an industrial sized spool. Examples such as this are why authorities need to constantly review import-export laws. The Federal Bureau of Investigation (FBI) refers to this concept as counterproliferation. It involves an understanding of intricate export laws, international diplomatic sensitivities, and a variety of sophisticated technologies. The notion also encompasses several different yet related threats including terrorism, weapons of mass destruction, international espionage, and the theft of intellectual property and its trafficking on blackmarket trade networks (Internet: http://www.fbi.gov/page2/dec07/counterproliferation121307.html).

BOSS™

According to the manufacturer, Omni Security, the Body Orifice Security Scanner, or BOSS™, is a safe, nonintrusive method of detecting objects concealed in body cavities. Currently, it is commonly used in correctional facilities to scan inmates for weapons and contraband, but clearly has potential applications elsewhere. The equipment looks much like a chair and is capable of detecting objects hidden in oral, nasal, vaginal, and anal cavities. Both federal and state correctional facilities personnel have extensively tested it.

Because the equipment is highly sensitive, it is capable of detecting such objects as razor blades, knives, and other potentially dangerous but small weapons. It is also able to detect metal foils and detonator caps. This particular piece of equipment minimizes the need for intrusive manual searches. It also increases the safety of not only airport security personnel, but ultimately passengers by eliminating the liability and safety issues associated with manual searches. Additionally, it saves time and the expenses of using portable x-ray machines to achieve the same result.

BOSS™ can be considered a powerful deterrent. It can be used not only to scan people, but is also useful in viewing small objects inside pens and lipstick holders. BOSS™ is well tested. In an article by a news staff writer, "Prisoners' Weapons No Match for BOSS Chair," the writer, Jim Krane indicated that in 1990, 1500 stabbings occurred in New York City jails, but after using the chair, they dropped to 229. BOSS™ is also mobile and is equipped with wheels.

The procedure is medically safe and completely efficient. Magnetic sensors located in the seat of the chair and the oral sensor assembly automatically scans for the presence of metal. Audio and visual alarms respond when metal is carried into the magnetic field. The measurement detects both ferrous and nonferrous material even if it is moving. The manufacturer claims it will detect contraband, which might go undetected by a hand-held detector. There is even a briefcase-sized model. The BOSS™ chair does require a power source of 110/240 V AC. Each piece of equipment weighs 68 pounds, and is 53×32×30.5 inches ("Body Orifice Security Scanner, B.O.S.S.," Internet:http://www.omni-security.com/product2/boss2.html, pp. 1-6).

FLIGHT VU™

AD Aerospace has created the Flight Vu Aircraft Data Recorder. This device combines a flight data recorder, cockpit voice recorder, and a flight video recorder. It is designed for large aircraft weighing

over 12,000 pounds and for helicopters weighing over 6000 pounds. Future air accident investigation teams could use the information for postincident investigation, but it also has security applications.

Flight Vu™ can engage up to eight channels of video pictures from inside and outside the aircraft. In the cockpit the equipment will help investigators understand what occurred or provide a real-time picture of what is occurring in the cockpit area. Reviewers could also get an idea of why an aircraft has had an accident or monitor an ongoing hijacking situation. This digital recorder is protected in a "crash free" environment and possesses a one hour "fire free" environment feature. This protects the flight data that has been recorded, as well as the cockpit voice and video from the external and internal cameras.

Airport and aircraft security is as important on the ground as it is in the air. Because Flight Vu™ offers up to eight cameras for internal and external use, the Flight Vu Defender™ constantly gives visual security for the aircraft, personnel, passengers, and the aircraft itself. While the aircraft is parked, protective measures are taken with Flight Vu™ to make sure the aircraft is safe and secure. Certain areas around the aircraft are constantly supervised, and when an incident occurs in these areas, the motion is taken note of by the video motion detection (VMD) technology. An onboard camera records the movement, and the picture is transmitted by a low-power microwave spread spectrum to a ground station location. These pictures can be transferred all over the world by continental telephone links whether they are mobile or on land. This transfer only takes seconds to complete and could be very useful to interconnected airports for security reasons; especially terrorist acts. The Flight VU Defender™ permits security to view the internal and external parts of the aircraft from any of the eight cameras, giving them a pretty accurate depiction of an overall situation. Flight Vu™ also allows security to monitor and keep track of airport personnel such as those who handle luggage and mechanics who work to fix and maintain the aircraft. The cockpit crew, flight attendants, and passengers may also be monitored. Using the Flight Vu™ witness system could also prevent passenger disturbances on the aircraft. It contains closed circuit television cameras that are attached to a video recorder that is digital. These cameras could prevent litigation if passengers are ejected because of "rage" incidents or disturbances. These cameras promote the safety and protection of passengers and the crew by letting potentially enraged people know they are being videotaped. The cameras cover the inside of the aircraft, which can record all of the passengers because of the wide angle. The camera can record during the entire flight or just when personnel desire it. A panic button can also activate the witness system. Because Flight Vu™ is a recorder, the video can be viewed anytime while on the aircraft or at a different time. Digital recording means that these videos are state of the art and are precise. They also can be rerecorded or copied for other purposes such as litigation.

Cabin security is a rising threat against flight attendants. There has been a significant increase in assaults. Flight Vu™ would not only have evidence, but also protect the crew from allegations of any misconduct. Additionally, Airbus is considering the purchase of and installation of a set of tiny concealed cameras above some of its passenger seats. The aerospace division of Goodrich is developing the technology. The newest video cameras have lenses no larger than a pinhole. The signal can travel up to 30 meters, and the transmitter will be surrounded by a small ring of infrared light-emitting diodes to send a readable signal in both daylight and darkness. The pilots will be able to monitor small screens in the cockpit.

BIOSIMMER™

Sandia National Laboratories has brought virtual reality into the realm of airport security. This particular virtual reality application allows rescue personnel to practice responding to a terrorists attack. The simulation involves the release of a biological agent in a small airport. The responding security or health personnel are immersed into a three-dimensional computer simulated setting of virtual patients in a virtual disaster. The program seeks to specifically aid medical personnel to make instantaneous and correct decisions and to avoid becoming victims themselves of the terrorists.

Like video games, the simulation can be run over and over again. Mistakes can be corrected and appropriate responses ingrained in the student. Such instinctive responses are difficult to teach, especially in a potentially contaminated environment. The computer simulation engages the user's eyes and ears by wearing sensors on the arms, legs, and waist. All the user's actions are fed back into the simulation. Users are also taught the significant lessons of self-protection by learning initial decontamination procedures for themselves and the victims.

The airport used in the simulation is a one-story, simple three-gate facility. The software program recreates the disbursement of the biological agent, in this case Staphylococcal enterotoxin B (SEB) throughout the airport. The program, although simulating a small airport explosion, would still be particularly useful for larger airport personnel as well. The Defense Advanced Research Projects Agency (DARPA) funded the research. The program's potential benefits are self-evident. The Department of Energy's Office of Science and Technology Pilot Projects in Biomedical Engineering Program continues working to make the program even more realistic.*

QUADRUPOLE RESONANCE DEVICES

Quadruple resonance devices, or QR technology, is a variation of the commonly used magnetic resonance imaging (MRI) technology used in hospitals and already in some baggage-scanning equipment at airports. MRI machines utilize large magnets that affect the magnetic properties of the nuclei of the water in the human body. Those magnetic properties enable the machine to generate an image. QR does not use a magnet. The technology operates under the principle that a magnetic resonance signal can be detected from explosives without applying a large external magnetic field:

- A transmitter emits pulses of low-intensity radio waves.
- Nuclei within the explosive are momentarily aligned with the radio waves.
- After each pulse, the nuclei emit a characteristic radio signal, like an echo.
- The signal is picked up, amplified, and analyzed.
- A computer issues a warning if it identifies a signal that is emitted only by explosives.

One of the problems with virtually all the existing technologies used to find hidden explosives, such as x-ray or radar, is that they pick up too many ancillary objects. A gun may give off a signal, but a rock or any piece of metal also may give a signal. QR sensors pick up the so-called resonance frequency, which is quite specific for different explosives. Additionally, unlike electromagnetic systems, QR sensors can detect plastic-encased explosives.

Pioneering developments in QR took place in the 1980s at the Naval Research Laboratory (NRL). The FAA came to NRL in 1983 looking for advice on how to use the QR technology for detecting explosives in luggage. Since 1987, funding for QR work has come from the FAA and the Department of Defense. NRL patented the technology, but in 1993, the laboratory gave an exclusive license to Quantum Magnetics, a San Diego-based company. One scientist explained that "the beauty of QR is that it is highly sensitive to the chemistry of explosives. If a bag containing explosives is scanned using QR, the machine flashes a red light. And so far, tests have shown that the technology accurately detects the presence of explosives without false alarms" (Irwin, 2001).

* *Note:* Sandia is a multiprogramming laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the Department of Energy. With major facilities in Albuquerque, NM and Livermore, CA, the company has major research and development responsibilities in national security, energy, and environmental technologies and economic competitiveness (Internet:http://www.sandia.gov/media/NewsRel/NR1999/biosim.htm).

INTELLISCAN™ 12000 METAL DETECTOR

This metal detector has 18 horizontal and vertical zones and is one of many metal detectors on the market. This particular model is manufactured by Ranger Security Detectors located in El Paso, TX and exhibits some of the newest state-of-the-art metal detection equipment currently available (Internet: www.rangersecurity.com). According to the manufacturer, the Intelliscan 12000™ was one of the first walk-through detectors to accurately pinpoint the exact location of weapons. They are continuous wave multiple-zone detectors. In other words, they are continuously active and cannot be switched or programmed to a deactivated mode. They provide a high level of protection and function in difficult environments because they are equipped with six computer-controlled horizontal zones of detection that perform as independent metal detectors. The vertical segments monitor the left, center, and right side of a person whereas the horizontal zones determine the height at which a weapon is carried.

As a weapon or contraband object is transported through a zone, the zone's receiver channels the data, and sophisticated mapping software compute its position within the archway. Security personnel can quickly and accurately locate the material identified. The equipment has a detection-enhancement option. This option is designed for sophisticated users that wish to design and optimize their own detection programs. It allows customized detection profiles to be created for advanced weapon and asset protection applications. The design procedure is implemented using a microprocessor. A software program analyzes metal objects that are passed through the detector. It generates a characteristic signature for each object. Once a signature has been created for an object, its detection response can be precisely manipulated. Ferrous, nonferrous, stainless steel, or composite objects that are difficult to detect can be specifically targeted. As is usual, their low-intensity magnetic fields have been certified safe for users of heart pacemakers and implanted defibrillators.

BIOMETRIC SYSTEMS

When an employee requests access to a restricted area, that person's identity needs to be verified before entry is granted. A guard has historically performed this process manually. However, the current generation of biometric identification devices offers numerous cost and performance advantages over manual security procedures. These innovations in technology have dispensed with the requirement of a human being present at all access points. Modern identification verification systems have greatly improved in the last decade and now include newer biometric recognition features.

Some of the available applications have been expanded to include physical access control at portals, computer access control at terminals, and telephone access control at central switching locations. Airports may have a single, stand-alone verifier, or it may have a large networked system consisting of numerous verifiers, controlled at a single central security site. In choosing the most suitable biometric device, serious consideration needs to be given to the performance criteria of a particular piece of equipment.

Essentially, biometric security systems recognize unique physical traits such as fingerprints, signatures, voices, and retinas. Another popular biometric access control system employs a technique of recognizing three-dimensional data about a person's hand geometry. Biometric systems are basically of two types: verification and recognition. A biometric identification device automatically verifies a person's identity from measuring a physical feature or repeatable action of the individual. However, the human factor significantly affects the performance. Each mechanism can also be affected by environmental factors such as noise, light, moisture, dust, temperature, and electromagnetic radiation (Hodgson, 1994).

Verification systems require that the individual seeking access have some sort of identification, such as a card, that is matched with some physical characteristic of that person to make the verification. A reference measurement of the biometric is obtained when the individual is programmed into the device. According to one expert, only retinal scan systems have the practical capability of

operating as a true recognition device, not requiring a personal identification number or code to corroborate the biometric search process (Bowers, 1994).

There are now numerous biometric systems on the market, and they vary in performance capability. Of course, performance is a very critical issue, but it is not the only factor to consider in choosing an appropriate biometric system. The best device for each particular environment must be determined, and the device must be suitable for the facility in which it is installed. The newest systems have computer interfaces and state-of-the-art software provides effective security management with real-time control, transaction recording, and audit capabilities. As mentioned, the current generation of devices is both reliable and cost effective, but the greatest challenge to the industry is to create product familiarity and acceptability.

In determining reliability, false positives are a key indicator. False rejection is the rejection of an individual who makes an honest attempt to be verified and gain entry. These are considered Type I errors. False acceptance or Type II error is the acceptance of an imposter. Some systems do indeed permit access to individuals without the proper authorization. False acceptance attempts are generally considered passive, meaning that the intruder has used his or her own biometric features as opposed to simulated or mechanically produced biometrics. Even if a system has a two percent false positive rate, that means that there is a 98 percent probability that an imposter will be unable to access the system, resulting in fairly good security management. Users seem to prefer a system that produces the fewest false rejects and takes the least time to use.

Most users would rather have the system slightly slower than have a high false rejection rate; but those gaining access who have to wait often get impatient. When evaluating systems, it is best to consider the average transaction time to enter a personal identification number (PIN), present the biometric feature, and to receive the verification or rejection result. In practice, the device must be effective and sufficiently quick not to annoy those using it. From a security prospective, prevailing computer interfaces and software provide real-time control, an audit trail, and sophisticated transaction records.

One of the first commercial passenger applications was tested at London's Heathrow Airport in the fall of 2001. The system, manufactured by Eye Ticket Corporation of McLean, VA, encompasses a scanner that scans the eyes of arriving passengers in about two seconds. Frequent fliers were encouraged to enroll in a six-month test program. "A similar Eye Ticket™ system has screened airline and airport employees at North Carolina's Charlotte Douglas International Airport since May 2000" (Heathrow to Try Eye Scanner, 2001).

FACE IT™- ACCESS CONTROLS

Super Bowl XXXV (2001) questioned the morality of a new biometric face recognition technology. Fans questioned whether the authorities had the right to use a public event to identify individuals by a mere photograph without any probable cause whatsoever. Cameras monitored fans as each ticket holder passed through the turnstiles. The Tampa Police Department had decided to use the new technology to scan for known criminals and terrorists as they entered the stadium. Civil libertarians wondered where this surveillance technology would lead and how such an intrusive system would affect the right to privacy of the average noncriminal fan.

One such system is commercially known as Faceit™. Developed by Visionics Corporation, it uses facial recognition algorithms to process facial images and match it to known criminals and terrorists. One competitor, Visage Technology, developed a similar system commercially known as "FaceFinder™," which was the actual system deployed during the Super Bowl (Face off Over Super Bowl Spying, Internet: www.securityfocus.com). Other suppliers of the technology include Graphco Technologies (Face-trac™), Raytheon, and Veltek International. All of the systems consist of computers that use a facial recognition software engine to accurately detect and recognize faces in a matter of seconds.

The system utilizes software called local feature analysis that codifies the face into different features. It operates from the statistical representation of universal facial shapes. In other words, the software is composed of various programming languages that turn numerical data into useful information, including digital photographs. The new technology uses both the characteristic facial shapes and its features, and the geometric pattern in which they are combined on a face. The software employs a complex mathematical formula to develop a map of an individual face, called a faceprint (FaceIT Face Recognition-the Technology, Internet: www.faceit.com/faceit/tech).

Once a particular face has been recognized, it is put through a process that normalizes the image. This process takes into account the expression, position, lighting, and size of a face and transforms the image into the faceprint. A faceprint has the ability to take into account the intrinsic features of facial shape and cannot be inhibited by attempts to alter one's appearance, such as glasses, hair, and facial expression. However, the identity of an individual is only acquired when it is compared against a faceprint already in the system. FaceIT™ can perform identity matches against a database of set individuals and individuals it has been programmed to recognize from its databases.

Common ways in which the FaceIT™ technology is used is in identification, verification, monitoring, and surveillance. Identification or one-to-many searching is used to determine someone's identity against a database of individual facial images. FaceIT™ can return a list of possible matches, those that resemble each other, or the exact identity of the subject. Verification or one-to-one matching matches the live faceprint to a stored faceprint. If the confidence level of the match exceeds a certain percentage of certainty, the match is considered successful and identity verified. Monitoring uses FaceIT's™ ability to follow the presence and position of a person in its field of view. Surveillance can continuously track an individual and select him or her from the field of view. The system also has the ability to detect an individual on a specific database, give notification of his or her presence, and track his or her actions.

FaceIT™ is tested for accuracy against false acceptance rates, false rejection rates, and equal error rates that are dependent on the database used to perform a facial analysis. These rates are a mathematical function, similar to a calculus function with trigonometric sine and cosign graphs showing how they intersect. The point at which the two curves intersect represents the equal error rate, the rate at which the number of people incorrectly accepted and correctly rejected is determined. For FaceIT™, the equal error rate is 0.68 percent. Automatic facial alignment failure occurs between 1 and 2 percent of the time.

The courts have yet to decide if the technology, when deployed in a public forum, should be considered unconstitutional as a violation of the Fourth Amendment's prohibition against unreasonable search and seizure. The Fourth Amendment only restricts the actions of government officials. It does not prohibit private firms such as banks or stadiums from face-scanning. It is likely the courts will note that citizens have the least amount of expectation of privacy when they are in public, including airports.

IMAGING TECHNOLOGIES

Imaging technologies generally involve the use of ionizing radiation (x-rays) to produce images of individuals and objects that may be concealed under layers of clothing. The images are produced using computer analysis of reflected, absorbed, or scattered radiation (active imaging) or of natural radiation emitted from the human body (passive imaging). Both processes are currently being used in airports. As mentioned previously, for active imaging, small doses of radiation are used in the imaging process. The level of exposure to x-rays in passenger screening in order of magnitude is well below the x-ray levels used in medical diagnosis and represents a fraction of one percent of the natural background to which the U.S. population is exposed annually (see Figure 13.2).

FIGURE 13.2 Backscatter technology has been criticized for revealing a tad too much.

TRACE-DETECTION TECHNOLOGIES

Trace-detection technologies for passengers have their own medical drawbacks, hygiene being the most basic shortcoming. Personal contact may be a vehicle for transmitting various microbial diseases from one individual to another. A trace-detection device that requires the passenger to actually touch the door before entering means that the individual could leave some disease-producing microorganisms behind. Experts have reasoned that if the transfer of infectious diseases in the passenger screening setting were to occur, it would most likely result from the hand-mediated transfer of disease producing microorganisms. The likelihood of disease transmission during passenger screening is dependent on numerous disease-specific factors. They include the integrity and cleanliness of the skin and other host factors, such as the virulence of a disease causing microorganism and the actual amount of organisms transferred.

Cleanliness is the key. The new trace detection equipment should be designed to allow frequent cleaning to minimize disease transmission from passenger to passenger. Passengers will demand it, and the airlines will not want to expose themselves to any unnecessary liability. The use of small wands that can sniff traces of explosives presents an interim alternative. Ion Track Instrument sells the small computer-enhanced wands for around 40,000 U.S. dollars. They are currently being used in Salt Lake City, UT where officers pass the wand over luggage while passengers wait in line at the ticket counter.

FUEL FLAMMABILITY

Fuel produced in a factory has to be moved to a transportation facility and eventually pumped into the using vehicle. Some fuel is shipped directly to a fuel storage facility at a transportation mode, but usually it must be shipped via several intermediate storage facilities. Many different transportation modes can be utilized including pipeline, ship, barge, railroad tank car, and tanker truck.

However, pipelines are best suited for large volumes of fuel. The fuel is vulnerable during the entire supply chain.

Additionally, the attack of 11 September utilized a new weapon of mass destruction, one that took advantage of a fuel-laden aircraft. An aircraft carrying 50,000 pounds of jet fuel has an energy content equal to millions of pounds of TNT, not including the impact energy of the plane itself. Most damage, however, is likely inflicted by burning fuel. This threat was exercised not only against passengers, but also against buildings and people on the ground. New requirements in the last decade such as fire-resistant materials inside all sorts of vehicles have reduced the danger, but most post-crash fires involve fuel as well.

The new threat scenario changed the ground rules for research in the area of fuel fire vulnerability reduction. Essentially, the approach of passenger survivability that assumed aircraft impacts of approximately 150 miles per hour was accelerated to impacts at velocities in the range of 500 mph, typical of terrorist-type threats such as those that occurred on 11 September 2001.

Technology advances in this area have focused on mist-control kerosene, and research is being conducted at the Jet Propulsion Laboratory, California Institute of Technology, and Southwest Research Institute. The primary difference in this concept and the earlier concept of antimisting control kerosene is the impact velocity mentioned above. The research is in its infancy but shows great promise. The difference involves the ignition energy and the state of the fuel, liquid or mist-vapor. Fuel in a mist state can be ignited at very low energy.

REMOTE-CONTROLLED AIRCRAFT

Military use of remotely controlled vehicles has been actively pursued. The government acknowledged immediately after 11 September that the government would indeed consider all kinds of technology including methods to enable air traffic controllers to take over control of distressed aircraft and to be able to land aircraft by remote control. Pilots, accurately pointing out a potential vulnerability, have expressed concern over potential terrorist ability to gain access to the controllers on the ground. Taking control from the ground is very feasible, and terrorists might just seek to avoid the problems associated with gaining entry to an aircraft by simply attacking the air traffic control tower or a remote site. However, the alternative applications and capability to land aircraft on the ground is an attractive one.

Researchers and corporations supporting those research efforts have publicly stated that it would not be difficult to adapt remote control technology to commercial aircraft. Tom Cassidy, President and CEO of General Atomics Aeronautical Systems Inc., wrote a letter to President Bush which stated, “Such a system would not prevent a hijacker from causing mayhem on the aircraft or exploding a device and destroying the aircraft in flight, but it would prevent him from flying the aircraft into a building or populated areas” (Long, 2001). General Atomics developed the remotely controlled reconnaissance plane for the U.S. Air Force.

The completed technology would provide the pilot with the choice, at the flick of a switch, to turn control of an aircraft over to a controller on the ground, preventing anyone else on board from diverting the aircraft. The system would control airborne aircraft nationwide from just two locations using satellite links, making efforts to protect the facilities more feasible. No pilot likes turning control of any aircraft over to someone else, but the technology has many attractive applications. It would also obviate the need for pilots to arguably be armed.

IMPROVED CLOSED-CIRCUIT TELEVISION TECHNOLOGY

The first closed-circuit television (CCTV) cameras used in public spaces were crude, conspicuous, low-definition black and white systems without the ability to zoom or pan. Modern CCTV cameras use small high-definition color cameras that can not only focus to resolve minute detail, but by linking the control of the cameras to a computer, objects can be tracked semiautomatically. For example,

they can track movement across a scene where there should be no movement, or they can lock onto a single object in a busy environment and follow it. Being computerized, this tracking process can also work between cameras. The implementation of automatic number plate recognition produces a potential source of information on the location of persons or groups. There is no technological limitation preventing a network of such cameras from tracking the movement of individuals.

CCTV critics see the most disturbing extension to this technology is the recognition of faces from high-definition CCTV images. With this technology, it would be possible to determine a person's identity without the need to stop and ask him or her in the street, or even alert him or her that his or her identity is being checked and logged. The systems can check many thousands of faces in a database in under a second. This combination of CCTV with facial recognition technology has been tried as a form of mass surveillance, but has been ineffective because of the low discriminating power of facial recognition technology and the very high number of false positives generated. This type of system has generally been proposed to compare faces at airports and seaports with those of suspected terrorists or other undesirable entrants.

The latest developments in CCTV and imaging techniques, being developed in the United Kingdom and United States, is developing computerized monitoring so that the CCTV operator does not have to endlessly look at all the screens. This also means that an operator can run many more CCTV cameras. These systems do not observe people directly. Instead they track their behavior by looking for particular types of movement, or particular types of clothing or baggage. The psychological theory behind this contends that people in public spaces behave in set and predictable ways. People, who are not part of the crowd, do not behave in the same way. The computer can identify their movements and alert the operator that they are acting out of the ordinary.

The same type of system can, if required, go one step further and track an identified individual as they move through the area covered by CCTV. This is currently being developed in the United States as part of the project cofunded by the U.S. DARPA. With software tools, the system will be able to develop three-dimensional models of an area and track and monitor the movement of objects within it. To many, the development of CCTV in public areas, linked to computer databases of people's pictures and identity, presents a serious breach of civil liberties. Critics fear the possibility that one would not be able to meet anonymously in a public place or drive and walk anonymously around a city. Demonstrations or assemblies in public places could be affected as the state would be able to collate lists of those leading them, taking part, or even just talking with protesters in the street. The use of CCTV in the United States is less prevalent than in Europe, although increasing, and generally meets stronger opposition. The use in France is also not as prevalent as in the United Kingdom. After the bombings of London on 7 July 2005, CCTV footage was used to identify the bombers.

COCKPIT DOORS

Current cockpit doors installed immediately after 11 September have proven problematic. An American Airlines Flight, for example, was 35,000 feet over Kansas when the Captain became incapacitated after a 12-pound panel from one of the newly fortified cockpit doors popped out and hit him on the head. In addition, a British Airways Flight from Calcutta, India to London was cruising over Europe when the captain declared an emergency after noticing a burning smell. The plan landed in Latvia and discovered an overheated electrical component in a new antihijacking door. There have been at least 35 reported incidents involving problems with the doors since August 2002.

The fortified doors, required by U.S. and international aviation authorities after the attacks of 11 September, were designed to withstand extreme pounding and a hail of bullets. In early 2003, a move to require fortified cockpit doors on cargo aircraft fell apart after cargo airlines were granted an exception if they filed a security plan. Regardless, FedEx now has reinforced doors on most of its aircraft. The government noted that although cargo airlines carry some passengers, cargo pilots are more likely to exclude suspicious passengers, usually noncompany employees.

Permali Gloucester Limited has completed the development and certification to FAA requirements of Permaglass X™, a hard armor material for use in the reinforcement of civil aircraft cockpit doors and bulkheads. Permaglass X™ is a lightweight composite that provides protection against hand-gun bullets per NIJ Level III A and also against physical attack. It provides high mechanical strength and stiffness, and is also fully compliant with all FAA flammability regulations for aircraft cabin interiors. A further benefit is that unlike metallic materials, the composite construction virtually eliminates the risk from ricochets. The composite also benefits from negligible water absorption and resistance to UV exposure.

All cockpit doors must comply with the following specifications:

- Ballistic protection to NIJ Standard-O101.04 Type IIIA
- FAR 25 APP F Part 1 – 60-second vertical burn
- FAR 25- APP F Part V – heat release
- FAR 25-APP Part F IV – smoke density

The measures to reinforce the cockpit door are noteworthy, and a lot of money has been expended to install them. However, the entire effort is only justifiable if the terrorists repeat the tactics of 11 September, which is certainly questionable.

CONCLUSION

New technology will ultimately completely change the face of all airport screening, whether it be cargo or passenger screening equipment. No airport or airline is completely secure and likely never will be. The advances made in technology will have both positives and negatives related to them. The public will have to decide just what is too intrusive or unsafe in the long run.

Scientific experimentation has determined that health issues are primarily a perception of risk rather than an actual health threat. Passengers are suspect of any device that can potentially cause cancer, interfere with their pacemakers or mechanical hearts, or hinder the development of their children. Any new technology on the market will have to take these perceptions into consideration.

Overall, the real risk is insignificant to the perceived risk. Consequently, airlines and the manufacturers of screening equipment need to educate the public. Airport security personnel also need to be trained on the basic principles of each device so they can answer basic questions of passengers. They are not required to understand all the technical theories relating to radiation, electricity, or possible medical repercussions, only enough to reassure the public. Written material should also be available for distribution if the passenger should request it. This type of resource material will be essential in convincing the public to accept even more intrusive screening methods.

One of the remaining facets of new technology is who has access to it. Terrorists are perfectly capable of using technology against democratic societies as quickly as new technology is developed and implemented. They are also capable of using beneficial technology in a sinister manner. The import and export of technology must be tightly controlled and monitored. Unfortunately, most technologies can be used in a number of ways, both positive and negative, and therefore will be.

REFERENCES

Arik Ben-Ari, Israel Civil Aviation Authority CNN, 2004.

Associated Press, "Bag Screening Underutilized Airlines Slow to Use Bomb Detection Equipment," *Chicago Tribune*, 11 Aug 1999.

Body Orifice Security Scanner, B.O.S.S., http://www.omni-security.com/product2/boss2.html, pp.1–6.

Bowers, Kim, "Premises Security Without Keys, Codes, Cards and Combinations," *Security Concepts*, December 1994, pg 19.

FAA Reauthorization Bill 106th Congress 201, 1999.

FaceIT Face Recognition-the Technology, www.faceit.com/faceit/tech.
Face off Over Super Bowl Spying, Security Focus.com, www.securityfocus.com.
Heathrow to Try Eye Scanner, *Los Angeles Times*, reprinted *Star Tribune* Sunday 26 August 2001, pg. G-5.
Hodgson, Karyn, "Hot and Cold Biometrics Heat Up Again," *Security*, Cahners Publishing Company, Newton, MA 1994, Vol. 31, No. 11, pg. 17.
http://home.earthlink.net/~jimlux/hv/hvtrigsg.htm.
http://www.signonsandiego.com/news/business/20070116–1146–c–airlineranti–missile.html.
http://www.fbi.gov/page2/dec07/counterproliferation121307.html.
http://www.sandia.gov/media/NewsRel/NR1999/biosim.htm.
www.rangersecurity.com.
Irwin, Sandra I. "Bomb-Detection Technology Useful for Countermine Ops," http://nationaldefense.ndia.org/article.cfm?Id=442, pg. 1–5, 9 August 2001.
Long, Jeff, "Landing by remote control doesn't quite fly with pilots." *Chicago Tribune*, 28 September 2001,
Shenon, Philip, "General Atomics developed the remotely controlled reconnaissance plane for the US Air Force." *New York Times*, reprinted *The Arizona Republic*, 7 August 2003, pg A-8.
Web Investor Conference, On-line, Wednesday, 20 May 2003.

14 Airport Operator Concerns and Other Safety and Security Issues

The Foundations of Security

NEWS

16 May 2001: The National Transportation Safety Board (NTSB) names runway incidents as one of the nation's top transportation safety issues each year since 1990.

2002: Nearly 60 percent of 800 business travelers polled in January by Yesawich, Pepperdine & Brown, a research firm in Orlando, FL, said they would drive rather than fly whenever they could for future business trips. And nearly 30 percent of 1000 workers said in February that their companies now required or recommended driving instead of flying on business trips, according to the Travel Industry Association of America.

23 April 2002: United Airlines has begun training its pilots to use stun guns for self defense in the cockpit. The idea that "frangible" bullets might be loaded into handguns carried by cockpit crews also represents a new turn. They are 30 percent lighter than normal bullets and shatter when they hit; being unlikely to penetrate aircraft panels.

February 2007: A passenger of "Somali descent" enters the cockpit of an Air New Zealand flight and stabs the two pilots. Authorities say the woman had been issuing bomb threats beforehand. It is still unclear how she got inside the cockpit, which is supposed to be secured at all all times, per ICAO and airline regulations.

March 2008: Two airline employees at Newark's Liberty International Airport are charged with smuggling heroin.

INTRODUCTION

Airport security managers are responsible for the safety of huge numbers of people, very expensive aircraft, in addition to airport terminals and surrounding areas. Clearly the burden is a difficult one and requires the possession and mastering of numerous skills. Passengers and luggage must undergo screening; building, ground crews, and maintenance people must keep things running safely and smoothly; and security guards must maintain the peace in lobbies, terminals, and parking areas. Security managers must be aware of threats not only from terrorists and common criminals, but also a myriad of other safety aspects of any complicated air terminal environment. The challenge is significant and any lapses can be costly in terms of human life and assets.

Sincere concern should be addressed to the problem of the proliferation of nuclear weapons. The International Atomic Energy Commission (IAEC) held a conference in Stockholm, Sweden, in May 2000. They reported more than 370 confirmed incidents of nuclear trafficking since 1993.

The General Director of the Commission was quoted as saying, "Looking toward the future, it is clear that real international cooperation will be needed to upgrade security measures, to improve capabilities for intercepting and responding to illicit trafficking, and to enhance the protection of facilities against terrorism and sabotage" (*World Tribune*, 2001). Unquestionably, the time and production capabilities to build a nuclear bomb are considerable. However, according to some leading scientists, the production of sophisticated devices is conceivable. A nationally supported program or a very wealthy terrorist group could produce a bomb if they are provided the necessary resources and facilities and an established working place with the time to build it (Carson et al., 2001).

As the potential threat of chemical, biological, and other unconventional weapons grows at the local, state, and federal levels, preparation for such an event is rapidly becoming a significant issue to the private sector. Private security managers and law enforcement officials at all levels now need to address the age-old question of "what if."

It has become clear that airport security officials need to be educated to the fact that biologic, chemical, and nuclear threats are not just the concern of international policymakers and national level law enforcement. More specifically, the silent partner of the weapons of mass destruction (WMDs) triumvirate, biologicals, could become the most insidious danger of the three. In March of 1996, the President of the International Association of Fire Chiefs informed the U.S. Senate that it would be the responsibility of local fire-fighting, police, and emergency personnel to cope with any attack by biological weapons and that unfortunately they were likely not up to the task.

During the Cold War, the United States and the former Soviet Union amassed thousands of nuclear weapons and stockpiled thousands of tons of chemical weapons. The Soviets, among others, were also developing a comprehensive biological weapons program designed for use against their potential enemies. With the disintegration of the former Soviet Union, thousands of technical specialists and an extensive array of biological weapons are still out there. Furthermore, there is very little being done to collect intelligence on issues of biologicals and even less is being done to share the information between agencies. If any effective management of an incident is to be successful, renewed interagency cooperation and communication will be a crucial necessity. In conjunction, private sector and airport security managers must recognize the threat as a viable one and take reasonable precautions to prepare for it. Conventional weapons remain a considerable threat, although knowledge of the entire terrorist toolbox is essential for defeating them.

AIRPORT RUNWAY INCURSIONS

The Federal Aviation Administration (FAA) definition of a runway incursion is an "encounter at an airport between a plane that is taking off or landing, and any other object or person that creates a risk of collision, or results in less than the recommended separation distance." Runway incursions have been an issue in aviation for more than three decades, but have become one of the primary safety concerns at modern airports as air traffic and congestion increase. Airport security obviously cannot control miscommunications between a pilot and air traffic controllers, but other incursions onto a runway can be monitored and controlled.

Incursions onto runways continued to increase, rising from 186 in 1993 to 325 in 1998. About 56 percent are admittedly related to pilot error; the rest are operational errors caused by controllers or vehicles and pedestrians who enter restricted areas (Levin, 2001). However, in fiscal year 2005, incidents numbered only 45 but rose again to 58 in fiscal year 2006. Overall, controllers at most large airports believe that understaffing and heavy workloads contribute the most to safety problems. Controllers are forced to work longer hours under tremendous amounts of pressure for unreasonable periods of time. According to the controllers' union, a majority of runway accidents occur on the fourth or fifth day after a five-day tour, when fatigue is a major factor (Alonso-Zaldivar, 2000).

The FAA has issued numerous "safety action plans," but little improvement has been seen. In addition, the airport surface system, or Area Surface Detection Radar systems, around the United States have been neglected for years. They need to be upgraded and improved. The FAA had agreed

to allocate $5 million to companies for developing new systems to improve security aspects such as better lighting, surface surveillance, and improved markings and signs. In May 2001, the FAA approved a new runway collision warning system. The system is operating in San Francisco and Detroit and has now been deployed at many other major airports. The system utilizes radar to track airplanes and airport vehicles on the airport field. It alerts air traffic controllers to the potential of a collision but not the pilots (New Technology Targets Runway Safety, 2001). This system alone will improve the runway traffic system but is not the total answer to the problem.

In a report on access control at airports, the Inspector General of the FAA criticized security measures and suggested greater use of access control equipment; more detailed training, and better-implemented oversight programs. In other words, controlling access to the runway is very important and remains the domain of airport security officials. It is advisable that all members of the security staff have at least a cursory understanding of the operational controls of the runways and taxiways so as not to interfere with them and to keep others from inadvertently intruding. Runway incurions are divided into three categories:

- Operational error (OE) – A failure of the air traffic control system that results in loss of separation
- Pilot deviation (PD) – The action of a pilot that results in violation of the federal aviation regulations (FAR)
- Vehicle/Pedestrian deviation (V/PD) – Any entry or movement on the movement area by a vehicle (including aircraft operated by nonpilots) or pedestrian that has not been authorized by air traffic control

The FAA further explains that all runway incursions are surface incidents, but not all surface incidents are runway incursions. To qualify as a runway incursion, an aircraft that is taking off, intending to take off, landing, or intending to land must encounter both of the following conditions: (1) at least one aircraft, vehicle, pedestrian, or object must be on the runway; and (2) a collision hazard or a loss of separation must occur (Internet: http://www.faa.gov/aso/RunwaySafety/runway_incursions.htm).

PASSENGER INTERFERENCE

Passenger misconduct on flights is a growing problem and becoming more serious as the passengers sometimes interfere with the ability of the crew to maintain a safe aircraft. Interference by passengers, during and prior to flight operations, includes everything from verbal abuse to outright assault and is usually caused by excessive alcohol consumption, but it can also be just the result of simple air rage. When the disruption in flight operations is between two passengers, the airline is in a very difficult position and may even be liable, depending on a court's interpretation of current law. In any case, airport security must be prepared to assist the crew both before takeoff and after landing.

The Association of Flight Attendants has adamantly criticized both the U.S. Justice Department and the FAA for alleged failure to require airlines to report all incidents and to train air crew members to handle these hostile situations. Additionally, the FAA has yet to levy and collect fines as a deterrent to such incidents (Hatcher, 2001). The U.S. Justice Department also has yet to empower local law enforcement or airport security to formally arrest perpetrators of air rage when it occurs on the aircraft. Jurisdiction of the crime is strictly federal. The flight attendants' association argues that because of this dereliction that the government is failing to protect passengers and to promote cabin safety. Contrary to published statistics, the flight attendants believe there were more like 4000 incidents of air rage in 2001 but the total number must be analyzed in light of the fact that more than 600 million passengers flew the nation's airlines. Consequently, the incidents are relatively isolated.

According to flight crews, passenger interference with flight crews has already reached epidemic proportions. Captain Stephen Luckey, Chairman of the National Security Committee of the Air Line Pilots Association, testified before the U.S. House of Representatives on 11 June 1998 about

the seriousness of this issue. He testified regarding the increasing problem of passenger interference with flight crews and the "Carry-On Baggage Reduction Act of 1997." Specifically, he stated, "passenger interference is the singularly most pervasive security problem facing the airline industry, not only in the United States but around the globe" (Internet:http://www.alpa.org/internet/tm/tm061198.htm, 22 April 2001, pg. 1). He clarified the concept that such interference poses demonstrably real hazards to the safety of passengers, crews, and the flight. He reasons that newer aircraft now have only two pilots in the cockpit. Therefore, sending a pilot into the cabin to resolve a dispute could seriously diminish the safety of the flight; especially if the pilot is injured.

He attested to the following incidents at the hearing (http://www.alpa.org/internet/tm/tm061198.htm, 22 April 2001, pg. 2):

- Shortly after takeoff on a flight from Savannah, GA, to Charlotte, NC, a man created an altercation with other passengers and flight attendants after his demands for more alcohol were not met. During this episode, he tried to break down the cockpit door. He also grabbed the lead flight attendant and threw her against the cockpit door, then attempted to throw her off the plane through an emergency door. The perpetrator was eventually sentenced to 51 months in prison and 200 hours of community service, and was ordered to pay $611 in fuel costs (July 1996).
- A visibly inebriated professional wrestler boarded an aircraft in San Francisco and was subsequently asked to disembark before takeoff. He was a gigantic man who was obviously intoxicated. The crew clearly viewed him as potentially dangerous because of his physical condition and obvious signs of alcohol-induced misconduct. He left the aircraft as requested, but became combative in the jetway, and several people, including police, were required to help restrain him (June 1996).
- On a flight from Frankfurt, Germany, to Dulles International Airport, a German tourist complained that the flight attendant had bumped him with the food cart. The flight attendant apologized, but the passenger nevertheless threw the flight attendant against the emergency exit and hit him on the head and face. Three other passengers eventually pulled the attacker off the flight attendant (1996).
- Two passengers boarded a flight at Los Angeles International Airport and became disruptive after being denied a request for an upgrade to the first class section of the airplane. One of the passengers went to the galley and grabbed two coffee pots, which he wielded as weapons. He poured hot coffee on two flight attendants, causing second degree burns on the hand of one of the crew members. A female passenger then joined in the fray and banged on the cockpit door yelling that she had a gun (July 1997).

Such incidents are statistically increasing in frequency and volatility. The passengers, who are without political goals like terrorists, are creating unpleasant and potentially dangerous incidents prior, during, and after flight. Airport security is currently simply "unavailable" once the flight is airborne. The crew needs to be prepared to handle the situations. Of course, all the resources available to control assaults on the ground are still on the ground. Some airline pilots, however, have been known to conceal plastic hand restraints inside their designated uniform hat, successfully getting them by security for use in the air if necessary. The limited resources the aircrew has to handle a potentially serious incident are sealed inside with them (see Figure 14.1).

FAR Part 91.17 or FAR 121.575 makes it illegal for airlines to board someone who appears to be drunk, but unfortunately it is not very easy to determine who exactly is drunk. Excessive alcohol consumption can be hard to detect during the boarding process. Not all "drunks" are initially boisterous and loud. Even if an individual is not technically intoxicated on boarding, it is fairly easy to become so while airborne. Disproportionate alcohol consumption on board aircraft, particularly in first and business class where it is free, is probably the most often-cited reason for passenger interference. However, other causes include narcissistic passengers, authoritarian business executives,

FIGURE 14.1 Pilots participate in training to become flight deck officers.

passengers with flying phobia, celebrities with an attitude, and increased crowding on board the aircraft. The Association of Flight Attendants has recommended more responsible alcohol policies. They would prefer that drinks not be offered prior to takeoff, permitting the service of only one drink at a time and never using free drinks as compensation for delays. It is unclear, however, if alcohol is really the primary cause of most air rage incidents.

It is also not unheard of that the aircrew may have had too much to drink. Amendments to the rules of the Department of Transportation (DOT) in August 2001 require flight crew, instructors, mechanics, and others involved in the operation and maintenance of commercial aircraft to undergo routine testing for drugs and alcohol usage. The DOT has described the changes as "increased protection measures for the employee if an initial test result indicates that a specimen may have been altered or substituted; a plan to make validity testing mandatory; a procedure for employers to remove employees from their jobs temporarily while a test is under review; greater authorization powers to contract services providers; and enhanced training requirements for testing personnel" (DOT Amends Drug and Alcohol Rules, 2001). It is unfortunate but true that airline employees are just as susceptible to alcohol and drug abuse as any other segment of the population. Permitting them to fly is dangerous and prohibited but difficult to completely eradicate. Some would argue that the drug and alcohol problems in America have been greatly underestimated, and there are no safe sectors from which to draw absolutely drug free employees (Carroll, 1992).

Additionally, airlines are held responsible for passengers getting hurt by other passengers. In *Stone v. Continental Airlines,* 905 F. Supp. 823 (Hawaii 1995), a court relieved Continental Airlines from any liability relating to an incident where a passenger punched another passenger. The court held the Airlines Deregulation Act barred the plaintiff a remedy. The court also pointed out that the plaintiff was also barred from any recovery under the Warsaw Convention because the act was not an accident as defined by the Act. Other airlines have not been so lucky. In *Romano v. American Trans Air*, 56 Cal. Reporter. 2d 428 (Cal App 1996*),* a California court ruled just the opposite and held that a passenger could hold the airlines liable for allegedly failing to prevent one passenger from assaulting another.

It should be pointed out that falsely accusing a passenger of misconduct can also bring the plaintiff's attorneys down on airlines and security companies. In *Curley v. American Airlines, Inc.* 846 F.

Supp. 280 (S.D.N.Y 1994), a court ruled that neither the Warsaw Convention nor the Federal Aviation Act preempted an airline passenger's lawsuit for negligence and false imprisonment, claiming that the airline falsely identified him to Mexican authorities as having smoked marijuana on the plane.

AIR RAGE AND PASSENGER INVOLVEMENT

An additional serious and new threat, exasperated by crowded aircraft, is the concept of air rage with passenger involvement. Because trained security personnel are not aboard most flights, passengers have voluntarily jumped into situations to assist. On occasion such involvement has resulted in unexpected grave repercussions. On 11 August 2000, aboard Southwest Airlines Flight 1763, an incident occurred that had deadly results. The plane took off from Las Vegas, NV at about 9:30 p.m. and was scheduled to land about an hour later in Salt Lake City, UT. The first 30 minutes of the flight were uneventful. Then a young man, Jonathan Burton, began to pace back forth in the aisle. At first, he was just talking to himself and walking around, but later he became more hostile. He ran up to the cockpit and started to pound on the door. He succeeded in kicking a hole in the door and proceeded to attempt to climb through it. A group of male passengers saw fit to intervene.

They returned him to his seat but in a few moments he lunged toward the emergency exit and tried to open it in flight. The same group of male passengers attempted to restrain him and drag him to the back of the plane. Jonathan responded vehemently. In the ensuing scuffle, someone stood on his neck, and he went limp. Everyone involved believed that the passenger had been brought under control and waited for security to remove him from the plane. When the plane landed, the paramedics were called, and it was discovered that he was dead. Just how much force one passenger exerts over another is difficult for the aircrew to monitor let alone control. Most crews just want to see the unruly individual brought under control.

Incidents of this nature have been increasing. They range from a German bodybuilder who broke into the cockpit and grabbed the controls to a Japanese rock star choke-holding a stewardess. In the first example the plane plummeted 2000 feet before a dentist on board tranquilized him. In the second case, another passenger hit the pop star over the head with a flashlight.

More recently, on 18 March 2005; an American Airlines 767 was enroute from Los Angeles to New York's John F. Kennedy International Airport (JFK). During the flight, a passenger allegedly assaulted a flight attendant. The 48-year-old passenger was restrained by the cabin crew using flexible handcuffs. Reportedly, seven passengers also helped to restrain the passenger during the latter stages of the flight. At some point, the passenger had difficulty breathing. After landing at JFK, the unconscious passenger was taken to a local hospital where he was pronounced dead. The New York City medical examiner's office later ruled the death an accident that was caused by acute cocaine and alcohol intoxication, which was aggravated by heart trouble. No other crew members or passengers were seriously injured or killed (see Figure 14.2).

In another incident, during a Canadian Airlines flight from Toronto to London on 6 December 2007, the flight was interrupted by a passenger who began shouting. The man was suffering from an apparent panic attack and expressed the fear that he was about to be shot to death. He continued to repeatedly utter obscenities and racist comments. He was restrained by several members of the flight crew, and the flight landed safely at Heathrow Airport. Authorities did not place the passenger under arrest at London, and Air Canada indicated there was no danger from this outburst, but the incident represents the constant problem of a passenger on a long flight becoming unruly. The incident was publicized on YouTube.

Air rage has proliferated in the terminal as well. As more and more flights are canceled or delayed, passengers have turned violent. One family on its way to Walt Disney World experienced several delays in their flight. When they did start to board, the ticket agent indicated that something was wrong with their tickets. Meanwhile their child proceeded down the jetway. When the mother went to retrieve him, the agent pushed the mother. The father and the agent became entangled, and the agent eventually broke his neck. The father was accused of aggravated assault and was later tried

FIGURE 14.2 Learning to disarm a violent passenger. All airline personnel should be required to undergo extensive training in protecting themselves and other passengers in light of not only the terrorist threat but the rising threat from disruptive passengers. (Source: Transportation Security Administration. www.tsa.gov)

but found not guilty. The airlines were clearly not pleased with the result of the trial. The proliferation of the problem is quite evident, and the airlines have had difficulty in inhibiting it.

The FAA has issued the following statement regarding air rage (Internet: http://www.faa.gov/apa/pr/pr.cfm?id=1354):

> The Federal Aviation Administration (FAA) rules clearly prohibit passengers from assaulting, threatening, intimidating, or interfering with flight attendants. Our nation's flight attendants perform vital safety duties, especially during an aviation emergency.
>
> Unfortunately, some passengers continue to put the flying public at risk by choosing to engage in dangerous behavior aboard an airplane. The repercussions for passengers who engage in unruly behavior can be substantial. They can be heavily fined by the FAA or prosecuted on criminal charges. The FAA aggressively pursues each reported case and proposes substantial fines for the most egregious incidents. The FAA can propose up to $25,000 per violation for an unruly passenger case. One incident can result in multiple violations.
>
> The FAA believes that widely publicized criminal prosecution of air rage cases serve as a strong deterrent. The FAA, Federal Bureau of Investigation (FBI), local U.S. attorneys, local law enforcement, airlines, and crew members are working together to help prepare cases that the Justice Department can then prosecute. At several major airports, FAA security agents respond to the more serious incidents and help interview victims, suspects, and witnesses. The FAA supports Justice Department efforts toward full criminal prosecution, when warranted. The FAA has provided model training programs to airlines to help flight attendants manage instances of passenger misconduct. The FAA urges passengers to do their part to make their trip as safe as possible.

Air Rage and Civil Liability

In essence, the terms air rage or sky rage have come to mean conduct occurring during air travel that can fall anywhere between socially offensive words involving inappropriate threats, racial epithets, or curse words to criminal misconduct. Air rage is also described as intentional acts that are out of proportion to the usual frustrations related to air travel. They potentially endanger the crew and other passengers. Crew and passenger alike manifest the acts. One judge has reasoned that "air travel in modern society presents formidable safety and security concerns, and often passengers with criminal intentions are the source of that threat. But even passengers with merely bad tempers are as dangerous in some respects as any would-be hijacker" (*Smith v. ComAir*, F.3d 254, 258 [4th Circuit 1998]). As mentioned, the frequency of these events are increasing exponentially.

Some airlines even estimate that 50 percent or more of all incidents involve the excessive use of alcohol (Normani, 1998). The remedy is prevention. American air carriers already have the right to refuse to transport a passenger if the airline determines that safety is an issue (Sec 49 USC 44902 (b) 1994). To protect itself from liability, the airline must always act reasonably in refusing someone access to the aircraft or removing them from one. However, beyond preventing access to the aircraft, little organized prevention of in-flight incidents exists. The Senate Commerce, Science, and Transportation Committee increased the maximum civil penalty for interference with aircraft safety from $1100 to $10,000 per incident almost a decade ago (Powelson, 1997). Passengers who are charged under federal law must fall into the definition contained in 14 CFR 91.11 which states, "no person may assault, threaten, intimidate, or interfere with a crew member in the performance of the crew member's duties aboard an aircraft being operated" (*FAA v. Hench*, No. CP97SO0004, 1998, 27 January 1998).

Civil Remedies

1. Warsaw Convention: Makes an airline liable for damages sustained if a passenger is wounded, suffers any other personal injury, or dies on board an aircraft (Article 17).
2. Death on the High Seas Act: Allows recovery by the personal representative of a decedent whose death was caused by the wrongful act, neglect, or default occurring on the high seas. Aircraft that crash into the sea fall into this category. It limits recovery to pecuniary losses and precludes recovery for predeath pain and suffering (46 USC 761-768 (1994).
3. Workman's Compensation: Depends on each state's applicable law.

An adequate means of appropriate redress currently does not exist. A better understanding of the causes of air rage and better legislation to protect the victim is needed. That victim could be either the passenger or the air crew member depending on the circumstances. International law is conflicting, and finding the proper jurisdiction to even hear the case is also a problem during international travel.

CONVENTIONAL WEAPONS

Terrorists have always been capable of acquiring manufactured weapons on the open market and also of improvised firearms requisitioned from professional arms dealers. Intelligence agencies and law enforcement agencies have been able to document that terrorists groups have come into possession of small arms, medium-size infantry weapons, and heavy infantry weapons.

Small arms weapons include those that are not belt fed. They are now mostly semiautomatic or self-reloading and were originally designed for military use. Considerable quantities of small arms are diverted to the black market each year. Manufacturers, including Beretta, Glock, and Kalishnikov, have failed to stem the flow of weapons, but not because they have not tried. The AK-47 is probably the most available automatic weapon for terrorists. During the Cold War, the Russians supplied the weapon to any and all left-wing insurgency organizations. The AK-47 has been replaced with the new AKM, which is available to anyone with the hard currency to buy it. Small arms continue to somehow make it aboard aircraft. In a GAO report published in February 2002 not long after 11 September, the investigators found the following:

- Investigators carried knives past screeners in more than 70 percent of tests.
- Screeners failed to spot guns in 30 percent of tests.
- Screeners failed to detect simulated explosive devices in 60 percent of tests.
- Overall, screeners failed to stop prohibited items in 48 percent of tests.

Investigators either secretly boarded an aircraft or gained access to the airport tarmac in 48 percent of tests. Similar findings have been made public in more recent tests (Internet: U.S. Government

Accountability Office, March 2005; and U.S. Government Accountability Office, May 2005). The classified version is U.S. Government Accountability Office, *Results of Transportation Security Administration's Covert Testing for Passenger and Checked Baggage Screening for September 2002 through September 2004*, GAO–05–437C. See also U.S. Department of Homeland Security, March 2005.

The problem is exacerbated by such weapons as the Glock and Sigma. However, in reality the Glock 17 and similar weapons are "made almost entirely of hardened plastic." The Glock still contain over a pound of steel (in the barrel, slide, magazine, and trigger mechanism) and is detectable both by metal detectors, due to the metallic content of the gun and any ammunition it might contain, and security x-ray machines, due to its clearly recognizable shape. Inside of exploring ways to upgrade security measures to deal with possible future technological threats such as nonmetallic firearms, Congress banned their production in the United States and required that all firearms sold and manufactured in the United States must meet an established detectability standard. The National Rifle Association helped draft the law, which was adopted, and fought to prevent the banning of detectable firearms containing plastic parts. The legislation, however, does nothing to prevent the eventual development of nonmetallic firearms in other countries, and the subsequent acquisition of such weapons by terrorists.

RPG-7's (rocket propelled grenades) were issued to the troops of the Warsaw Pact and in China and North Korea. They are easily manufactured and are a very functional weapon. They play an antivehicle antiarmor function when used against a stationary or moving target. They vary in quality but generally have a range of about 300 to 500 meters. They are easily available to the terrorist.

U.S.-made Stinger missiles have proliferated in the underground international arms market. A stinger is a manportable infrared-guided surface to air missile, capable of bringing down a commercial aircraft. It has an effective range of about 5500 meters. The United States generously supplied them to the "freedom fighters" during the Afghan war, and they are now available to terrorists, including Usama bin Laden. The Russians have sold sophisticated weapons and continue to sell such materiel. Thousands of SA-7 Grail missiles were sold that were equipped with optical sight and tracking systems. They have effective ranges up to 6125 meters and are designed to target aircraft.

EXPLOSIVES

Explosives are chemical compounds that undergo quick burning or decomposition with the generation of large amounts of gas and heat accompanied by the inevitable production of sudden pressure effects. Explosives do have many commercial applications and are therefore mass-produced for civilian purposes. The military, and unfortunately, terrorists and criminals also acquire the same materials for destructive purposes. Explosives are also used as propellants for projectiles and rockets and as bursting charges in bombs.

Gunpowder has been available since the 13th Century. Nitrocellulose and nitroglycerin were developed in the mid-19th Century. Since that time, nitrates, fulminates, and azides have been the ingredients most widely used, either alone or in combination with a fuel. Xenon trioxide became available in the early 1960s.

Such materials are categorized into two separate classes. Low grade explosives burn at rates of inches per second, and high explosives undergo detonation at rates of 1000 to 10,000 yards per second. In addition, some explosives are more or less susceptible to conditions of heat, cold, and humidity. The shattering effect, known as brisance, depends on the velocity of detonation. Explosives used as propellants in guns need to burn slowly because they are required to deliver a steady increasing push to the bullet rather than a sudden shock that would make the gun explode instead of ejecting the projectile. High explosives, such as dynamite are often mixed with inert materials to reduce sensitivity and therefore lower brisance.

Other explosives need to undergo detonation to explode. For example, trinitrotoluene (TNT) has a very high resistance to shock and can therefore be handled quite easily without fear of an

unintended detonation. Nitroglycerin, on the other hand, is so sensitive that it has to be mixed with something else to maintain stability for practical use. Technology has improved the quality and efficiency of newly developed explosives. Two developed during World War I include cyclonite and pentaerythritol tetranitrate. Cyclonite, or RDX, is often used as a detonator in bombs when mixed with TNT.

Since the 1950s several types of high explosives have replaced dynamite. A mixture of ammonium nitrate and fuel oil has proven quite effective. Unfortunately, it is extremely easy to acquire and produce a bomb. For detonating bombs, compounds are used that will themselves detonate under a shock or some heat to force the explosive of the main charge. For many years, mercury fulminate (Hg [ONC] 2) mixed with potassium chlorate was used. It takes some training and skill to use these materials, plus the combination cannot be stored in heat without some decomposition taking place. Today, diazodinitrophenol, lead azide (PbN6), and mannitol hexanitrate are most commonly used. These combinations have brisance and high explosive strength values.

Terrorists can buy explosive devices on the international black market, or they can improvise them fairly easily. All they need is a charge, a fuse, and a triggering device. They acquire the necessary materials by stealing them from military supplies or legitimate commercial users. They can make effective crude devices by purchasing the components at a hardware store. Terrorists are known to possess Semtex, cyclonite, C-4 plastic, TNT, dynamite, and, of course, common fertilizer. They have been known to assemble the materials into pipe bombs, Molotov cocktails, fertilizer truck bombs, and barometric bombs.

NUCLEAR AND BIOLOGICAL WEAPONS

To build a nuclear weapon, the manufacturer would need a critical mass of uranium or plutonium, or uranium oxide or plutonium oxide. As a substitute, it is possible that an oxide powder might be used. The process would require a highly trained technical team with specialized equipment. Fuel elements of any type would have to be subjected to chemical processing to separate the fissile material they may contain from the inert cladding material or other dilutents. Spent fuel from power reactors would contain some plutonium but at such low concentrations that it would have to be separated from other materials in the fuel. The fuel would contain enough radioactive fission fragments that the chemical separation process would have to be carried out by remote operation: a complicated undertaking.

Terrorists have three options; they can build a very crude nuclear weapon or sophisticated design similar to the nuclear weapons built by industrialized nations. Terrorists, however, do not care whether it looks pretty or whether it makes as large a crater as a hydrogen weapon. They only want it to explode or to have the authorities think that they have the ability to make one explode. The ancient Chinese used to say, “Kill one, scare 10,000.” In the case of a nuclear weapon, the concept of threaten one, scare a million is highly applicable. They could also lace a conventional weapon with radioactive materials creating a “dirty bomb.”

A crude design is one that deploys either a gun-type or the implosion-type device similar to those used on Japan during the World War II. In a gun-type device, a subcritical piece of fissile material is fired speedily into another subcritical piece such that the final assembly goes supercritical without a change in the density of the material. In an implosion-type device, a near-critical piece of fissile material is compressed by a converging shock wave resulting from the detonation of a surrounding layer of high explosive and becomes supercritical because of its increase in density.

The proliferation of nuclear weapons is fact. The disintegration of the Soviet Union and its subsequent inability to control its own stockpiles of weapons-grade nuclear material is also well established. Out of work nuclear physicists and technicians are also abundant. Their expertise is a valuable commodity to terrorists, and due to exorbitantly high unemployment in Russia, they are also available. Additionally, whether or not a security practitioner believes or does not believe a terrorist organization can build a nuclear weapon, experts cannot assure that the possibility does not exist. Consequently, the threat of use of such a weapon is sufficient to “scare a million.”

There are two basic categories of biologicals. First are microorganisms, which consist of living organic germs, like anthrax. The second includes toxins that are the by-product of living organisms such as botulism. The U.S. Biological Weapons Act of 1989 defines a biological agent as any "microorganism, virus, or infectious substance capable of (1) causing detrimental changes in the environment; (2) harming or damaging food, water, or equipment supplies; (3) causing disease in humans, animals, or plants or other living organisms." Nonetheless, all biologic agents need to be weaponized to be effectively used as a tool in a terrorist or hostile situation.

Even though biological incidents have taken place throughout history, technological advances of the 20th Century have changed the threat considerably. Previous uses were clumsy by comparison. Today, one incident could literally kill millions. Challenges to the potential perpetrator most singularly relate to the manufacturing process. Even the most virulent agent needs to be stabilized and made predictable. Therefore, the criminal actor is particularly vulnerable to discovery in this acquisition and preparation phase.

Regardless, in part due to a lack of resources targeting biologic threats, individuals and groups can now rather easily create a workable delivery device filled with a deadly agent free from detection. Many officials merely dismiss the idea as just too horrific to consider and fail to pursue it. The threat is clearly out there even though not well publicized, as evidenced by discoveries in France and Japan.

In 1984, French police raided a safe house of the German Red Army Faction terrorist group and located a bathtub containing flasks, which were filled with clostridium botulism, one of the most lethal substances known. More recently, Japanese police confirmed that Aum Shinrikyo had been stockpiling biologic agents. Adding to the seriousness of the situation, the current revolution in biotechnology may well produce other agents that could be even more toxic and resilient.

Even the acquisition of seed stock no longer poses a significant challenge. For example, some pathogenic organisms are simply endemic to specific geographic regions and are found in natural reservoirs. All that is required is a plane ticket and some basic knowledge of microbiology. In addition, agents can be bought from the American Type Culture Collection or the Microbiological Research Establishment in weakened form or from financially strapped Russian laboratories. It should be noted that controls in Western laboratories have been strengthened since the Iraqis bought their initial supply. Those control improvements, however, do not change the fact that almost anything is probably available on the Russian black market.

On a scary note, future genetic research may be able to pinpoint the genetic characteristics of both the target population and the potential agent. In other words, the agent would target specific individuals genetically. This could lead to an "ethnic" agent. The ramifications of this are almost unspeakable in the hands of a terrorist group or a deranged individual.

The problem is further intensified by the fact that these agents are *almost* impossible to detect. The same production facilities can produce toxic agents in something as legitimate as dried milk. In addition, the technology to detect a biological agent in transit is not readily available. The inability to detect the agents is only worsened by the fact that once located and identified; medical prophylactic measures have proven to be inadequate. Furthermore, considering the fact that security managers are already fighting tooth and nail for their part of budgetary resources, personal protection equipment has not been considered to be essential additions to private security equipment supplies.

Realistically, it is both expensive and impractical to vaccinate personnel against all agents, equip personnel with individual protection suits, or even to have decontamination kits, respirators, and other response tools. Even if victims are provided with emergency medical care and later hospitalization, it is unclear whether these agencies are up to the task. Clearly, the technical community needs to expend considerably more effort to develop effective detection equipment to work as well as metal detectors.

Some efforts have been made. For example, the *New Scientist* revealed in 1998 that Washington's Naval Research team had tested a plane weighing 42 lbs. that is capable of detecting minute quanti-

ties of biological agents. The planes were designed to fly into suspected contaminated areas and detect up to four separate bacterial agents.

> An onboard sampling chamber has been designed to allow air to pass through and thus create a vortex in a pool of water. Every five minutes the water in the chamber washes over a sensor composed of four optical fibers. The optical fibers have a probe affixed to the core of each fiber. Each of the probes is coated with an antibody for a particular bacterium, allowing for the adhesion in water if present of the spore of the particular bacterium to the probe.

At a minimum, security managers should review all procedures with biologicals in mind. For example:

- Get outside help! The effectiveness of appropriate liaison with authorities such as Federal Emergency Management Agency, the Department of Defense, the Federal Bureau of Investigation, and the Centers for Disease Control is crucial (CDC [404-639-1293]).
- In the event of an incident, as much as possible control and contain any further release of any suspected biologicals. Determine the actual nature and extent of the threat.
- Evacuate personnel to a safe distance. Ascertain the actual identity of the agent. Both a primary and secondary secured perimeter must be established.
- Always control physical security and access to your premises. Periodically review security procedures for detecting and reporting suspicious delivery of devices or packages.
- Emphasize employee training in response to specific telephone threats: Always attempt to determine the type of biologic agent, location, dispersal mechanism, etc. Review decontamination procedures.
- Staff awareness to this type of threat needs to be regularly reinforced.
- Determine whether appropriate procedures for a terrorist-type attack include a search plan, an evacuation strategy, a postincident recovery plan, and a crisis communication strategy.
- Reevaluate the effectiveness of surveillance systems in deterring, detecting, and documenting suspicious activity as simple as placing a "bug bomb" in a room.
- Be prepared to make a complete after-action report.

Furthermore, it will be important not to overlook the psychological reaction of the public to such an incident. They will certainly react to feelings of being unprotected and helpless. Those reactions could present issues of crowd control, rioting, or outright opportunistic crimes. Consequently, a close working relationship between public affairs officers and the media must be developed. Security managers must have preplanned how they will deal with a panic mentality on the part of the public and maybe even their own employees. Senior managers must keep local, state, and federal officials informed and seek early intervention by experts and government authorities.

If both private and public security officials take a biologic threat seriously, a major effort will be needed to develop contingency plans and initiate coordinated and mutually supportive programs across a broad spectrum of agencies. Currently, major health professional organizations are a long way from providing adequate training and education to their own health care community, let alone the rest of the population. Adequate diagnostic and identification will require a major push. Public health, intelligence, and law enforcement agencies as well as the private sector should recognize the threat for what it is — a national priority considering the potential consequences.

EMBRACING RISK MANAGEMENT

Risk management should effectively reduce the consequences of a crisis. The overall purpose of risk management is to create a secure environment, yet permit the company to remain consistent with normal operations and company philosophy. In other words, risk managers should consider not only

potential vulnerabilities and countermasures, but also how they relate to profits and the aesthetic and operational needs of the company. A risk is a known threat that has effects that are predictable in either timing or extent. Pure risk is usually defined as the potential for injury, damage, or loss with no possible benefits. Dynamic risk, on the other hand, has the potential for both benefits and losses. A systematic approach to preventing loss will involve risk analysis, appropriate policy, countermeasures, and follow-up. The most important factor in preparing any response plan is to consider vulnerability, probability, and criticality of all assets, including the most valuable resource: human life. Airport managers therefore need to develop a logical, systematic approach to deal with recognized threats to aviation.

ASSESSING THE THREAT

The new generation of risk management professionals tasked with managing risk and security will need to embrace the world as it is, and not as it once was. The value of intelligence will continue to increase as security professionals struggle to maintain an awareness of their areas of responsibility. As the steady hum of globalization continues on, world events become increasingly more difficult to track and predict as they unfold. Further making matters worse, the underlying causes for global trends and issues are increasingly difficult for security professionals to discern. There are two general reasons for this. One, events that can potentially have an adverse affect on an organization increase every day as globalization continues to add to the connectivity of global society. In other words, events across the globe that may not have affected an organization yesterday will continue to creep ever closer as time goes on. It is not uncommon for the logistical chains of American companies to literally stretch around the globe, and it needs to be recognized that events abroad, no matter how far away, can send ripples up these chains all the way back home. Foreign markets are also becoming more accessible, and today's risk managers will not only need to develop awareness of their own neighborhoods, but also potential environments in which to expand as well.

A second more concerning reason is that as events continue to increase in frequency and complexity, mainstream media outlets will have little choice but to tone down the quality of reporting to accommodate the largest audience possible. Mainstream media is becoming increasingly incapable of delivering quality reporting. In other words, the security community is only a very small part of the overall audience mainstream media outlets target. Unfortunately for security professionals, the watering down of mainstream media reporting will only make their work more difficult as much of this reporting will target a more general audience potentially resulting in a misleading, or an inaccurate, portrayal of events. As this trend continues, security professionals will be increasingly forced to seek out alternative sources for information.

Current and future generations of security professionals in the United States will find that global events continue to influence the day-to-day business of managing risk, while their ability to interpret and assess the significance of these events declines. However, globalization itself is also placing greater demands on security professionals as specific areas of responsibility become increasingly larger and more complicated. Today, demands on security professionals are being stretched to encompass responsibilities that span large geographical areas such as logistics, foreign market evaluation, overseas employee management, and stakeholder perception. Additionally, modern and future security professionals must still concern themselves from hostile adversaries, as well as environmental threats. With such varied responsibilities, it is difficult to imagine security professionals fulfilling information requirements independently. Not only would maintaining full-blown information gathering and analysis capabilities "in house" be exceptionally challenging, it would also be very expensive. A more practical alternative is for an organization to maintain a robust security capability to manage risk, while allowing its security professionals to seek outside help. In doing so, an organization plays the role of a customer with requirements for information, analysis, and assessments. As a customer the most economical solution to meet these demands is to combine all

these requirements in the form of intelligence as needed. Today, there are three primary directions for an organization to reach for informed intelligence shopping.

Law Enforcement

Local law enforcement remains an obvious supplier of intelligence for any organization regardless of size. Police have the ability to gather information that no one else can, and their knowledge of respective localities is unmatched. These two realities make local law enforcement a primary player in the world of intelligence. However, intelligence acquired from local law enforcement has its pros and cons. To begin with, whereas local law enforcement has exceptional reach in its ability to acquire information, it does not necessarily always have the resources to do so. The overall responsibilities of local law enforcement extend far beyond intelligence, and resources are always limited. Perhaps more importantly, this limitation in resources can make it difficult for organizations to collaborate with local law enforcement. Building relationships is a long and time-intensive process. The priorities of local law enforcement will pull capabilities away from an organization by default, making collaboration an unnatural endeavor for the two parties.

Further complicating matters, the intelligence activities of local law enforcement are driven by investigations and prosecutions, not the requirements of outside organizations (Carter, 2004). This reality makes it difficult for organizations to fulfill intelligence requirements by reaching out to local law enforcement because the acquisition and analysis is not tailored to the organization's needs. However, in the case of an investigation that obviously concerns an organization, it is not uncommon to integrate a member of that organization's security into the investigative process. In this rare exception, both parties' interests are aligned. This scenario provides some insight into the value of building an ongoing relationship with local law enforcement.

Federal Resources

Much like local law enforcement, the key to reaching out to federal intelligence resources is in relationship building. A federal level intelligence agency's interests will lie within the realm of national security, or at a minimum in accordance with the directives of a parent department. While this is good for all U.S. organizations with security concerns as a whole, it does not do much for them individually. On the other hand, federal intelligence resources are accessible in a way that local intelligence generally is not because of jurisdictional issues. While an individual organization may find it impractical to approach federal intelligence groups on their own, it is effective to engage them on an industry basis (Masse, 2005). For example, a chemical company might not be able to build a relationship with the FBI because their interests are too unaligned, but when combined with every other chemical company in the United States, it could participate in a more generally based relationship. By acting as part of an industry, a single organization can benefit from industrywide and specific intelligence from the federal level. The key to successfully tapping into this resource is typically the positioning of a special advisor, or agent, within the federal intelligence group (Masse, 2005).

Private Intelligence Services

A third option for organizations seeking intelligence is a growing number of private intelligence services. Private intelligence services gather information much like mainstream media outlets do, primarily focusing on open sources, and produce a product similar to the open source intelligence (OSINT) resources associated with federal intelligence groups. They, in turn, analyze gathered information for the benefit of clients in exchange for a fee. Unlike local law enforcement, or federal resources, private providers have the capability of custom-tailoring intelligence to an organizations' needs. Perhaps more importantly, the potential for relationship building with regard to private intelligence services is far greater than with a public sector entity. This opens up the possibility of

pursuing any type of information that may be desired by an organization's security professionals. Desired products and services could include intelligence briefings, market analysis, or even executive protection. This is possible because the question of aligned interests never needs to be asked because both parties must actively engage one another to achieve their respective ends. In the case of the private intelligence provider, the objective is to obtain a fee for their services, thus they will work very diligently at providing a superior product. There is also a benefit in having private intelligence providers compete with another in that there are many products on the market for organizations to choose.

Stratfor Strategic Forecasting, Inc.

The Austin-based group, Stratfor Strategic Forecasting, is a private intelligence service widely regarded by its impressive list of international corporate clients as a "shadow CIA." Its founder and Chief Executive Officer, Dr. George Friedman, founded the company in 1996 and currently guides the company's overall long-term geopolitical forecasting, in addition to tactical intelligence operations (Internet: stratfor.com). While the average user can obtain briefings through the company's website, Stratfor also provides a host of other services including threat assessments, executive travel security reports, specific situation monitoring, and even on-call consultations. For its upper tier corporate clients, Stratfor also specializes in personalized briefings that can cost upwards of 10,000 dollars per presentation, whereas some clients opt for continuous consulting services that can reach over $20,000 per month.(Leineweber, 2001.)

Stratfor's services have a great deal of value to a risk manager because they do not simply filter or report open-source information. Instead, they gather information from a network of sources with diverse backgrounds ranging from retired military members to former three letter agency analysts, or partnered in-country sources. Information, gathered from "the ground up" as it were, is analyzed state-side, resulting in actionable intelligence that can be custom-tailored to industries as a whole, the average subscribed user, or individual corporate clients. This concept of developing an "actionable product" has been the key to Stratfor's success. Stratfor clients receive highly refined intelligence products that are a combination of high-quality reporting and analysis. The aim of these products is not to merely filter mass media, or discover trends, but to decipher the underlying meaning of world events to Stratfor's constituents.

Jane's Information Group

Jane's history is rooted in the defense industry when its founder, Fred T. Jane, began publishing sketches of warships more than a hundred years ago. Later, Jane became a naval author, journalist, and was even associated with the founding of the United Kingdom's domestic intelligence service MI5 (janes.com). Fast forwarding to the 1990s, Jane's began offering private intelligence and consulting services to clients that could be custom tailored to fit individual needs. Although the defense industry continues to be their specialty, today Jane also specializes in market forecasting, public safety, public transportation, and law enforcement.

What makes Jane's products different from that of other private intelligence service providers is the use of "electronic platforms." An example of such a platform would be Jane's Terrorism and Insurgency Center (JTIC) launched in 2003 (janes.com) Through this center, which is not really so much a physical center but rather a virtual one, users can access information in a variety of forms. Much like other providers, Jane's members can access intelligence briefings; however, they are focused with respect to the platform's subject area. In the case of the JTIC platform, user access will be directed toward global developments in terrorism exclusively. Jane's employment of electronic platforms has a significant advantage for many of its users in that they serve as a searchable database for clients who are interested in specific information. Clients can also establish a customizable "alert" system informing them via email of events or briefings of special relevance.

Economist Intelligence Unit

Founded in 1946 as a spinoff to *The Economist* newspaper, the Economist Intelligence Unit (EIU) has grown into a private advisory firm with 40 offices worldwide covering one 185 countries (eiu.com). Unlike other intelligence providers, EIU has a special emphasis on country analysis from a business perspective, or what it sometimes calls "markets in motion." The underlying notion is that markets are driven by a variety of factors including locality, culture, history, geography, politics, and a virtually limitless number of other issues. Intelligence, they would argue, is the key to successful investments abroad, making them an attractive option for American corporations looking to invest in unpredictable overseas markets.

Another interesting aspect of the EIU is there range of services. Whereas Stratfor tends to focus on security, and Jane on the defense industry, the EIU aims at getting involved in the decision-making process of its clients. The EIU is particularly adept at advising in overseas investments and prefers to partake in even the early stages of corporate strategizing. The EIU refers to this full scope advising as "360 decision-making" support (eiu.com).

Despite the fact that they may fall short of one-stop shopping, private intelligence services offer organizations a unique option for acquiring intelligence. Unlike other options, products produced by private intelligence providers will be custom tailored to the needs of an organization. Perhaps their greatest advantage lies in their ability to operate in near real time, which can arm an organization with foresight, something they may have difficulty in developing on their own.

The modern-day demands of globalization require organizations to bear heavier burdens of security for the benefit of stakeholders. Intelligence, it would seem, is one tool in particular that provides a great deal of utility, or value, in relation to other alternatives. The ability, or inability, to acquire intelligence as a tool in security presents the modern organization with an interesting dichotomy. On one hand, an organization can continue to rely on other institutions for security, such as mainstream media, local law enforcement, or federal intelligence groups. In reality most organizations benefit from these institutions every day whether they are aware of it or not. On the other hand, an organization can embrace intelligence as a core component of its security, whether it be by developing internal capabilities, building relationships, or by reaching outward to a private provider. How it achieves this is up to the organization itself, but many indicators point toward a future where private intelligence services will continue to meet more of this demand. The difference between the organization that does not embrace intelligence and the one that does is quality of security. An organization that does not embrace intelligence in a proactive manner will entrench itself in a continuous state of complacency. In other words, adverse events in the world will come as surprises more often they should, and the organization will be forced to spend more time and resources "reacting," as opposed to mitigating. By relying on systems and institutions outside of its control, organizations that do not embrace intelligence are practicing risk avoidance, not management (Gurley, 2004). Security professionals and organizations that will excel in today's globalized world will be those that embrace risk management as a continuous element of security. The advantage of this is that it is in an organization's interest to reduce its risks and also to identify opportunities before they arise. Integrating intelligence into an organization's security management process is a precursor to both of these objectives.

FLIGHT CREW INVOLVEMENT

Regardless of the refinement of any crisis management plan, the ultimate test of aviation security occurs on the ground, on the tarmac, and in the cockpit. Therefore it is critical that the flight crew be included in all aspects of security planning and implementation. Crew members can more easily assess whether proposed security measures will be effective, and their involvement needs to extend beyond the technical aspects of aircraft operation. Crew training in matters of security should always include integration with the intelligence function. To exercise the "need to know"

argument simply keeps the crew in the dark unnecesssarily. They must be provided with sufficient information to prevent, deter, or manage a security incident.

In addition, due to the nature and complexity of issues associated with corporate aviation programs, it is recommended that a security committee meet regularly. Representatives to the committee should be able to contribute to the expertise needed to advise on security measures and procedures that will best result in adequate security. At a minimum the committee should do the following:

- Review inspections and security surveys of frequently used airports
- Review and document the security training of all crew members
- Institute measures to enhance security awareness among all employees
- Review intelligence data on the security of all overseas airports utilized
- Establish and consistently update company security policies and widely disseminate them
- Create and maintain liaisons with appropriate law enforcement and intelligence services

In that the threat environment is constantly changing, effective crisis management must be preventive and not reactive in nature. It presents quite a challenge, and if outside help is needed it should be acquired. Proactive measures will reduce the likelihood of an incident and potentially save the company huge sums of money in the long term.

CONCLUSION

Airborne criminal activity nonrelated to terrorism is a growing problem. It is not limited to alcohol-related incidents but includes aspects of air rage and the involvement of other passengers in the fray. Unfortunately, all security assistance available is locked into the plane with the air crew and passengers. Crews need to be trained to handle these situations, and ground security needs to be immediately available to take over control of the incidents. Additionally, local security and local law enforcement must acquire concurrent jurisdiction along with federal authorities.

It is undisputed that many modern terrorist organizations are extremely well financed. They can afford a nuclear weapon, and they can also afford the components of a poor man's weapon of mass destruction, both biological and chemical. One of the primary goals of the terrorist is fear. Terrorists hope the public will panic if nuclear, biological or chemical (NBC) weapons are deployed against commercial air carrier passengers. The second goal of the terrorist is publicity. The media would be drawn to an actual or threatened NBC attack in droves, assuming they felt they could protect themselves from the danger. Some security experts would argue that terrorists would not use these methods for fear that they could not protect their members or control the outcome. However, this type of analysis reflects the fears of the security practitioner rather than any fears of the terrorist. Fanatical terrorists are not necessarily concerned with a rational approach. This is why the study of terrorism, the terrorists themselves, and the causes behind the terrorism are so important.

In addition, the creation, implementation, and testing of security plans will continue to drive security measures within general aviation and corporate aviation programs. The developing and conducting of exercises or simulations can range from simple command-post exercises to full-blown realistic incident training. In the final analysis, however, it is up to the security practitioner to identify and effectively handle the security-related problems that all aviation industry workers confront on a regular basis. Special problems can seriously inconvenience the crew, the customer, the company, and the public and must be anticipated and appropriately handled. This sequence of events is easier said then done, considering today's threats and the costs of efficiently responding to them.

REFERENCES

Alonso-Zaldivar, Ricardo, "LAX Leads US in Close Incursions," *The Los Angeles Times*, 2000, pp. 1, 3.
Carroll, Charles R., "The Dilemma of De-toxing the Work Force," *Security Management*, May 1992, pg. 54.

Carson, Mark, Theodore Taylor, Eugene Eyster, William Maraman, Jacob Wechsler, Can Terrorists Build Nuclear Weapons, http://www.nci.org/k-m/makeab.htm, pg. 1–13, 10 August 2001.

Carter, D.L., November 2004. Law enforcement intelligence: a guide for state, local, and tribal law enforcement agencies. *Federation of American Scientists.Internet:* http://www.fas.org/irp/agency/ doj/lei/chap1.pdf. Accessed on November 16, 2007.

DOT Amends Drug and Alcohol Rules, *AIN Weekly*, 20 July 2001, pg. 4.

Gurley, D.M. The Limits of Intelligence: Iraq's Lessons, *Survival 46:3*, 7–28 Autumn 2004.

Hatcher, Thurston, CNN.com, 6 July 2001, pg. 1.

http://www.alpa.org/internet/tm/tm061198.htm, 22 April 01, pg. 1.

http://www.faa.gov/apa/pr/pr.cfm?id=1354.

http://www.faa.gov/aso/RunwaySafety/runway_incursions.htm.

U.S. Government Accountability Office, *Aviation Security: Screener Training and Performance Measurement Strengthened, But More Work Remains*, GAO–05–457, May 2005, at *http://www.gao.gov/new.items/d05457.pdf* (July 17, 2006).

U.S. Government Accountability Office, *Aviation Security: Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems*, GAO–05–365, March 2005 at *http://www.gao.gov/new.items/d05365.pdf* (July 17, 2006).

Leineweber, J. (October 12, 2001) Stratfor private intelligence service gaining momentum. *The Daily Texan.*

Levin, Alan, "Runway Incidents Called Top Hazard," *USA Today*, 16 May 2001, pg. 4A.

Masse, T.M., 24 March 2005. The national counterterrorism center: Implementation challenges and issues for congress. *Federation of American Scientists.* http://www.fas.org/sgp/crs/intel/RL32816.pdf. Accessed November 16, 2007.

New Technology Targets Runway Safety," *USA Today*, 30 May 2001, pg. 7a.

Normani, Asra K., "Airlines Tell Boozers To Put a Cork In It," *Wall Street Journal*, 28 August 1998, pg. W1.

Powelson, Richard, "Bill Boosts Civil Penalty for Unruly Air Travelers," *The Times Union*, Albany, NY, 12 February 1997, A7.

U.S. Department of Homeland Security, Office of Inspector General, *Follow-Up Audit of Passenger and Baggage Screening Procedures at Domestic Airports (Unclassified Summary)*,OIG–05–16, March 2005, at *http://www.dhs.gov/interweb/assetlibrary/OIG_05-16_Mar05.pdf* (July 19, 2006).

U.S. Government Accountability Office, *Results of Transportation Security Administration's Covert Testing for Passenger and Checked Baggage Screening for September 2002 through September 2004*, GAO–05–437C.

World Tribune, 17 May 2001, http://www.worldtribune.com/worldtribune/Archive-2001/ss-terror-05-17.html, 10 August 2001.

15 Access Controls, Perimeter Security
Another Foundation

NEWS

April 1999: A Transportation Department report notes that investigators deliberately set off 25 emergency exit alarms. Security personnel never responded to 10 of them.

18 January 2000: A driver, who had lost his way at the Auckland International Airport, is arrested and charged with illegal entry into restricted airport zone, driving on the runway, and assaulting a police officer.

July 2002: The U.S. government issues a warning to airlines to be on the alert for people in stolen uniforms after numerous reports of stolen air crew and airline employee uniforms are received.

May 2003: Boston's Logan Airport begins using thermal imaging intrusion detection equipment to monitor a state-mandated 250-foot arrest zone and a 500-foot security zone around the perimeter. Algorithms built into the software identify abnormal movements or objects, which are then displayed graphically on a standard PC running Microsoft Corp.'s Windows operating system, alerting airport personnel of potential security violations.

7 December 2005: An American Airlines 757 arrives from Medellin, Colombia, and is on a roughly two-hour stopover in Miami before continuing to Orlando. It is alleged that one of the passengers, a 44-year old U.S. citizen, claims to have a bomb in his carry-on luggage. Air marshals confront the man on the jetway and shoot him after he appears to reach into his bag. The man dies sometime later as a result of his wounds. No explosive is found in the bag. This is the first time since 11 September that air marshals have fired a weapon on or near an aircraft.

Today: Communication is crucial to good security. The common phrase "out of sight, out of Mind" loosely translates into Russian as "Invisible Idiot."

INTRODUCTION

Sometimes the most basic measures can prevent real tragedy from happening. However, sometimes the most basic measures are often overlooked or under utilized. Basic physical security equipment consists of three items: locks, lights, and alarms. The three basic lines of physical defense at an airport are the following:

- Perimeter (fence around the airport)
- Buildings (the terminal and collateral buildings, both interior and exterior, including the runways, taxiways, and their surrounds)
- Aircraft (the airplane and jet way)

The degree of security required will determine exactly just how sophisticated these three options and areas need to be. For example, at airports, access to the sterile concourse is not controlled only at the security checkpoint. Access to jetways, restricted areas, and the airport itself require some consideration. When considering interior security, the airport security professional must address not only sterile concourses, but also doors, windows, ducts, and any other openings large enough for someone to go through. The initial step in any risk assessment program is to determine where the airport is most vulnerable and assess the likelihood that its security will be breached at that point. Each area identified as a problem area requires an appropriate degree of attention, depending on its criticality and vulnerability. Access control is always a primary issue.

ACCESS CONTROL

The Office of the Inspector General for the Federal Avation Authority (FAA) issued a report on Airport Access Control in November 1999. They identified several vulnerabilities but generally confirmed that there were four general reasons for concern (Report NumberAV-2000-017). The agency identified:

1. Airport operators and air carriers not successfully implementing procedures for control
2. Employees not meeting their responsibilities for airport security
3. FAA not successfully implementing its oversight program for ensuring compliance with programs
4. FAA policies that contribute to weaknesses in access control

In the past, the primary means of gaining access to a controlled area was to merely be wearing whatever was considered to be the ramp uniform. Clearly, apparel and uniforms can no longer be safely accepted as an appropriate means of identification. The uniforms of airline personnel, flight operations, and security personnel are too easy to duplicate. Additionally, in May 2002, the Federal Bureau of Investigation (FBI) reported that a truck containing airport worker uniforms was stolen from a Kansas City, MO uniform company. The truck was recovered but the uniforms, from Delta, Midwest, and Vanguard Airlines, were not. You can even buy a duplicate copy of airport security sleeve patches in some airport gift shops. Technology has advanced to the point that badges have become the next level of standard security practice.

The government obligates (FAR 107.14; TSA 49 CFR Chapter XII, Part 1540) that airport access control systems must:

- Enable only those persons authorized to have access to secured areas to obtain that access
- Immediately deny access at the access point to individuals whose access authority has changed
- Have the capability of zone coding, so that it can admit or deny access by area
- Have the capability of time coding, being able to admit or deny access by time and date

Locks

Locks are probably the most commonly used means of controlling access to an area (the airport); a building (the terminal, control tower, or hangars), a room (package area), or a container (an aircraft). Locks are one of the oldest means of security in use: the Egyptians used them more than 4000 years ago. Variations on the general theme, however, have been expanded. A proficient thief or terrorist will boast that any lock can be opened. However, locks are still very valuable in that they increase the time an intruder needs to actually gain access. That time can be used to increase the probability of being detected. Locks include those that are key operated, combination-type, card-activated, and electronically operated.

The concept of using a key is simple and efficient but will not likely protect assets very well. First of all, keys can be easily duplicated. Unless a closed circuit television (CCTV) system monitors every door or access point, a key will also not enable security to document who and when an individual enters. It also becomes a bit expensive to change all the keys when an employee is terminated or quits or retires and to administratively track the keys. Keypads with access codes have some of the same problems. Even doors with codes require downtime when replacing old codes and having employees memorize the new codes.

Card-operated locks make use of a card reader installed near a door or restricted passageway. When an appropriately authorized card is inserted, a minicomputer unlocks the access. More sophisticated card-operated locks record the time a lock was opened and who opened it. These types of locks are very useful in areas that are restricted to the general public but must still be made accessible to large numbers of employees or workers. In 1000 BC, the Chinese required servants at the Imperial Palace to wear rings engraved with unique intricate designs identifying palace areas they were permitted to enter. Historians credit this method by the Chinese as the first comprehensive access control system (Naudts, 1987169). Advancement in science and technology has improved on the Chinese system. Some systems can be programmed to lock and unlock access points at specific times and on specific days.

Access Cards

Wiegand, magnetic strip, and proximity cards previously dominated the market. Today, optical memory cards and smart card technology is the way of the future in the field of access cards. They possess one or more integrated circuit chips capable of storing a great deal of information and interpreting it. Military identification cards now use similar technology to encode someone's entire medical history onto the card. Weigand cards have metallic rods or wires embedded inside the card. Named after their inventor, the cards have the data encoded in the embedded wire, which has been twisted under tension and heat tempered. The manufacturing process gives the treated wires unique magnetic properties. The cards are difficult to duplicate and are also resistant to moisture and temperature. Radio frequency interference or external magnetic fields do not affect these cards (Protective Technologies International, Inc. Access Control System, 2001).

Magnetic strip cards use a strip similar to those on credit cards. A magnetic strip is affixed directly onto the surface of the card, and the data is recorded magnetically just like tape recording. These cards can be encoded on site but are also subject to being easily copied and or modified and are easily damaged when placed near magnetic media. Watermark cards also use a magnetic strip but have a permanently encoded number that cannot be altered. Barium ferrite cards or magnetic sandwich cards contain information encoded in soft pliable magnetic materials positioned between layers of plastic. Rows and columns of spots on the magnetic sheet are magnetized to create a code that is read by magnetic sensing heads. Infrared cards use a pattern of shadows inside the card and a low-level infrared light in the reader to detect the pattern and determine if entry should be granted.

Smart cards have embedded computer chips in them that consist of either a microprocessor with internal memory or a memory chip with nonprogrammed logic. Two general categories of cards exist. One is a contact card, requiring direct physical contact to a conductive micromodule on the card. The other type is a contactless card, which requires only close proximity to a device designed to read the card. Original research on the card was done in both Europe and Japan where the first patents were filed. Advances in technology in the 1980s enabled the card to transmit commands, data, and other information. The micromodule is actually embedded into the plastic substrate of a credit card-looking piece of plastic. Glue is used to affix the micromodule to the card (Smart Card Overview, http://www.scia.org/knowlefgebase/aboutSmart Cards/primer.htm. pp 1-5).

Proximity cards are either active or passive. "The active technology card has an embedded lithium battery and transmits a signal; a passive card has no battery and relies on the strength of the receiver's signal to retransmit the encoded number" (Bordes, 1994). They are very difficult to

duplicate and correspondingly rather expensive. The system uses a radio receiver plus transmitter implants. The reader, usually mounted on the wall, transmits a low-frequency radio signal. The card receives the data and interprets it sometimes from as much as a couple of feet away. Some manufacturers claim the card does not even need to be removed from a wallet to be used. Because proximity cards use radio frequency signals, personal identification numbers (PINS) or frequencies are also a means to gain access in some sophisticated systems.

None of these cards provide effective security in the wrong hands. The card does not know who is holding it, and the machine reading the signal or data does not know either. An access card can simply not identify a specific individual using the card. It is only wishful thinking to assume that every time a card is used that the person using it is actually the person authorized to use it. As frequently occurs, piggy backing is also a problem. One person opens the door or access point, and several people follow them through. Another issue arises when terminated employees fail to turn in their security badges. One company, TEMTEC, has overcome this problem with identification badges that expire. The *VOIDbadge*™ from TEMTEC of Suffern, New York, is a plastic badge printed with the word void that becomes valid when a two-part authorization sticker automatically expires by turning red. Currently the technology is only being used on photo identification cards, but it forecasts a future concept (Marketplace, 2001, pg. 142).

Electronic Locks

Electronic locks are also an option at smaller airports without a 24-hour access requirement. It is important to recognize that there are two kinds. A failsafe lock will remain unlocked when the power is off. Such locks are usually used on doors in the path of a fire exit, and a fail secure lock remains locked when the power is removed. Historically, the most common form of protection from an intruder penetrating these interior systems was "magnetic contacts." They were placed in a position so that if a door or access point was opened without the proper authority, a signal was sent to a control panel and an alarm activated. Today's locks hold forces that even range from 650 to 1500 pounds and can be controlled and monitored individually, sequentially, or simultaneously from one or multiple locations.

Sensors

If a glass door or window is breached, glass-breaking sensors can detect either the acoustic or the seismic breaking of the glass and also send a signal. Newer microprocessor-based glass-break pattern analysis ensures detection reliability and prevents false alarms. Rokonet Electronics Ltd., based in Israel, manufactures a product containing audio discriminators that sample the environment 40,000 times per second, and the microphone analyzes a combination of low and high frequencies against 30 specific sound patterns (Marketplace, 2001, pg. 141). Infrared and temperature alarms have also become more popular. A ceiling mounted detector works on the same principle as a smoke detector. They both can cover a 360-degree field of review. Wall units have a field of vision of 180 degrees but are usually equipped with a longer range. Corner placement is sometimes the best, but each room must be evaluated individually.

Biometric Security Systems

Biometric security systems have been hailed as a major advance in access control. The newest systems can accurately verify an individual's identity through fingerprint scans, hand geometry, iris scan, retinal scan, voice patterns, and facial scan. A biometric system needs three functioning components including (1) enrollment of the individual into the system providing baseline information, (2) entry into the biometric device by the person seeking access, and (3) acceptance or rejection by the device, based on technical comparison with the enrolled data.

Retinal Scans

Retinal scans are actually one of the oldest and most accurate biometrics. Researchers in the early 1930s discovered that patterns of blood vessels on the back of the eye are unique to each individual. *EyeDentify*™ is the primary manufacturer of the devices. They are expensive, and the public has generally not accepted its use.

Fingerprint Verification Readers

Fingerprint readers read an encrypted template in a smart card or a biopatch. Systems are either semiconductor chip-based or optical. Optical prisms resist distortions caused by dirt, oil, or moisture buildup. Semiconductor systems are susceptible to damage from electrostatic energy, especially near carpets. At least one manufacturer claims the false rejection rate is 0.1 percent and the false acceptance rate is 0.001 percent.

Voiceprint Identification

The method can be defined as a combination of aural and spectrograph comparison of one or more identifiable voices with an unknown voice for the purpose of identification. The first factor in determining voice uniqueness lies in the vocal cavities and vocal cords. The second factor depends on use of speech articulator use patterns. The system is widely used within the criminal justice system but has so far not been extensively used in an airport environment.

Hand Geometry

This system uses the geometric shape of the hand for authenticating a user's identity. However, individual hand features are not descriptive enough for accurate identification. It takes a three dimension of 90 different points on your hand. The measurement is turned into a unique algorithm and stored in the reader. At San Francisco International Airport more than 30,000 employees are enrolled in Recognition Systems Inc.'s Handreader™, which controls access to over 180 doors.

Iris Scans use video cameras to scan the iris, the colored ring that surrounds the pupil in the human eye. The system translates the 266 independent characteristics of the iris into a 512-byte digital code. A 30-frame-per-second, black-and-white video camera is used to take a picture of the eye from 6 to 36 inches away. EyeTicket Corp. in McLean, VA, begun initially to register passengers at Charlotte Douglas International Airport in North Carolina and Frankfurt Airport in Germany. Others have adopted similar systems since. The scans can confirm a person's identity in less than 30 seconds.

Facial Scans

Facial scans require the use of a digital camera to develop a facial image of the end-user for authentication purposes. Eye scans are similar to facial scans. Face recognition is a complex process and has proven to be somewhat unreliable. Detection is the process of locating a human face in an image and isolating it from other objects in the frame. After the face is isolated, then the process of recognition begins that compares the face being captured with a database of faces to locate a potential match. During detection, the hardware and software combination isolates the facial elements of an image and eliminates extraneous information. The software examines the image for typical facial structures (such as eyes and nose), and once it has found them, it calculates the remainder of the face. It then cuts away background details, leaving a closeup of a face inside a rectangular frame.

SIGNS

Areas identified as those needing to be restricted, especially air operations areas, should be so designated. A sign should make even the casual observer aware that a specific area is restricted to authorized personnel only. They must be large enough and sufficiently eye-catching to alert the

most absent-minded traveler. Furthermore, international airport officials must be acutely aware that not everyone speaks English. Many airports absolutely require that critical information be communicated in several languages. Such signs will obviously not deter the determined terrorist. However, those travelers accidentally straying near an area can be deterred. Signs should be posted at intervals of no more than 100 feet.

Signs are also extremely important on the flight line. It is a busy and constantly moving area. Signs are crucial for the safe flow of traffic. Both aircraft and servicing vehicles must know where they are at and where they are going. Due to the noise, signs are an important means of communication. Security personnel also should always be trained in understanding the hand signals used on the flight line. Signs at the entrance to the field and along any perimeter road or access road are also important. Inadvertent access to the flight line needs to be minimized. Although seemingly incredible, it is always possible that a wayward traveler may seek to drive directly to the plane or somehow drive across the flight line. In most jurisdictions, trespassing prosecutions require that a sign has been posted, legibly and in clear view of the public.

PERIMETER FENCING AND LIGHTING

Some airports have huge areas to monitor, covering acres and acres of land. Monitoring these perimeters can prove to be extensively manpower-intensive and cost-intensive, depending on the equipment used to patrol the circumference of an airport. Perimeter barriers, according to the National Crime Prevention Institute (NCPI) are "any obstacle which defines the physical limits of a controlled area and impedes or restricts entry into the area. It is the first line of defense against intrusion… At a minimum a good perimeter barrier should discourage an impulsive attacker" (National Crime Prevention Institute, 1986). Fencing will deter the wanderer, but again the determined terrorist will easily breach the fence. However, terrorists can be slowed down, and the fence can give security the benefit of time and distance to reach the intruder if detected soon enough. The general purpose of the fence is to define the airport's perimeter and to channel passengers and employees to authorized gates.

The fence itself needs to be sufficiently high. Chain-link fence is the most commonly used, is cost effective, and should stand at least eight feet from the ground level with a mesh no larger than two inches. It should also be topped with some type of barbed wire extending at an outward angle. Security personnel, however, must be thoroughly aware of all local ordinances because some communities have restricted the use of outward barbwire. Outrigging, like razor wire, must also be appropriate to the height of the fence. A six-foot fence could easily be brushed by a six-foot tall individual causing some serious bleeding. Anyone panicking would be cut severely, possibly fatally, if he or she does not receive assistance. Concertina wire also can create a formidable barrier. Concertina wire is often used in emergencies to lock access when a fence or gate is no longer secure.

The fence must be at least 11-gauge wire. Cost is always a factor, but the stronger the fence, the better. Plus, the larger the mesh, the larger the wildlife that can cross through it. Critical areas may need double fencing. This is especially true of the fuel farm area. This crucial area is a highly desirable target for a terrorist seeking to get attention, causing a lot of damage, and killing a large number of people. Another highly vulnerable area is the power source access points. Double outrigging of the fence would be most appropriate, including the use of razor wire if permissible.

The fence must always be flush with the ground. If the airport is located in a sandy soil or loose soil area, the fence needs to extend down into the ground. Embedding the fence into cement would be even better, although costly. Intruders should not be able to tunnel directly into the airport, especially near the fuel farm, power sources, or navigational equipment. The fence should also have a clear space of at least 20 or so feet on both sides, providing a full field of vision for security. On the field side, the grass near the fence must be maintained or mowed at regular intervals. Snow should

not be piled high near the fence. Nearer the terminals and hangars, cargo should not be permitted to be piled up near the fence enabling the intruder to literally step over. Fences can also be electrified, but issues of liability present themselves when this method is chosen. If budgetary constraints permit, fiber optic sensors can be mounted on a fence, which present a safer alternative.

Adequate lighting on the perimeter is also a mandatory security function. An unobstructed 20-foot view is useless if it is cloaked in complete darkness. Four types of lights are commonly available. They include floodlights, streetlights, fresnal units, and searchlights. Inside, the perimeter lights should be positioned about 30 feet from the boundary, 50 feet apart, and 30 feet high. If an officer cannot read the headlines of a newspaper, some additional light is needed. When dark areas remain unlighted, security may be required to investigate in the shadows with a flashlight, a function that is both time-consuming and dangerous. Providing night-vision goggles to security personnel can also be effective, but is another costly measure.

FAR Part 139 requires that lighting must "… show that all surface apron, vehicle parking, roadway, and building illumination lighting….is so designed, adjusted, or shielded as not to blind or hinder air traffic control or airport operations." Perimeter lighting deployed in conjunction with a chain-link fence should project light toward the fence, preferably from inside the fence, keeping control over the source of the light with airport authorities. The illuminated zone outside the fence should reach about 20 yards or more.

Parking lots can often present some unique problems. They are compounded by the scarcity of space and the need for travelers and employees to be provided with long-term and short-term parking. When possible, privately owned vehicles should be parked at a distance for the terminal, even though this is quite unpopular. Vehicles should be parked outside the perimeter in a parking lot with its own fence, gate, and lights. Obviously, the potential for assault and theft in these areas is significant. Consequently, either an escort service or other appropriate security measures deserve some attention. Emergency call boxes are useful in these areas. Lighting is a crime prevention measure that is an absolute requirement.

The number of gates providing access should be limited to the number of essentially required entry points. Gates either need to be guarded by a security officer or constantly viewed by some sort of electronic equipment, either CCTV or by use of a card actuation system to gain access. Earlier methods involved simply padlocking the gate and providing keys to only those truly needing them. Advances in technology enable security now to utilize electronically generated controls, key card access, keypad access, and others, depending on the budget of the operation. Dogs are also a viable option.

It should also be remembered that natural boundaries of airports also deserve some attention. Lakes and rivers will not stop a well-equipped terrorist. Additionally, any opening greater than 96 square inches is considered large enough for a human to pass through. Openings larger should be secured with metal bars of sufficient strength to deter an intruder. Whatever method is utilized, fences and gates in whatever configuration need to be periodically inspected. Security should always be alert to wear and tear on a system or man-made damage.

Security experts, unfamiliar with airport operations, sometimes view the air traffic control tower as a security tool. This is a misleading perception. Air traffic controllers are kept busy enough controlling air traffic on the ground and in the sky. Tower operations personnel cannot be expected to perform a continuing security role. Most controllers will alert security to anything they observe that is unusual or dangerous. Permanently stationing airport security personnel in the tower is another matter. Certainly they have an expanded field of vision.

EXTERIOR ALARM SENSORS

A fence provides minimal protection. Lighting adds to the protection level. However, the combination of a fence, proper lighting, and at least two sensors greatly increases the probability that an intruder will be detected. Sensors can be expensive, and the actual threat must be weighed against

FIGURE 15.1 The FiberPatrol® FP llOO series features fiberoptic sensor technology available for fence-line perimeter security. These location-sensing intrusion detection systems are distinguished by their ability to pinpoint the absolute location of an intrusion attempt to within one or two fence panels. (Photo courtesy of Optellios, Inc.)

the cost. A professional should be consulted. Product knowledge, proper installation techniques, site surveys, and choice of the correct protective device are critical to satisfactory performance. Such factors as weather, terrain, area to be covered, and electromagnetic interference need to be evaluated. Sensors come in all shapes and sizes, and the technology is constantly improving. Such devices are either mechanical, electronic, or a combination of both (see Figure 15.1).

Sensors in alarm systems range from simple magnetic switches to sophisticated Doppler radar. There are literally thousands of differing types of magnetic switches. The simplest sensors are electromagnetic devices in which an electric circuit is broken or closed. There are varying degrees of integrity. Shock sensors are also still available on the market today as Piezo-electric sensors and can be installed directly on a fence. They originated as mechanical or acoustical vibration detectors. Some sensors are pressure devices that respond to the weight of an intruder. Taut wire detectors are also quite functional. Any change in the tension of the wire activates the alarm. Photoelectric sensors are activated when a light beam is interrupted. Some sensors currently on the market include the following.

Motion Detectors

These devices are based on the simple concept of detecting motion. Earlier models were referred to as ultrasonic motion detectors and used the Doppler effect to work. Each unit had an emitter and a receiver. The detector would flood the designated area with ultrasonic sound waves not detectable by the human ear. The sound waves would span outward and bounce off any inanimate objects returning the wave to the receiver. A human intruder would interrupt the constant flow of sound waves triggering an alarm. These devices do not function in an open area, and unfortunately lots of natural phenomena will also set them off.

Microwave

Microwave motion detectors also operate on the Doppler effect using an emitter and a receiver. They function in the gigahertz band of the radio frequency spectrum. Unlike ultrasonic motion detectors, wind currents or changes in temperature do not especially affect them. The greatest drawback is that sometimes they are "too accurate." Due to their extremely high radio frequency, the microwave detection pattern can see "too much," causing confusion as to what is actually a threat. Additionally, microwave reflects metal, easily setting off the alarm. Line of sight is required, and blind spots can occur between the transmitter and receiver.

Charged Coupled Devices

Charged coupled devices are solid-state image sensors that convert light into an electrical signal. There are numerous types on the market. It is sometimes referred to as a chip camera because it has a small, photosensitive unit that has replaced the imager or tube in a CCTV.

Portal Coaxial Cables

This system involves the use of two cables. One cable transmits, and the other receives. The detector senses any changes in the electromagnetic field surrounding the coaxial cables. Specifically, ported coaxial buried line sensors are coaxial cables that have small, closely spaced holes in the outer shield. These openings allow electromagnetic energy to escape and radiate a short distance. Emissions from these cables create an electric field that is disturbed when an intruder enters the field. Ported coaxial cables are installed in pairs, approximately 5 feet apart. Processors emit a pulse of radio frequency energy through one of the cables and receive it through the other. The speed at which the pulse travels is constant, creating a standard amplitude signature that is picked up by the signal processor. This signature is stored and continually updated to account for minor or gradual changes in the burial medium and environment. When an intrusion is attempted, the pulse signature changes radically and is picked up by the signal processor. If the variation falls outside allowable parameters, an alarm signal is generated.

There are two basic types of buried ported coaxial sensors available: (a) continuous wave sensors and (b) pulsed sensors. With regard to portal coaxial communication cables, the latest network protocols and business applications are capable of transmitting vastly increased amounts of data, and many existing cabling systems cannot cope. With the emergence of fast ethernet, gigabit ethernet, and more recently 10 gigabit ethernet, outdated and inadequate systems running on earlier versions of unshielded twisted pair technology, coaxial, and twinaxial are now being replaced by structured cabling systems and wireless networks to keep up with modern performance levels.

Electric Field

Electric field devices used to be quite popular. They require a field generator that includes a long field wire and a sense wire that are placed parallel to each other. If an intruder approaches the fence, the signal is interrupted. Electric fences are a system all together. The potential for inadvertent severe injury to "wanderers" as opposed to intruders have made electrified fences impractical and outdated. Fiber optics mounted onto fences has replaced this concept of protection.

Vibration and Stress Detectors

These units can detect someone simply walking into a protected area from a completely concealed unit. Near fences, they can be installed underground to follow along the terrain, and the actual weight of the intruder affects the system. Most systems can be adjusted for sensitivity so that small animals do not trigger it. Depending on the need, they can be extremely sensitive. In one interior setting, an alarm at a restricted military facility was repeatedly initiated when geckos ran across the device. The sensors are also referred to as seismic sensors or buried-line intrusion detectors. Vibration detectors can be mounted right onto the fence at specific intervals and will detect anyone trying to climb or cut the fence.

Closed Circuit Television

CCTV has become the security device of choice in many applications, not just along a perimeter. It can be used in corridors, entrances, and secured areas. Cameras can instantly monitor activity near

a fence and record the intruder if needed. Some cameras are equipped with motion detectors to alert a guard that a camera has detected an individual near the fence. They have become indispensable in today's security world and come in all shapes, sizes, and budget requirements.

A significant enhancement to CCTV comes with digitization. For example, now a QUAD can compress images from four cameras into a single frame of VCR tape or DVD, allowing the operator to view all four cameras on a four-way split screen. Video multipliers also allow the system high-speed, full-frame recording from multiple sources. Infrared cameras are used for night surveillance.

Once the exclusive domain of sophisticated aerospace and military imaging systems, high-quality infrared (IR) focal plan arrays have been refined to give security professionals affordable see-in-the-dark technology. Designed to integrate into existing CCTV systems or operate alone, these new high-resolution cameras are rugged, easy to operate, and portable. IR cameras can be put to work wherever poor visibility hampers the performance of visible CCTV cameras. With IR cameras in place, as much as 50 percent of a facility's night lighting costs can be eliminated for both interior and exterior surveillance (Frank, 1991).

Infrared Motion Detectors

Active Infrared

Active IR systems are photoelectric, using visible or invisible pulsed IR beams. They are not lasers. The alarm is actually triggered when someone breaks a beam of light being sent from a transmitter to a receiver. Most systems utilize dual beams, and the system requires that both beams be broken at the same time before an alarm is set off. This significantly cuts down on false alarms. Line of sight transmission is required for satisfactory operation. Beam ranges vary from anywhere between 10 and 800 feet.*

Passive Infrared

IR detectors were the next generation motion detectors after sound waves. Largely as a result of research done as part of the space program, they became more commonly used and reasonably priced. However, in reality they do not really detect motion. An IR detector literally sets a "virtual" barrier along a path. Passive IR detectors do not emit any energy. They are in the strictest sense only receivers, which detect the body heat of an intruder. The device detects and registers the "normal" ambient temperature of IR energy in a particular zone. When an intruder violates that space, the temperature changes, and an alarm is activated. Generally, they work best indoors. The best devices incorporate two different sensors in the same equipment, for example, IR and Doppler combined.

Glass-Break Detectors

There are two categories of these. One attaches directly to the glass being protected and a second, space coverage type of acoustical sensors that protect all the glass in a specific area. Glass-break detectors are extremely sensitive, and modern ones can distinguish between glass actually being broken and noises similar to glass breaking. They have advanced electronic detection circuits, which are no longer fooled into many previously tedious false alarms.

THE CONTROL ROOM

All the unique devices installed in an airport security system need to be controlled from a central point. A control panel in a control room is generally considered the heart of the system. Today most

* *Note*: Except for a very few highly specialized fiber optic systems in military or government use, no laser beam technology is currently available on the mainstream commercial market.

control centers have the following (Internet:http://www.aloha.com/~sednat1/prod02.htm#detection, 14 August 2001):

- Alarm device inputs or zones
- Reporting device outputs
- Timing circuitry
- Power supplies
- Back-up batteries
- Programmable microprocessors
- Memory for user codes
- Memory for activity logs that can be displayed locally or downloaded
- Digital communications
- Supervisory circuits to monitor zone status, AC power, battery power, phone line integrity, self-diagnosing programs, and fuse integrity

Alarms

Alarms can be silent, audible, or visual. Visual alarms are specifically designed to catch someone's attention to a potential problem. A blinking red light is the classic example, either on a control panel console or at the site of the alarm involved. Audible alarms are intended not only to alert security, but also to scare the intruder. Any noise is acceptable, including bells, sirens, whistles, chimes, or music. One system actually plays the Star Spangled Banner at 118 decibels. Silent devices are designed to alert security as well as law enforcement.

No Power, No Security

Unless a security system has power, it is severely handicapped to say the least. The power supply provides the necessary voltage to operate not only the command center, but all the devices installed throughout the airport to provide security. Most alarms panels are connected to a primary current through a transformer. The power supply provides constant power to all systems and their components. In the event of catastrophic failure, the back-up battery system takes over. Alarm systems should always be programmed to report a current failure or low battery conditions. Testing of the back-up system is critical.

Media Intrusion

The role of the media has become a significant factor in all hijackings. Margaret Thatcher, former Prime Minister of Britain, referred to "the oxygen of publicity" as constituting a vital requirement of any terrorist undertaking. Photographs of armed police lying in wait near an aircraft could pose considerable problems for police negotiators should the photos reach the hijackers. Consequently, the police and the media are often at odds. The public is eager to soak up any sensational and news-breaking pictures, and the press seems willing to do whatever it takes to get them, regardless of the delicacy of any negotiations. In any democratic society, the value of the press and its principal focus of newsgathering must be weighed against the impact on the situation at hand. Cooperation with the media is necessary and sometimes difficult but must be addressed. Airport security must always be prepared to handle, some say massage, the media.

Some would take the point of view the media are only interested in sensationalism. They are allegedly interested only in what sells. Arguably, they make terrorism possible and profitable. Large terrorist organizations, like the Irish Republican Army (IRA) and the Palestine Liberation Organization (PLO) have well-developed press sections within the organization. They have well-planned and organized long-term strategies for the use of the media to project their central message.

These press specialists can respond immediately to an event, feeding material to a sympathetic journalist and making attempts to justify any violence. The security forces at airports must operate in the same way. Media management and propaganda feature as an important policy consideration in determining the appropriate response.

Some scholars have reached the conclusion that use of the "…media does not cause terrorism, but they can make it worse by poor reporting practices, by allowing themselves to be manipulated by interested parties, and by not giving audiences a better understanding of the issue" (Picard, 1993). The most important function of the media when a terrorist act is occurring is not really to literally describe the acts but to influence the meaning assigned to the acts. For violence to become a terrorist act, there must be witnesses. Airports provide the victims and the witnesses in one package.

Computer Security

Although the issues behind terrorism are usually national, regional, or issue specific, the impact of terrorist campaigns is international. Domestic terrorism often has spillover effects. Combating terrorism has encompassed efforts to use the law, efforts to infiltrate and destroy, and efforts to remedy the underlying cause of the violence. However, with the dawning of the computer age, terrorism can now be accomplished by individuals thousands of miles from the target. Airports, airlines, and their computer networks are no less vulnerable than anything else. In fact, they may be one of the softest targets available to terrorists while offering the least amount of physical risk to the perpetrators. They present an easy and potentially massively destructive tool to create panic. To completely shut down the airways or to cause several aircraft to crash or have a midair collision is a real danger, somewhat ignored by the airlines. The FAA is aware of the problem and has made significant strides to establishing failsafe systems.

On the other hand, airport security and airlines in general need to stay on top of state-of-the-art computer security systems. Computer crime includes but is not limited to accessing a computer's database without authorization for the purpose of sabotage or fraud. Obviously, the information revolution is on, and electronic access to information is the wave of the future. Electronic kiosk systems are one of the key means by which to acquire this access. The benefits include providing connectivity and flexibility of access while avoiding the security-related problems of using personal computers. Problems arise because technologies that give access enable fraud. All computer systems suffer from security vulnerabilities that can threaten the integrity of the services they provide and can infiltrate any computer to which they are connected. Airport security officials must recognize the full risks that information and service computer systems represent. Terrorists could also seek to access the computer systems on which a nation's entire air traffic control is based. To hack into a signal circuit could give the intruder the ability to purposely collide aircraft on the ground or in the air.

The Central Intelligence Agency (CIA) has admitted its concerns with regard to its ability to stop hackers and the use of sophisticated technology by smart terrorists. Lawrence K. Gershwin, the CIA's top advisor on science and technology issues, admitted that "… we end up detecting an attack after it's happened" (Schroeder, 2001). He went on to testify that despite a major increase in intelligence efforts dedicated to computer security, potential hackers still develop means to get into the system faster than the authorities at the CIA can detect and nullify them. The CIA does believe that the threat from computer infiltration is greater from foreign governments than it is from terrorists, but that does not mean that the threat does not exist (Internet: http://news.cnet.com/news/0-1003-200-6344815.html?tag=prntfr). A "cyber-attack" from a terrorist organization is always possible. It is a well-accepted concept in criminology that crime is strongly linked to opportunity, and computers at airports offer some unprecedented opportunity for easy access. Once terrorists have mastered the technology, it is likely that they will use it. More than likely, they will seek to disrupt the financial networks or communication networks on which the industrialized nations and their airports are so dependent.

Kiosks

A kiosk is a publicly accessible computerized unit that gives information and services to authorized clients who are not particularly computer proficient. Most airlines have already implemented automated kiosks that deliver information to users. Passengers can now purchase tickets, locate flight information, and even print out boarding passes. Kiosks are a cost-effective means of providing services to clients. Every transaction performed on a kiosk is one that an employee does not have to perform. The shift represents a savings in not only the costs related to personnel, but also the costs of building and maintaining offices and infrastructure. They also have a security price; exposing the airlines to problems of ticket theft and fraud. The Electronic Communications Privacy Act of 1986 makes it illegal to intentionally access, without authorization, a facility providing electronic communication services, or to intentionally exceed the authorization of access to such a facility. However, successful prosecutions are rare, and the damage is already done; i.e., the fraud has taken place or an incident has occurred. Security measures for computer systems include logical controls such as encryption, physical controls, administrative controls, and protecting the equipment from fire and heat.

Logical controls are unique programs written into the software of the system. The most common, of course, is the use of passwords. Multilevel access capability allows some operators to access some information, with only a limited number of people having access to the entire system. A callback modem is also a good logical control. A user attempting to access the system enters an identification code after dialing the computer; the modem scans its directory for the appropriate code and phone number and calls back. After the code is verified, the connection is completed, and the user is connected to the computer system. A corollary is the use of encryption. The device puts the data into code before it enters the transmission line, and it is decoded at the receiving end.

Computers need adequate physical controls as well. At airports they should be located in restricted areas with locked doors, equipped with alarm systems. If the public has access to them, a supervisor should be on duty to monitor their usage at all times. Always remember SAM, that is, Secure it, Alarm it, and Mark it.

Cyber-security officials have praised the administration's efforts to have an Information Analysis and Infrastructure Division within the Department of Homeland Security. The new office will combine elements of the FBI's Cyber-division and Commerce Department's Critical Infrastructure Assurance Office. The National Infrastructure Protection Center's multiagency analysis and warning function would also be combined into the new office.

CONCLUSION

Access control to an airport is vital. Locks, alarms, and sensors best control that access. A mixture of these measures is usually the best approach. Key and lock controls, placement of the devices, electronic access cards, fences, and signs all play an important part in managing the flow of people through an airport. The use of computers has greatly facilitated this effort. Using computers, manufacturers of access controls can create huge systems that provide security with a tremendous amount of flexibility. All access-control systems should be based on a risk assessment analysis in concert with the latest versions of access-control technology and computerized systems. The media is just one of many potential intruders that need to be reasonably controlled. Also important is strict control of computer and kiosk access.

EPILOGUE

Over seven years have passed since one of the worst acts of terrorism in American history. The site has been cleaned up, but the scars remain, while fear of another attack lingers. That fear is well justified. Another attack will undoubtedly take place, and the aviation industry is still a prime

target. To avoid such a tragedy, an independent group, consisting of security experts, should advise policymakers and members of Congress on what measures can best serve the interests of the industry. These recommendations should subsequently not be amended on the basis of political or profit-making goals. Much money has been thrown at the problem. Unfortunately, airline security continues to consist largely of window dressing; possessing gaping holes. The vulnerabilities appall serious aviation experts.

During the fiscal year that ended in September 2002, airline passengers paid the federal government nearly 1 billion U.S. dollars for security. Each passenger was charged a $2.50 security fee added onto the price of a ticket. Additionally, the airlines in turn paid approximately $160 million, which doubled in 2003. Currently, airlines pay one-twelfth per month of their 2000 screening costs to the Transportation Security Administration on a monthly basis. However, it does not appear that the money has been particularly well spent. For example, controls over airline employees, service and maintenance personnel, and cargo continue to be weaker than they should be. Many solutions have been offered, yet many of them contain aspects of corporate or personal gain or political motivation and manipulation. Arguably, the American public is being duped into a false sense of security.

Changes

There are still many changes being reviewed and implemented by governments to combat the threat of terrorism, specifically as it relates to aviation. Some are temporary fixes like locks on cockpit doors, and some are more long range such as more sophisticated explosive detection systems and improved preventive law enforcement. The TSA has focused considerable effort on attempting to ensure that a passenger does not carry a bomb or weapon onto a commercial aircraft (see Figure 15.2). Unfortunately, about one-half the cargo hold is usually filled with nonpassenger cargo. Despite several reports issued by the General Accounting Office (GAO) recognizing the potential problems has been discussed a lot, but little has actually been done. Such vulnerabilities threaten the entire transportation network and provide terrorists with a target of opportunity.

The More Things Change, The More They Remain the Same—Screeners Are Screeners

The TSA is facing the same challenges that private security incurred prior to TSA involvement. So far they have not been able to avoid the same missteps that private security firms have encountered for years. If administrators do not address these issues, the same potentially disastrous results will eventually occur. The opt-out program is a diamond in the rough and needs to be more effectively pursued.

FIGURE 15.2 A knife hidden inside a lipstick container represents the lengths to which people will go to conceal weapons. (*Source*: Transportation Security Administration. www.tsa.gov)

The quality and caliber of air baggage and passenger screeners represents a persistent problem. Not long after the holidays in December 2002, at Seattle's International Airport, a baggage screener was found sleeping on the job. Prior to 11 September, he simply would have been a private security company employee sleeping on the job. Twenty-three incoming flights were delayed while dogs and security personnel checked the concourses. Employee training and dedication levels are often less than optimal. Scores of instances of weapons and potentially dangerous instruments passing through checkpoints have been well documented by the press in the past year. Screening at most airports in reality remains a sieve.

On top of this, screeners wanted to unionize. The Bush Administration announced it would deny 56,000 federal airport security screeners the right to negotiate for better working conditions and higher pay. Admiral James Loy, Agency Chief of the TSA at the time, proclaimed that mandatory collective bargaining is not compatible with the war on terrorism. The American Federation of Government employees promptly threatened to sue. In rebuttal, the administration denies that there is widespread dissatisfaction among screeners. This approach may well be shortsighted. Screeners are also complaining that they are suffering from back and knee injuries from lifting heavy bags that they are required to carry from conveyor belts to newly installed screening machines. They also have expressed displeasure at the placement of the machines, indicating they are often in dark and dirty terminal basements. A TSA spokesman has confirmed the injuries and claims the agency has addressed them. However, some of the same problems of employee satisfaction that plagued private airport security are resurfacing.

The TSA grows by leaps and bounds. Starting with about 13 employees, it had grown to more than 64,000. Congress originally imposed a 45,000-member employee cap. Admiral Loy had requested nearly 6 billion U.S. dollars for the 2004 budget. Early in January 2003, agency executives met to determine just how they were going to pay their employees. Congress would prefer the agency focus more on equipment and airport modifications than staffing. The TSA is part of the new Homeland Security Department, which employs an additional 170,000 people. Consequently, with size comes bureaucracy, and with bureaucracy ultimately comes inefficiency. The current director, Michael Chertoff, has changed the tone of the agency and recognized the need for formal risk-management cost-effectiveness analysis.

Arming Pilots

An additional change involved arming airline personnel. Stephen Luckey, chairman of the National Flight Security Committee of the Air Line Pilots Association told Congress that pilots were willing and prepared to assume the responsibility. That was clearly true. In response, Congress agreed. Regardless, problems have already emerged. Claiming he did not know it was not appropriate, a Northwest Airlines pilot in January 2003 was arrested at New York's LaGuardia Airport with a loaded gun in his bag. The over-eager pilot claimed it was all a big mistake. Since that time, another pilot has indvertently fired a weapon on board an aircraft in flight, and problems will continue to persist.

The key to effective airline security is on the ground. Security experts learned this in the 1970s, and apparently it needs to be relearned. The argument that aircrew are the last line of defense is an emotional but not a particularly realistic approach. Hopefully, no air crew member is going to let a passenger or fellow crew member die to retain a weapon the terrorists has demanded be given up. A firefight at the OK cockpit is a really bad idea. Shooting a terrorist before he or she takes over a flight and drives the aircraft into a populated building or neighborhood will not prevent an already horrendous situation from playing out.

Other experts have indicated that arming pilots will serve as deterrence. More than likely it will serve to provide a ready-made armory for the terrorist. Why risk secreting a weapon through airport security when you can take one off an air crew member? As mentioned, the terrorist will present a no-win situation to the air crew. Die, have a hostage or hostages killed, or relinquish the weapon. In

a worse scenario, the terrorist will simply kill the air crew members. Five terrorists versus two pilots is not a particularly winnable fight, especially while continuing to fly the plane. One pilot standing guard at the door while the other pilot flies the plane is a good movie scene. It does not represent an effective tool to stop a terrorist either determined to explode an aircraft or to produce a passenger cabin full of dead souls.

Last but not least, dismissing the concept of airline civil liability as a nonissue because a litigious society exists in the West does not make it disappear. A gun-slinging pilot could theoretically bankrupt an airline. Again, the key to effective aviation security is on the ground. Realistically, once the aircraft is airborne it is too late to avoid some sort of a disaster

The Federal Air Marshal Program

The original Sky Marshal Program has changed considerably over the years. As long ago as the 1970s administrators recognized that the program was one tool in the airport security toolbox but not the absolute solution to airport security. As recently as 2001, the program had a $4 million budget and only about 33 armed officers who flew on international flights. A year later, thousands of marshals and a budget of over a billion dollars have not resulted in concrete proof that the well-intentioned officers have foiled a single hijacking attempt. On top of that, just because an officer is on board does not mean the aircraft will not be hijacked or destroyed.

A major problem is that it is logistically impossible to have an officer on each and every flight. It is even impossible to have an officer on every aircraft considered at some higher risk. In an attempt to cover more aircraft, the program rushed to hire. However, in the rush to grow, the agency got ahead of itself. Marshals have complained that poor scheduling, inadequate training, insufficient supervision, and cutbacks in the marksmanship training have diminished the force. Indeed, at one point the agency was hiring approximately 800 marshals a month. The administration of such a process carries its own problems. The question therefore presents itself: is the public getting sufficient protection considering the cost?

Emerging Technology

There are so many emerging technologies with applications to airport security it is impossible to discuss them all. What is relevant boils down to what technology will provide the most security for the most reasonable price, within the context of a complex airport environment. For example, literally hundreds of unique devices previously applicable within a broad private security context are available for use in an airport. The challenge is to determine what will suitably add to the appropriate mix of gizmos in the overall big toolbox.

For example, Imaging Automation's document checker matches documents against a database that indicates what the document should look like. They are already in use at Dallas-Fort Worth and Boston's Logan airports. They essentially compare driver's licenses, passports, and other identifications (IDs) against the real thing. The system was developed to weed out job applicants with forged ID documents. The company would like to convince the TSA that scanners the size of a small toaster could perform the same check on passenger documents.

Another issue relates to the sophistication of more expensive pieces of equipment. Many explosive detection devices, trace detection devices, biometric access control devices, and others are undergoing intensive research and development. Again, cost is a gigantic issue. Because the technology exists does not mean it can adequately be integrated within the airport context for a reasonable cost. Some experts have questioned the decision to pour billions of dollars into baggage screening equipment that is error prone, labor intensive, and extremely expensive for smaller airports to finance. The TSA claims to have met its deadline of 100 percent baggage screening by 31 December 2002. However, they did so by weakening the requirements, using a combination of explosive detection systems, explosive trace detection systems, dogs, and manual inspection. The whole issue raises

the question whether spending $12 billion dollars on already outdated, but approved, technology with error rates as high as 30 percent and slow throughput is the answer.

Consideration of the European model of a several tier baggage screening system must be reviewed. Additionally, Heinmann's explosive detection machines scan 1000 bags per hour and are cheaper. However, U.S. manufacturers are balking at the purchase of foreign-produced machines. In conjunction, the detection of high-risk people, not baggage, is critical. The Israelis and the Europeans have recognized this for years. Airport security officials need to be smarter, more efficient, and more realistic in approaching the security needs of airports in the 21st Century. Not to heed the lessons learned of the past and not to recognize the successes of the Europeans and Israelis condemns the air transportation industry to constant threat of disaster.

Civil Liberties

In January 2003, a federal appeals court ruled that the administration had the authority to designate U.S. citizens as "enemy combatants." This enabled the government to label citizens and detain them in military custody if they were considered a threat to national security. In the case of Yaser Hamdi, a Louisiana-born American citizen who was captured in Afghanistan fighting for the Taliban, a lower court had originally ordered the government to release more information to the defense. The government had been able to deny him access to his public defender and had not filed charges against him. The court opinion said, "Because it is undisputed that Hamdi was captured in a zone of active combat in a foreign theater of conflict, we hold that the submitted declaration is a sufficient basis upon which to conclude that the commander in chief has constitutionally detained Hamdi pursuant to the war powers entrusted to him by the United States Constitution" (Advance sheets). The ruling originated from one of the most conservative jurisdictions in the nation. Later the Supreme Court ruled in the case of *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004) with even firmer language. It reversed the dismissal of a habeas corpus petition brought on behalf of Yaser Esam Hamdi, the defendant. The Court recognized the power of the government to detain unlawful combatants, but ruled that detainees who are U.S. citizens must have the ability to challenge their detention before an impartial judge.

This case parallels but is easily distinguishable from Padilla versus Bush. Jose Padilla, the alleged "dirty bomb" suspect, has also been designated an "enemy combatant." However, he was captured on U.S. soil after arriving at Chicago's O'Hare International Airport as part of an alleged scheme to explode a conventional bomb laced with radioactive material. His attorneys contended that the government should be forced to comply with standard criminal court procedures including the right to counsel. On 3 January 2006, he was finally transferred to a Miami, FL jail to face criminal conspiracy charges. He was found guilty of all charges on 16 August 2007, by a federal jury, which found that he conspired to kill people in an overseas jihad and to fund and support overseas terrorism. On the civil side, a Pakistani businessman from Los Angeles lost a discrimination suit he filed against United Airlines. He had been blocked from boarding a plane following 11 September. The jury reasoned that the discrimination was justified. The civil suit involving the 11 September incident remains bogged down in litigation.

SUMMARY

Better management and better utilization of resources is needed. An independent committee of experienced security experts could help policymakers to determine the best methods of creating an effective toolbox of assets to combat the threat to aviation. The threat is not going to evaporate anytime in the near future. Good judgment and common sense aspects need to be integrated into the system, devoid of personal, political, or corporate profit. Many security analysts argue that all U.S. airport security policy rests on a faulty proposition.

Certainly it is arguable that by conducting equal screening resources to all passengers and all bags, the system *acts as if* security officials are assuming that every passenger and every bag is equally likely to be a threat. This risk analysis squanders limited security resources on low-risk passengers and bags, conversely devoting fewer resources to higher-risk passengers and bags. In addition, this approach has generated a now well-recognized "hassle factor" at airports that drives away airline passengers. A more intelligent approach to airport security is to apportion security resources to passengers and baggage in proportion to estimated risk. Risk-based airport security would mean a reduced focus on finding *dangerous objects* and an increased focus on identifying potentially *profiled actual threatening people*. This approach would single out those individuals most worthy of additional scrutiny. Screening resources would be applied in accordance with a passenger's risk category. Risk-based principles are already in use by the federal government with respect to border-crossing, where a number of programs (such as INSPASS and NEXUS) permit travelers to volunteer for preclearance, facilitating them in bypassing long lines when they actually pass through border facilities. Likewise, in the cargo area, "known-shipper" programs represent additional appropriate uses of risk-based decision-making. Overseas airports, in Israel and Europe, use risk-based techniques such as passenger profiling and trusted traveler programs to sort passengers into different risk groups for differential processing at the airport. The United States should be doing the same.

REFERENCES

Bordes, Roy N., "Pick a Card, Any Card," *Security Management*, 1994, pg. 74.
FAR 107.14; TSA 49 CFR Chapter XII, Part 1540.
Frank, Jeff, "Out of Darkness," *Security Management*, 1991, pg. 45.
http://news.cnet.com/news/0-1003-200-6344815.html?tag=prntfr.
Marketplace, *Security Management*, August 2001, pg. 142.
National Crime Prevention Institute, *Understanding Crime Prevention*, Stoneham, MA, Butterworth Publishers, 1986.
Naudts, John, "Access Control; It's in the Cards," *Security Management*, 1987, pg. 169.
Picard, Robert G., *Media Portrayals of Terrorism*, Iowa State University Press, Ames, Iowa, 1993, pg. 29.
Protective Technologies International, Inc. Access Control System, http://www.pti-world.com/Access control. htm, pg 1. 3 May 2001.
Report NumberAV-2000-017, http://www.securitymanagement.com/library/faa1299/txt.
Schroeder, Ray, "CIA Can't Keep Up With Hackers," *The Associated Press*, 21 June 2001.
Smart Card Overview, http://www.scia.org/knowlefgebase/aboutSmart Cards/primer.htm. pp 1–5.

SELECTED BIBLIOGRAPHY

Adams, James. (1986). *The Financing of Terror*, New York: Simon and Schuster.
Anderson, Teresa (15 February, 2001). "Airport Security, All Systems Go," pg.1–8, http://www.securityman-agement.com/library/000539.html.
Anderson, S. and Sloan. (1995). *Historical Dictionary of Terrorism*, Metuchen: The Scarecrow Press. http:// www.securitymanagement.com.
Alexander, Yonah. (1976) "From Terrorism to War: The Anatomy of the Birth of Israel." *International Terrorism*, New York: Praeger.
Alexander, Yonah. (1994) *Middle Eastern Terrorism: Current Trends and Future Prospects*. New York: Hall.
Alexander, Yonah, and Kenneth A. Myers (eds.). (1982). *Terrorism in Europe*, New York: St. Martin's.
Aris, Stephen. (May 1980). "Terror in the Land of the Basques," *New York Times*.
Basque Fatherland and Liberty (ETA), www.ict.org.il/.
Boyne, Sean, (11 April 2000). "Uncovering the Irish Republican Army-Organization and Command," Frontline.
Bahgat, Gawdat. (1994). "Democracy in the Middle East: The American Connection," *Studies in Conflict and Terrorism,* 17:87–96.
Barton, John H. (1980). "The Civil Liberties Implications of a Nuclear Emergency." New *York University Review of Law and Social Change* 10:299–317.

Bassiouni, M. Cherif (ed.). (1983), *Terrorism, Law Enforcement and the Mass Media*, Rockville, MD. National Criminal Justice Reference Service.
Becker, Julian. (1984). *The PLO*. New York: St. Martin's.
Beckwith, Charlie, and Donald Knox. (1985). *Delta Force*. New York: Dell.
Berkowitz, B.J., et al. (1972). *Superviolence: The Civil Threat of Mass Destruction Weapons*. Santa Monica, CA: Advanced Concepts Research.
Bill James A., and Carl Leiden. (1984) *Politics in the Middle East*. Boston: Little Brown.
Blumberg, Abraham S. (1979). *Criminal Justice and Ironies*. New York: New Viewpoints.
Bollinger, Paul P., Jr., "Airport." World Book Online Americas Edition, http:///www.aolsvc.worldbook.aol.com/wbol/wbpage/na/ar/co/0009760, (24 July 2001.)
Bolz, Francis. (May 1984). Hostage Negotiation Training. Grand Rapids Police Department, Grand Rapids, MI.
Bruce, Steve. (1985). "Paramilitaries, Peace and Politics: Ulster Loyalists and the 1994 Truce." *Studies in Conflict and Terrorism*, 18:187–202.
Bullion, Alan J. (1995). *India, Sri Lanka, and the Tamil Crisis, 1976–1994: An International Perspective*. London: Pinter.
Bureau of Alcohol, Tobacco, and Firearms, U.S. Department of the Treasury. (1995). *Violent White Supremacists Groups*. Washington, D.C.: ATF.
Cameron, Gavin. (1999). *Nuclear Terrorism*, Palgrave Macmillan, UK.
Carter, D.L. (November 2004). Law enforcement intelligence: a guide for state, local, and tribal law enforcement agencies. *Federation of American Scientists.* http://www.fas.org/irp/agency/ doj/lei/chap1.pdf.
Chubin, Shahram. (1997). "Iran and Its Neighbors: The Impact of the Gulf War." *Conflict Studies* 204:1–20.
Clark, Robert. (1984). *The Basque Insurgents*. Madison: University of Wisconsin Press.
Clutterbuck, Richard. (1975) *Living with Terrorism*. London: Faber & Faber.
Coates, James. (1987). *Armed and Dangerous: The Rise of the Survivalists Right*. New York: Hill and Wang.
Cobban, Helene. (1984). *The Palestine Liberation Organization: People, Power, and Politics*. Cambridge: Cambridge University Press.
Combs, Cindy (2000). *Terrorism in the Twenty First Century*, 2nd Edition, Little Saddle River NJ: Prentice Hall.
Costigan, Giovani. (1980). A *History of Modern Ireland*. Indianapolis, IN. Bobbs-Merill.
Cranston, Alan. (1986). "The Nuclear Terrorist State." In Benjamin Netanyahu (ed.), *Terrorism: How the West Can Win*. New York: Avon.
Crozier, Brian. (1975). "Terrorist Activity: International Terrorism." Hearings Before the Subcommittee to Investigate the Administration of the Internal Security Act and Other Internal Security Laws of the Committee on the Judiciary, 79th Congress, 1st Session, Washington D.C., U.S. Senate.
David.B. (1985). "The Capability and Motivation of Terrorist Organizations to Use Mass Destruction Weapons." In Ariel Merari (ed.), *On Terrorism and Combating Terrorism*. Landham, MD: University Press of America.
Debenham, J.K. (1973). "A Brief Description of the Effects of x-ray Inspection on Unprocessed Photographic Film," Film Technical Services Division, Eastman Kodak.
D'Oliviera, Sergio. (1973). "Uruguay and the Tupamaro Myth." *Military Review,* 53:25-36.
Dobson, Christopher, and Ronald Payne. (1982). *The Terrorists*. New York: Facts on File.
Donnelly, Sally B., (2001) "A Safety Fight at the FAA," *Time*. http://www.atag.org/ECO/default.htm.
Duff, Ernest and John McCamant. (1976). *Violence and Repression in Latin America*. New York: Free Press.
Ehteshami, Anoushiravan. (1995). *After Khomeini: The Iranian Second Republic*. London. Routledge.
Finn, John E. (1987). "Public Support for Emergency Anti-Terrorist Legislation in Northern Ireland: A Preliminary Analysis." *Terrorism* 10:113–124.
Flynn, Kevin and Gary Gerhardt. (1995). *The Silent Brotherhood*, New York, NY, Penguin Group, http://www.front14.org/rac/88pre2.htm.
Fooner, Michael. (1989). *Interpol Issues in World Crime and International Criminal Justice*, New York: Plenum Press.
Friedlander, Robert, (1979). *Terrorism*: *Documents of International and Local Control*, Dobbs Ferry, NJ: Oceana.
Gesell, Laurence E. (1981). *The Administration of Public Airports*, Coast Aire Publications.
Getler, Michael, "Move to Combat Air Piracy is Viewed as Toughest Yet," *Washington Post,* 18 July 1978.
Goo, S.K. (2003, May). *Airports favor private-sector screeners*. Retrieved November 10, 2006 from http://www.firstlinets.com/news/news_053003.htm.

Goo, S.K., (2004, July). *Airport screeners' new guard: Private security firms want to replace government in 2005.* Retrieved April 10, 2007 from www.washingtonpost.com.

Goodboe, Michael E. (April 1995). "Should Security Practice Andragogy," *Security Management*.

Goodwin, J. (2004, December). *Will U.S. airport convert to commercial screeners?* Retrieved November 7, 2006 from http://www.gsnmagazine.com/dec_04/us_airports.html.

Hill, Jim. (3 July 2000). US News, "New Airport Security Means Dogs, Better Scanners," http://www.cnn.com/US/9711/23/airport.security/.

Hiro, Dilip. (1987). *Iran Under the Ayatollahs*. London: Routledge and Kegan Paul.

Hodgson, Karyn. (1994). "Hot and Cold Biometrics Heat Up Again," *Security*, Cahners Publishing Company, Newton, MA.

Holden, Bruce. (1995). "Historical and International Perspectives on Right-wing Militancy in the United States," *ACJS*, Las Vegas, NV.

Horchem, Hans Josef. (1986). "Political Terrorism: The German Perspective." In Ariel Merari (ed.), *On Terrorism and Combating Terrorism*. Frederick, MD: University of America Press.

Horchem, Hans Josef. (1987). "Terrorism in West Germany," *Conflict Studies*. 186.

Interagency OPSEC Support Staff, (May 1996). *Intelligence Threat Handbook*, Section 4., http://www.terrorism.com/terrorism/IntelOperations.shtml/.

International Security Council. (1986). *State Sponsored Terrorism*. Tel Aviv: ISC.

Israeli Foreign Ministry. (1996) "Hizbullah" http://www.israel.mfa.gov.il).

Iyad, Abu. (1978). *My Home, My Land: A Narrative on the Palestinian Struggle*, New York: Times Books.

Jenkins, Brian. (1980). "Nuclear Terrorism and Its Consequences." *Society*, July/August: 5-16.

Jenkins, Brian. (1975). *Terrorism*: *Will Terrorists Go Nuclear?* Santa Monica, CA: Rand.

Juergensmeyer, Mark. (1988). "The Logic of Religious Violence." In David C. Rapaport (ed.) *Inside Terrorist Organizations*. New York: Columbia University Press.

Kane, Robert M. and Vose, Allan D., *Air Transportation,* Eleventh Edition, Kendall/Hunt Publishing Company, Dubuque, Iowa, 1999.

Kennedy Tom and David Phelps. (22 September 2001) "NWA will lay off 10,000; $15 billion airline aid OK'd," *Star Tribune*.

Kernodle, K. (2006). *Federal v. private–Security screeners: Where's the buzz?* Retrieved November 7, 2006, from http://www.fkassociates.com/Fed%20vs%20Private%20Security%20Screeners.html

Klaidman, Daniel. (18 May 1999). "The New Secret Weapons," *Newsweek.*

Kupperman, Robert H. and Darell M. Trent. (1979) *Terrorism, Threat, Reality and Response*. Stanford, CA: Hoover Institution Press.

Laquer, Walter. (Sept/Oct 1996). "Post Modern Terrorism," *Foreign Affairs*.

Lochmuller, C.H. (2001). "Fact Sheet: Tagging and Taggants for the Detection and Identification of Explosives, Smokeless Propellants, Black Powder, http://www.ca-rkba.org/ncrkba/nccda_taggant.html. 16 August 2001.

Mario, Leo, Stewart, Stanley, and Sharpe, Michael. (December 1999). *Air Disasters: Including Dialogue from the Black Box,* Barnes and Noble Books.

Masse, T.M. (March 24, 2005). The National Counterterrorism Center: Implementation challenges and issues for congress. *Federation of American Scientists*. Internet: http://www.fas.org/sgp/crs/intel/RL32816.pdf.

Melman, M. (1986). *The Master Terrorist*, Adama Publishers, New York.

Moore, Kenneth. (1991). *Airport, Aircraft and Airline Security*, Oxford, UK: Butterworth Heinemann.

Nambisan, Shashi Sathisan. (September 1999). *The 2020 Vision of Air Transportation: Emerging and Innovative Solutions*, American Society of Civil Engineers.

Nojeim, Gregory T. (1998). "Aviation Security Profiling and Passengers' Civil Liberties," 13 *Air and Space Law*.

Pan Am Flight 103 Disaster, (April 1992) United States Department of State, US Government Printing Office, http://www.emergency.com/panam103.htm., 13 Mar 01.

Panghorn, Alan. (5 May 1996). "How Far Has Europe Come Since Pan Am 103?" *Intersec*, Three Bridges Publishing, Vol. 6, p. 195.

Patterns of Global Terrorism. (1984). *Terrorism, an International Journal*, Crane and Russak Company, 1987, Vol. 9, No. 3.

Richardson, David B. (17 March 1980). "Basque Country: Violence is a Way of Life," *US News and World Report*.

Rose, Paul. (June 1986). "Terror in the Skies," *Contemporary Review*, p. 248.

Schroeder, Ray. (21 June 2001)."CIA Can't Keep Up With Hackers," *The Associated Pres*s.

Sharpe, Michael. (September 1999). *Air Disasters: The Truth Behind the Tragedies*. Brown Partworks Ltd.
Simonson Clifford E. and Spindlove. Jeremy R., (2000) *Terrorism Today, The Past, The Players, The Future*. Prentice Hall, Upper Saddle River, NJ.
Sjursen, Katie. (2000). *Globalization,* The Reference Shelf, Vol. 72, No. 5, H.W. Wilson Publishing.
Spence, Charles F. *Aim Far Aeronautical Manual, Federal Aviation Regulations*, McGraw-Hill Professional Book Group, August 2000.
Steinberg, M.(1988). "The Radical Worldview of the Abu-Nidal Faction," *The Jerusalem Quarterly*.
Study and Report to Congress on Civil Aviation Security Responsibilities and Funding, (1998). U.S. Department of Transportation, US Government Printing Office, Washington, D.C. (http://cas.faa.gov/reports/98study/98study.html.
Taylor, Qualye, E. (1994). *Terrorists Lives*, London: Brassey's Publishing.
Tibon, Jack. (1998). "Customs Hunt Air Smugglers" Government Computer News, Internet:http://www.pals.msus.edu.
The National Commission on Terrorist Attacks Upon the United States (9-11 Commission), (2004). Retrieved on April 08, 2007 from www.9/11commission.gov/report/911Report.pdf.
Transportation Security Administration. (2003) *Private airport security firms could get back in screening* business, Congress Daily. Retrieved December 21, 2006, from http://www.govexec.com/dailyfed/0803/080803cd1.htm.
Transportation Security Administration, (2004.) *Background on PP5 Airports* Retrieved on February 07, 2007 from http://www.tsa.gov/what_we_do/optout/editorial_1719.shtm.
Transportation Security Administration. (2004). *Guidance on screening partnership program.* Retrieved October 26, 2006, from www.tsa.gov/assets/pdf/SPP_OptOut_Guidance_6.21.04.pdf.
Transportation Security Administration, (2004). *Screening Partnership Program (SPP).* Retrieved on March 02, 2007 from www.tsa.gov/optout/spp.
Transportation Security Administration, (2006). *TSA Screening Partnership.* Retrieved on March 11, 2007 from www.tsa.gov.
Transportation Security Administration. (n.d.). *Results of PP5 and TSA airport survey*. Retrieved November 7, 2006, from www.tsa.gov/assets/pdf/Combined_TSA__PP5.pdf.
United States Government Accountability Office. (1987). *Aviation security: FAA preboard passenger screening test results* (GAO/RCED-87-125FS). Retrieved March 2, 2007 from www.gao.gov.
United States Government Accountability Office. (2003). *Airport passenger screening: Preliminary observations on progress made and challenges remaining* (GAO-03-1173). Retrieved September 27, 2005, from www.gao.gov.
United States Government Accountability Office. (2003). *Transportation Security: Post September 11 initiatives and long term challenges* (GAO-03-616T). Retrieved April 9, 2007 from www.gao.gov.
United States Government Accountability Office. (2004). *Aviation security: Private screening contractors have little flexibility to implement innovative approaches* (GAO-04-505T). Retrieved November 7, 2006, from www.gao.gov.
United States Government Accountability Office. (2004). *Aviation security: Preliminary observations on TSA's progress to allow to use private passenger and baggage screening services* (GAO-05-126). Retrieved September 21, 2006, from www.gao.gov.
United States Government Accountability Office. (2004). *Aviation security: Transportation security administration has made progress in managing a federal screening workforce and ensuring security at U.S. airports, but challenges remain* (GAO-06-597T). Retrieved September 21, 2006, from www.gao.gov.
United States Government Accountability Office. (2005). *Aviation security: Screener training and performance measurement strengthened, but more work remains* (GAO-05-457). Retrieved November 7, 2006, from www.gao.gov.
United States Government Accountability Office. (2006). *Aviation security: Progress made to set up program using private-sector airport screeners, but more work remains* (GAO-06-166). Retrieved October 24, 2006, from www.gao.gov.
U.S. Department of State (1996). *Patterns of Global Terrorism*, US Government Printing Office, Washington, D.C.
U.S. Department of State (2000). *Patterns of Global Terrorism*, US Government Printing Office, Washington, D.C.
Washington File. (2001) "Justice Department on Verdict of Pan Am 103 Bombing," http://www.usembassy.org.uk/terr127.html, 13 Mar 01.
Wells, Alexander T., (1998) *Air Transportation a Management Perspective*, Wadsworth Publishing Company.
White, Jonathan. (1998) *Terrorism An Introduction, 2nd edition*, Wadsworth Publishing, Belmont, CA.
White, Jonathan. (2002) *Terrorism An Introduction, 3rd edition*, Wadsworth Publishing, Belmont, CA.

Whiteman, Marjorie, (1998). Digest of International Law, Washington, D.C., Department of State, Vol. 11, Chapter 35, Article 2, 3518-3520.

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Terrorism/Aviation Security

AVIATION AND AIRPORT SECURITY

Terrorism and Safety Concerns

Second Edition

Kathleen M. Sweet

"It is a thorough review … leaving no avenue unexplored. And it has those gems of insight that will confirm it as a 'must have' volume on security and transport professionals' shelves."
—Phil Wilkinson, Air Commodore, Royal Air Force (retired), Hampshire, England, from the Foreword

Considered the definitive handbook on the terrorist threat to commercial airline and airport security, USAF Lieutenant Colonel Kathleen Sweet's seminal resource is now updated to include an analysis of modern day risks. She covers the history of aviation security and compares current in-flight security practices with those of other countries.

Covering Transportation Security Administration changes in security, policy, and training regulations since 9/11, this authoritative reference:

- Discusses a broad range of aviation terrorist incidents
- Considers aviation security in the present geopolitical climate
- Addresses cargo and passenger security
- Determines how security considerations are factored into business processes
- Details new regulations for the TSA
- Includes extensive background information on various terrorist groups

In addition to cargo and passenger security, the text looks at airport and aviation business practices and how security considerations are factored into business processes. The first edition quickly became required reading for air service operators and airport management training programs. This edition is certain to follow suit.

An Instructor's Manual with Test Bank, as well as PowerPoint™ slides, are also available for instructors.

Kathleen M. Sweet, Lt. Col., Ret., USAF, JD, currently teaches courses in strategic intelligence, security, and terrorism at the University of Maryland, University Campus. While in the military, she was an instructor at the Air War College at Maxwell AFB, Alabama, an assistant air attaché to the Russian Federation, and an intelligence officer, among other positions. Lt. Col. Sweet is also a consultant with International Risk Control Ltd., London, England and President and CEO of Risk Management Security Group, a transportation security consulting firm.

CRC Press
Taylor & Francis Group
an **informa** business
www.taylorandfrancisgroup.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

AU8165

ISBN: 978-1-4200-8816-8
90000
9 781420 088168

www.crcpress.com