Practical Aviation Security

Practical Aviation Security

Predicting and Preventing Future Threats

Third Edition

Jeffrey C. Price

Jeffrey S. Forrest

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Butterworth-Heinemann is an imprint of Elsevier

Butterworth-Heinemann is an imprint of Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-804293-9

Publisher: Candice Janco
Acquisition Editor: Sara Scott
Editorial Project Manager: Hilary Carr
Production Project Manager: Punithavathy Govindaradjane
Cover Designer: Victoria Pearson

Typeset by MPS Limited, Chennai, India

This edition of Practical Aviation Security is dedicated to all victims of air terrorism, and to those who diligently serve to keep aviation safe and secure

Forewords

Today as I was about to board the commuter train to my job in Manhattan, an older gentleman approached me on the platform saying, "I noticed the pin on your lapel. I was there too." It is a small pin that at first glance appears to be two streaming American flags hung side by side in vertical fashion. The chairman of my agency presented this to employees and colleagues 7 years ago in commemoration of an event that has since defined our lives and professions, wrenched our industry, and absorbed our national attention and resources. It was an event, as this gentleman's remark showed, that continues to bring strangers together in remembrance and renewed commitment to protect what is precious to a free society.

The work that the aviation industry and government have undertaken to ensure the security of air travel and commerce now informs other industry and business sectors of our economy. Indeed, security is now a pervasive element of business and social life around the world. The challenge of aviation professionals and government officials is how to achieve this security while preserving the vitality of the industry and the liberties of our citizens.

Jeff Price and Jeffrey Forrest's thorough text on aviation security instructs us in the history of assaults against civil aviation, which is nearly as old as civil aviation itself, while underscoring the changing nature of the assaults and the evolution of our government's response to these threats. The book documents the dramatic restructuring of transportation security oversight and regulation following the terrorist attacks of September 11, 2001, and provides us with a detailed understanding of the laws and regulations, the agencies and stakeholders, and the operating procedures and technical resources now brought to bear in the security of aviation.

Much has been accomplished to protect commercial flight from hostile intent, and time has proven the resiliency of the aviation system and our nation. There is, of course, still more to do, and we will look to those who follow us, perhaps some who are reading this book, to continue the vigilance and stewardship of this great industry.

May this little lapel pin that symbolizes the World Trade Center long remind us of those we lost in New York, NY, Arlington, VA, and Shanksville, PA, on September 11, 2001, and inspire us with confidence in the endeavor to pursue tolerance and understanding by drawing the world closer when we exercise our freedom and right to travel.

Jeanne M. Olivier
General Manager, Aviation Security and Technology,
The Port Authority of New York and New Jersey

The morning of September 11, 2001 (9/11) will go into history as a time that changed the way we live for many years to come. The bold and cruel nature of the terrorist attacks that led to the death of thousands of innocent people demonstrated how vulnerable we are when the enemy ignores the "rules of war." We were caught unprepared as the terrorists attacked one of the most sensitive and fragile technological systems we rely on—aviation. For the sake of accuracy, we should underscore that the attacks were not against aviation per se, but instead used aviation as a means to damage targets symbolizing our way of life and our sources of societal power—free enterprise, military infrastructure, and a democratically elected government.

Terrorists have targeted aviation many times in the past. However, prior to 9/11 hijacked airplanes had not been used as weapons against ground targets in such dramatic and strategic ways. Terrorists have been more attracted to using aviation than other modes of transportation. Nevertheless, many voices doubt as to whether the enormous investments in protecting the aviation system are reasonable since in the best case we can only divert terrorism from aviation to other targets. These are valid concerns that responsible governments must address. In this regard, governmental decision making creates policies and laws that not only protect global aviation but also establish national priorities.

A fundamental premise for this book is that the protection of aviation should be a national priority. On the morning of 9/11, the U.S. government and its security forces had relatively little knowledge of how to protect aviation from terrorism. In the United States, the pre-9/11 era was characterized with aviation security as a low national priority. Aviation security was perceived as an unproductive budget item. Therefore, many decisions related to aviation security were based on trade-offs related to costs rather than effectiveness. Additionally, there was no attempt to create an effective security system that would challenge the increasingly sophisticated methods of global terrorism. As a result, the United States lacked a knowledge base to defend itself against the 9/11 attacks. Since 9/11, the United States has partially addressed this weakness by importing knowledge and expertise from other countries, such as Israel and the United Kingdom. This book will help to minimize this concern by greatly enhancing the reader's knowledge and expertise related to U.S. aviation security.

In the first few years after 9/11, aviation security focused mostly on improving the screening of passengers and baggage. This policy resulted in a few critical misconceptions, including the belief that passenger checkpoints and screening of baggage can inclusively protect us from all threats to aviation security. Recently, the Transportation Security Administration has recognized the need for other security measures at airports like perimeter protection, access control, and suspicious behavior detection (among many other methods and strategies). In the spirit of adopting new security measures, we must always be reminded of the cliché that any security system is as strong as its weakest point. Therefore, developing proactive and comprehensive methods and strategies for use in our aviation security system is a continuous challenge. The attack resulting in the destruction of a

Russian passenger aircraft taking off from Sharm El Sheih (Egypt) with Airport employees involvement and the latest attack at Brussels Zaventem Airport public areas (both carried out by ISIS) are a tragic reminder that our job is not yet done. New terrorist organizations like ISIS push the envelope of uncivilized human behavior beyond anything we have seen in the past and we must be prepared to challenge them.

This is the reason why I compliment the authors of this text for rightly choosing a broad approach to addressing aviation security. Mr. Price and Dr. Forrest did a great service to worldwide aviation security by covering the subject in a very comprehensive manner, from the history of attacks against aviation to the detailed discussion of today's threats, from mitigation tactics to the different technological systems. The detailed discussion of different strategies from *profiling* to *everybody is equal* and various solutions that try to keep the system effective without jeopardizing the social values we try so hard to protect is a critical discussion. The reader will find all these issues well handled by the authors, and as a result be able to perform with greater understanding. This is the first time that interested readers can find a concise guide to aviation security. The industry requires this kind of book that will lead readers not only to a better understanding of this very complicated subject, but will also resolve many of the myths that surround aviation security.

Rafi Ron
CEO, New Age Security Solutions (NASS)/Director of Security
at Tel Aviv's Ben-Gurion International Airport (1997−2001)

Preface

The profession of aviation security continues to change by embracing new threats, challenges to security management, and adoption of new technologies, processes, policies, and legislation. In reflection of this dynamic, aviation security courses and professional development opportunities in aviation security have flourished globally. We both recall that in the few years following 9/11, many colleges and universities that had started aviation security courses were beginning to eliminate them from their curriculum. These cancellations were primarily attributed to a lack of expert derived course materials that could be used to support those classes. This is the principal reason we decided to write *Practical Aviation Security—Predicting and Preventing Future Threats*. This text, which is now entering its third edition, has been widely adopted by national academic intuitions, professional organizations, and security practitioners to meet the academic and professional needs of the domain of aviation security. Those using previous editions of this textbook will note significant changes in almost every chapter of the third edition.

As stated, our industry is highly dynamic and constantly challenged with new threats. In just the year prior to this publication, we witnessed several major attacks on aviation; for example, the (a) bombing of a Metrojet over Egypt, (b) hijacking of an EgyptAir flight, (c) takeover by a pilot of a Germanwings aircraft, who in an act of suicide and homicide crashed into the French Alps killing all on board, and (d) suicide bombing attack in the public area of the Brussels Airport. Additionally, the global proliferation of unmanned aerial vehicles (UAVs) is posing both new safety and a security hazards—demonstrated at the time of this writing, as one UAV recently hit a British Airways airliner. Nonetheless, UAVs convey the potential to improve security surveillance techniques, better emergency management situational awareness, and improved intelligence gathering. There were also several airport perimeter breaches since the second edition of this text, causing a demand for more focus on perimeter security at airports and the development of intrusion detection systems. Airport security managers are now administering more requirements as related to security credentialing and issuance of airport identification badges and control access to the airfield. In the third edition we have also continued to add to the history of aviation security incidents, which are important to remember and understand as we continue to manage future threats to security!

Increased focus on threats to aviation also include the militant group of the Islamic State of Iraq and Syria, the “radicalized” US citizen terrorist, and the “insider-threat” to the aviation industry. Although the insider-threat is not new to aviation, lawmakers have recently called for the total screening of all aviation workers as a result of the strong probability that a recent Metrojet bomb was placed by an inside aviation worker. Also, several airline employees were recently

caught in a weapons smuggling operation between Atlanta/Hartsfield International Airport and John F. Kennedy International Airport. Atlanta/Hartsfield adopted the new all employee or airport worker screening policy (Orlando International and Miami International are examples of airports that have been doing total employee screening for the past several years). While the decision has still not been made whether to require 100% employee and airport worker screenings at airports, the US Transportation Security Administration (TSA) and the industry are already moving forward with implementing "employee inspections," which varies from total screening, but may still provide the same level of protection and at a lower cost.

During the release of our last edition, the TSA was beginning to implement risk-based security (RBS). Today, the TSA's passenger Pre✓ (PreCheck) program is the primary method of RBS used by the TSA. PreCheck continues to grow, albeit much lower than the TSA had anticipated. The TSA also experienced challenges when an inspector general's "red team report" was released documenting a near 97% failure rate for their screeners to detect weapons and other prohibited items. Another similar report revealed that as many as 73 TSA employees were also on their active terrorist watch list! In partial response to these notifications, a new TSA administrator has been placed in charge. However, in the new administrators attempt to address the poor screening detection rates, passenger screening lines have slowed throughout the nation drawing the ire of airport directors and passengers. Tragically, the TSA also suffered the death of Gerardo Hernandez, a TSA agent at LAX, who was killed in the line of duty by an active shooter, on November 1, 2013. There have also been attempts to defund the Federal Flight Deck Officer (FFDO) program, along with the removal of the secondary flight deck protection barriers from airplane cockpits. These actions were sought, despite research that demonstrated that there is a significant reduction in the risks of being hijacked, when the FFDO and flight deck protection barriers are sustained.

A challenge to writing about airport security is doing it without providing critical information to your adversaries. However, we believe the potential benefits of sharing information and knowledge related to airport security with industry members outweighs this risk. We also think it would be a disservice not to help inform and educate industry about basic strategies for protecting its infrastructure and, more important, the traveling public. For these reasons, we decided that the goal for this text is to serve as a resource for those interested in gaining a better understanding of airport security and applying practical strategies to improve aviation security processes.

The basics of airport security—the practical strategies—are not difficult to comprehend. Indeed, it is probable that your adversaries are already familiar with most of the common airport and airline security strategies. This dilemma is similar to challenges faced by police agencies. For example, police departments might hesitate to share with the public information that could deter theft. In this example, police agencies may fear that by releasing this information, burglars will

better understand what defenses they need to overcome to commit a robbery. On the other hand, information shared by the police may help the public learn better ways to secure their property and potentially lower the risk of a robbery. We recognize that even with these strategies, criminals continue to seek ways to overcome various forms of security. That is why it is important for security experts to share new or improved methods for implementing security strategies. Planning and implementing airport and airline security procedures are constantly evolving, requiring continual long-term evaluation and implementation.

Even with the most current knowledge and security procedures, airports and airlines will remain threatened by criminal or terrorist activities. Perpetrators will consistently seek new paths to overcome security methods. We refer to this as pursuing a *strategy of least resistance* that the criminal or terrorist will exploit to accomplish the goals. This is an important premise for those concerned with airport and airline security. In this text, a history of air terrorism and related lessons learned will demonstrate that most attacks on aviation were and continue to be simple strategies developed by perpetrators to overcome established security methods with the least amount of effort.

In addition to the effect security procedures have on criminals or terrorists, the value of the perpetrator's goal or target will also affect where and how the perpetrator will strike. Aviation is a high-value target. It is the economic lifeblood of global commerce; global societies now depend on aviation to conduct business. Business travelers constitute a significant portion of the air-traveling public. Over the years since the attacks of 9/11, vacationers have returned to the skies as a primary mode for traveling to resort destinations, and there is strong demand for same-day or next-day delivery of high-value cargo. The reliability, safety, and security of air transportation are critical to global economies.

Industry professionals and others, such as the traveling public and the media, would prefer a "silver bullet" to address all aspects related to planning and implementing aviation-related security programs—especially airport security. The reality of aviation or airport security is that it is a highly dynamic and complex system of "layers of security" containing policies, strategies, tools, and processes. Each layer is designed to prevent, deter, or enable response to a particular attack or set of attacks. Providing layers of security is a well-established security strategy. In his book *America the Vulnerable*, Stephen Flynn (2004) described layered security as the constant application and evolution of multiple security measures designed to provide high levels of deterrence. Flynn also recommended that security measures should balance the probability of criminal activity in relation to the value of the target. In this regard, the more valuable the target, the more need for increased layers of security. The TSA commonly refers to these layers as "concentric rings of security." Airport and aircraft security managers must understand that a single layer of security will not be 100% effective in blocking criminal or terrorist activity. However, through proper planning and implementation, multiple layers of security initiatives may provide a probability of nearly 100% effectiveness against these threats. Therefore, we believe that each layer of security,

performed to its fullest level of effectiveness and combined with other layers of security, will result in the highest level of deterrence obtainable.

A major goal in aviation or airport security is that security agents should strive for maximum effectiveness in their area (layer) of responsibility. Essential to embracing this goal is an understanding by all personnel that attacks will probably occur regardless of how many layers of deterrence are in place and how effective those layers are. If the target or goal is sufficiently valuable, the criminal or terrorist[1] will continue to evaluate or attempt new strategies of least resistance to achieve their objectives.

Despite numerous security improvements implemented globally after the 9/11 attacks in the United States, criminals and terrorists continue to disrupt or destroy facets of the global aviation system. Terrorists view aviation as too valuable of a target to ignore. This is a grave realization when one considers that many in the industry argue that aviation security processes remain faulty, even when considering post-9/11 security-related initiatives.

Accepting the premise that attacks will continue to occur regardless of what we do is usually unacceptable. We do not argue that there should be acceptable losses and that we should continue to tolerate these losses. Rather, we believe losses will continue to occur regardless of the security system. As security advocates, we should design and implement practical and effective security measures to help mitigate or minimize these losses. These efforts are analogous to managing and enhancing safety in commercial aviation. Although occasional aircraft losses occur (as a result of pilot, maintenance, or manufacturing errors, as well as other causes), the industry strives to reach a "zero loss rate," while simultaneously acknowledging that the perpetual realization of this goal is unlikely.

Another precarious assumption made by some aviation security practitioners is to consider aviation security as being restricted to addressing acts of terrorism and therefore only focusing security efforts on preventing terrorist acts. The aviation security system must also address crimes against aviation and those using aviation to facilitate other forms of crime, such as drug trafficking, human trafficking, and the transportation of stolen property. Airports and airlines are businesses and experience crimes similar to those affecting nonaviation companies, such as employee theft, workplace violence, and cyber-threats. Airports and airlines are entities with a large general population passing through their facilities and onto aircraft every day. In this environment, there are numerous opportunities for criminals.

Many government agencies have offered various definitions for *terrorism*. However, law enforcement agencies and the US District Attorney's Office determine whether a particular act is a form of terrorism. For example, the attempted bombing of American Airlines Flight 63 by Richard Reid (the "shoe bomber") was considered an act of terrorism. In contrast, the shooting by a single

[1]We use the terms *crimes against aviation* and *criminal and terrorist acts* interchangeably with the commonly used phrase *acts of unlawful interference*.

perpetrator of three individuals waiting in line at the El Al ticket counter at Los Angeles International Airport in 2002 was considered under the criminal definition of murder (ie, not terrorism). The aviation security practitioner should not be distracted with whether the event she or he is trying to prevent is rooted in terrorism or criminal activity. Rather, the security practitioner should focus on developing and implementing practical systems, measures, and procedures to prevent all forms of attack and criminal activity.

As individuals concerned with aviation security, our primary goal should be to do everything possible to ensure that the layers of security for which we are responsible are effective. There is an old saying in military law enforcement: "Not on my watch." This adage implies that, as individuals, we are not in control of everything but do acknowledge our responsibilities for those factors we do control. In this spirit, we must routinely create and implement practical strategies for managing these factors in ways that continuously improve aviation security.

Practical Aviation Security—Predicting and Preventing Future Threats is a comprehensive reference for academicians and students, new and experienced aviation security practitioners, airport and airline administrators, government security personnel, and researchers. It is written by career professionals Jeffrey Price (MS) who is a well-recognized international aviation security practitioner and commercial pilot and Jeffrey Forrest (PhD) who has directed many research applications in aviation and aerospace science and is also a commercial pilot. Both Price and Forrest are also Professors of Aviation and Aerospace Science at Metropolitan State University of Denver, Colorado. We recognize that one cannot embark on such an endeavor, particularly within the fast-moving field of aviation security, without taking the risk that certain information will be out of date by the time the book reaches publication. To that end, we encourage you to visit the companion web site at http://www.leadingedgestrategies.com for updates and additional information on changes that have taken place in the ever-evolving aviation security industry.

Jeffrey C. Price and Jeffrey S. Forrest

Acknowledgments

This book would not have been possible without the contributions and sacrifices of the following individuals:

First and foremost, to our wives, Jennifer Price and Betsy Forrest for their understanding and all the extra work they endured (along with managing wildly swinging emotions) while we worked long days and late nights, for months on end. JP would also like to thank his kids, Austin, Alex, and Ashton, who again gave up precious "dad-time" and he hopes they one day understand his passion for making aviation safer and more secure. JP would also like to thank his parents, Zig and Dianne Price, who helped with a lot of the kid-duty and other life's essentials throughout this time, and for their overall support and love. A very special thanks goes to Dawn Escarcega and Megan Jones for manuscript preparation, initial copy edits and reviews, and various last-minute critical jobs—this book would not have happened without Dawn and Megan!

We would also like to thank our colleagues in the Aviation and Aerospace Science Department at Metropolitan State University of Denver for their support during the development of this edition. A special thank you is also extended to Dr. Sandra Haynes, Dean of the College of Professional Studies at MSU Denver for her patience and considerations as we expended many long hours on this project.

Thank you to Pam Chester from Butterworth-Heinemann for believing in this book from the very beginning; Hilary Carr and Sara Scott from Elsevier for their support, time, and patience; and Punithavathy Govindaradjane for your un-ending patience as our copy editor. We do not envy your job, and you are extraordinary at it.

We would like to thank those that contributed essays or other elements to this edition of the text: Joshua Ball, Lori Beckman, Ilana Brodesky, Dawn Escarcega, Pat Gannon, James Hiromasa, Kyle Konishi, Chris McLaughlin, Robert Olislagers, Jeanne Olivier, Rosemary Rizzo, Rafi Ron, and Bernard Wilson.

And many thanks to the following people who contributed their time and expertise to the first, second, or third editions of the text—in no particular order: Philip Baum, Jeanne Olivier, Lori Beckman, Mark Nagel, Brad Dalton, Teakoe Coleman, Sean Broderick, Barbara Cook, Colleen Chamberlin, Carter Morris, Sarah Pilli, Spencer Dickerson, and the staff at the American Association of Airport Executives, John Duvall, Bernie Wilson (again!), Michelle Freadman, Carrie Harmon, Robert Olislagers, Joram Bobasch, Mike Pilgrim, Norm Dawkin, Rafi Ron, Rob Hackman, Rob Rottman, Tim Barth, Tom Kinton, James Simmons, Jennifer Caine, Steve Davis, Lynne Gunter, Craig Williams, Tanya Sweeney, Huw Farmer, James Hiromasa, Dennis Treece, Al Graser, John Costigan, Nahum Liss, Anthony Robbins, Chuck Burke, Charlotte Bryan, Yael Liberman, Eran Sala, Jim Slevin, Cathleen Berrick, Tinamarie Seyfer, Gerry

Berry, Gary Smedlie, James Henderson, Rick Nelson, Michal Morgan, Wesley Fue, Pat Alhstrom, Dave Bassett, Al Meyers, Lynne Georold, Deven Smith, Brad Westoff, Duane McGray, Christopher L. McLaughlin, Doug Hofsass, Chuck Guffey, Martin Daniels, and J. David Rigsby. Sincere appreciation also goes to the Air Line Pilots Association, and all the attendees of the Airport Security Coordinator and Airport Certified Employee-Security courses that I have conducted over the many years, and from whom I have learned so much.

Jeffrey C. Price and Jeffrey S. Forrest

CHAPTER

Overview of the aviation industry and security in the post-9/11 world

1

OBJECTIVES

This chapter provides an overview of the national aviation system and an introduction to the development and environment of aviation security since the September 11, 2001 (9/11), terrorist attacks. Readers gain insight to the national aviation system and its importance to society. A fundamental framework describing the roles of airports, aircraft operators, and regulatory agencies involved in sustaining effective aviation security is presented. Fundamental to modern aviation security strategies and methods are lessons learned from the 9/11 attacks. Aviation security practitioners and students of aviation security should have at least an elementary understanding of the circumstances surrounding 9/11. Therefore, a case study describing the events of 9/11 and integrating concerns of aviation security is also provided.

INTRODUCTION

Despite other targets, terrorists remain fascinated with aviation. Throughout most of the history of aviation, terrorists and criminals have used aircraft and airports to conduct many forms of unlawful activity. Examples include special-interest groups or terrorists using aviation to gain geopolitical attention and criminals using commercial aviation or general aviation (GA) to smuggle drugs, weapons, cash, and stolen goods. In these cases, aviation has provided a public stage for the former and an expedient distribution channel for the latter. Aviation is essential to sustaining the economic viability of world commerce, the movement of people and cargo, and the flow of information and knowledge throughout society. Therefore, those responsible for protecting the aviation industry must be proactive in developing and implementing strategic and tactical systems that are effective in mitigating criminal and terrorist activity. Since the terrorist threat is always evolving, aviation professionals must be proactive in predicting future threats.

The aviation industry is composed of a series of overlapping operational areas or a "systems of systems" that security personnel must protect. Examples include the management of passenger needs, such as parking, baggage check-in, and screening (Fig. 1.1), along with other requirements, such as health concerns or

Practical Aviation Security. DOI: http://dx.doi.org/10.1016/B978-0-12-804293-9.00001-1

FIGURE 1.1

Passengers go through security screening at Denver International Airport.

guarding secured areas. Those responsible for each area must work in harmony to maintain aviation as an effective form of global transportation. Evaluating effectiveness in aviation security requires a variety of methods—from ratios used to develop metrics measuring baggage throughput or passenger flow, to extensive security evaluations conducted by various government agencies and private corporations.

Aviation is an effective and efficient mode of transportation affecting worldwide social and economic stability. In a little over 100 years, aviation has completely changed the way people travel around the planet. The entire world is now reachable in a matter of hours, and the miracles of today's world would not be possible without aviation. In the IMAX movie, *Living in the Age of Airplanes*, narrator Harrison Ford says: "What was once a migration, is now a vacation." As a symbol of modern commerce and prosperity, aviation is a highly desirable target to terrorists and criminals.

The ability of aviation to move people and property faster than competing forms of transportation is essential to its economic viability. The Internet and related technologies such as videoconferencing and telecommuting provide additional options to transport information, knowledge, products, and services. The advantage aviation has over rail, trucking, and watercraft is speed, whereas its advantage over videoconferencing is that people generally prefer face-to-face communication.

Shortly after the terrorist attacks of 9/11, it was thought that if there was another major terrorist attack on aviation, travelers would shift modes to different forms of connecting, such as videoconferencing. While that has yet to occur, sustained criminal or terrorist activity on aviation often causes a temporary shift in passenger demand from airline travel, of which business travel is a significant percentage, to alternate forms of interaction or travel, such as videoconferencing or traveling via privately owned or chartered aircraft. These changes in demand for transporting people, cargo, or information could present airlines with serious economic challenges. Had several additionally planned terrorist attacks, such as the shoe bomber in 2001, the liquid bomb plot in 2006, and the underwear bomber attempt in 2009, been carried out, more people might switch to alternate forms of connecting, at least until their confidence in the system is restored.

If business travelers switch to alternate modes of travel, commercial airlines will have to increase the cost of tickets to those passengers (usually leisure travelers) who cannot afford business rates. As costs increase, leisure travelers may not be able to afford air travel, resulting in more "staycations," which do not require air travel. Airlines would then have to raise prices to compensate, as more leisure flyers switch to ground transportation. Additionally, many industries, such as the hotel, rental, and tourist industries, rely heavily on air transportation for their businesses to be successful. Repeated attacks on aviation could lead to a significant restructuring of commercial aviation.

THE COST OF FAILING TO PROTECT AVIATION AND THE IMPORTANCE OF THREAT RESPONSE

Despite its complex nature, the aviation industry's primary infrastructure consists of aircraft operations, airports, and supporting agencies. Many types of aircraft are used in various operations around the world. These operations are commonly categorized as commercial service, private operations (categorized as GA), and military operations. Airports are usually categorized as commercial service, GA, private, or military.

The terrorist attacks in the United States on September 11, 2001 (9/11) were designed to damage global security and the US economy—an economy reliant on aviation. A critical strategy for responding to terrorist threats is to moderate the response to not cause further deterioration to the economy or stability of a society. Terrorist organizations understand that they usually do not have the forces or resources to defeat an enemy in a traditional military conflict. Therefore, terrorists operate more indirectly, striking in ways that cause targeted countries or societies to incur loss of life, economic damage, changes in policies, or other effects. These attacks are usually designed with the hope that countries or societies overreact in ways that further diminish the ability to protect or sustain safety and economic viability. Terrorists also know that with each subsequent attack, the targeted populace

gives up more of its freedom through changes in laws and policies or by accepting that intrusion into private lives is unavoidable and required. In these ways, terrorists cause economic and social degradation within nations and societies.

Terrorism has additional effects beyond the initial loss of life and property. The direct economic effects of the 9/11 attacks showed a financial loss of $190 billion dollars (Mueller and Stewart, 2016, pp. 275–276), but other, less direct impacts occurred. As a lasting effect of 9/11, large amounts of resources were committed to secure the production, distribution, communication, and financing industries from terrorist attack (Makinen, 2002, CRS-2), as well as to secure the US aviation system.

Another concern after 9/11 was the increased price of oil. However, oil prices spiked only briefly before returning to relatively normal prices, at least until 2008. Additional concerns resulting from 9/11 also affected US trade partners, especially Canada, Mexico, and Japan. Numerous businesses, including financial institutions, insurance companies, commercial banks, pension funds, and stock exchanges, were also affected by the attacks. Also directly affected was the destruction of the World Trade Centers (WTCs), shattering the leading dealer in US Treasury securities, Cantor Fitzgerald including the loss of their staff, who accounted for almost one-quarter of all those killed in the WTC attacks. The grounding of all aircraft also created a financial impact, as the clearing of checks and the distribution of paper currency were hampered (Makinen, 2002, CRS-2).

US airlines were already experiencing financial problems leading to the US Congress approving an aid package worth over $5 billion in short-term assistance and $10 billion loan guarantees. The insurance industry experienced a loss of an estimated $40 billion, and while the insurance industries had the capital to cover the costs at the time, they may not be able to if devastating attacks continue. The impacts of 9/11 on the agriculture and food industry were minor setbacks in the commodities market; however, the subsequent Anthrax attacks resulted in the passage of new laws to reduce the industries vulnerability to bioterrorism. Also, nearly 1800 businesses were disrupted, relocated, or destroyed as a result of the attacks, and 462 mass layoffs displaced 130,000 employees. In New York City (NYC), the destruction of the WTC towers and nearby businesses had a major impact on the Gross City Product (GCP) of NYC, reducing the GCP by approximately 27.3 billion and tax losses as a result of the attacks, reducing city tax revenues by over $2 billion in fiscal 2002 and another $1 billion in fiscal 2003 (Makinen, 2002, CRS-5 and 6). In addition to appropriate responses to terrorist or criminal attacks, those charged with protecting aviation must ensure that strategies and technologies remain current and viable for defending against new threats. Security practitioners employing outdated strategies and tactics create opportunities for terrorists to use these systems to their advantage. For instance, the 9/11 attacks showed ingenuity and were organized using modern technologies (eg, the Internet) to defeat what was essentially at the time, a 1970s aviation security system.

Flawed management in designing and implementing modern security systems can also create opportunity for criminals or terrorists. For example, industry is responding to terrorism by investing billions of dollars in research and

development for improved explosives detection equipment. Of concern is that much of this technology has not undergone extensive testing before deployment. Although technologies used in various explosives detection equipment[1] are mostly valid, the *mean time before failure (MTBF)* for these technologies is often low when used in a non-airport environment. As an example, the deployment of the thermal desorption unit proved to be ineffective when the units were not resilient enough to handle the airport environment. Many early-model explosive detection devices were not designed or tested to sustain the day-to-day usage at commercial service airport screening checkpoints. The industry is still catching up in developing other security strategies, such as employee security awareness and passenger profiling—strategies that other nations have used since the 1980s—and, perhaps most critically, the ability of our intelligence agencies to penetrate groups that represent credible threats. The increased focus on tracking and either arresting or eliminating known threats, such as the attack on and subsequent death of Osama bin Laden and Anwar al-Awlaki, have weakened one of aviation's primary enemies, al-Qaeda, but others, such as ISIS/ISIL have taken their place.

In response to the challenges in aviation security, the US National 9/11 Commission on Terrorist Attacks upon the United States (the 9/11 Commission)[2] and other security and policy experts developed and recommended strategies that should be effectively and efficiently implemented. However, implementing new aviation security methods has traditionally been reactive rather than proactive. Those charged with protecting the aviation industry must adopt a philosophy of sustained proactive improvement. Therefore, aviation security practitioners must not stop moving forward in implementing proactive forms of security—our foes are committed to their cause and we must be exceedingly committed to ours, but we must also not ignore existing and successful strategies to attack aviation, or else terrorists and criminals will continue to exploit identified weaknesses until the method of attack is no longer successful.

Although time is of the essence in commerce, it is critical in the aviation industry. Passengers must travel safely and efficiently. However, reasonable compromises must be made for the system to continue functioning. A terrorist attack may be devastating and certainly tragic. Nevertheless, it would be even more tragic to allow such an attack to cause further economic and social damage by impeding global aviation. Resiliency: the ability of a security system to appropriately respond and quickly recover is a fundamental principle in planning and managing aviation security systems.

[1]For example, a gas chromatograph or a programmed thermal desorption unit.

[2]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 September 11, 2001, terrorist attacks, including preparedness for and the immediate response to the attacks'. The Commission is also mandated to provide recommendations designed to guard against future attacks" (see www.9-11commission.gov).

FIGURE 1.2

Aviation security embraces the protection of passengers, airports, airlines, and the national aviation system.

As discussed, aviation is vital to the survival and growth of the world's economy (Fig. 1.2). Aviation is also a symbol of prosperity and stability among societies. An essential responsibility of those charged with protecting aviation is to balance responses to threats with the requirement to facilitate safe, secure, and efficient transportation of passengers.

AVIATION ECONOMICS

Airports are the closest object to a time portal to the rest of the world. Walking, driving, or moving by rail can take days or weeks, to cover the distances that aviation covers in hours. US air carriers transport an estimated 800 million passengers and over 61 billion tons of freight every year. Expenditures from passenger spending during air travel are estimated at over $260 million annually, and civil aircraft manufacturing continues to be the top net exporter in the United States with a positive trade balance of $54 billion (FAA, 2014, p. 4). According to a study by the Federal Aviation Administration (FAA), civil aviation accounts for $1.5 trillion in total economic activity, supports 11.8 million jobs, and contributes to 5.4% of the nation's Gross Domestic Product (FAA, 2014, p. 5).

Aviation's economic effect is not only to the industry itself. While primary impacts of aviation include air transportation and supporting services, travel and other trip-related expenditures by passengers, secondary impacts include the results of expenditures to supporting businesses and entities, and the spending by direct and indirect (hotel, restaurant, ground transportation, etc.) employees (FAA, 2014, p. 8). Commercial aviation accounts for the majority of civil aviation's economic contribution, with operations generating $373 billion in total output (as calculated by earnings, output—the value of goods and services produced, and jobs that are directly or indirectly related to the industry). When airline passengers reach their destinations, they spend money to the tune of over $671 billion on hotels, rental cars, and entertainment.

Despite the setbacks on 9/11, the airline industry is growing at nearly double the growth rate of the US economy (FAA, 2014, p. 14). In several measurable categories, including output, earnings, and job growth, aviation continues to grow in both the commercial aviation and GA sectors (FAA, 2014, p. 14). The introduction of commercial space and commercial, government, and recreational drone operations is likely to continue to increase these numbers.

GA aircraft operations account for nearly $79 billion in total annual output (FAA, 2014, p. 8), just from an operational perspective that does not including multiplier and other factors. Taking into account induced activity, GA generates more than $150 billion in economic activity on an annual basis and employs more than 1.2 million people (General Aviation Manufacturers Association, 2013). Sixty-five percent of all GA flights are conducted for business or personal services that the airlines cannot offer in terms of flexibility, services, and access. Commercial airlines are restricted to the estimated 450 commercial service airports in the United States, with the majority of flights going to only 70 major airports (National Business Aviation Association, 2014), whereas GA can access the slightly more than 5000 GA airports, not to mention additional airports throughout the world (Aircraft Owners and Pilots Association, n.d.).

The United States is geographically (and socially) oriented to rely on air travel. Unlike many countries with well-organized systems that enable efficient travel internally and internationally by rail (and thus have less of a need for air travel), the United States has no national high-speed railway system. Additionally, the United States shares borders with Canada and Mexico only, further limiting opportunities for international commerce by land. As a result, the United States relies on air travel to enable commerce with the rest of the world.

Although most of the world's freight still moves via sea, the demand of *just-in-time* goods delivery is increasing. The primary advantages of just-in-time shipping are that it allows for shorter production and development cycles and eliminates excessive inventory. Aviation is the primary means for economic growth with a significant influence on the quality of life of populations around the globe, often bringing food and relief, such as medical supplies and equipment to rebuild after disasters or other tragedies. Aviation facilitates the world economy and promotes the international exchange of people, products,

investment, and ideas. Indeed, to a large extent, civil aviation has enabled small community and rural populations to enter the mainstream of global commerce by linking such communities with worldwide population, manufacturing, and cultural centers.

The impact of 9/11 on the aviation industry was devastating. Overall, the aviation industry experienced direct losses of $330 million per day (Kumar et al., 2003). In addition to the direct loss of revenue, airlines and airports had to bear an increased cost of doing business to meet government-mandated security improvements. The costs to airports of purchasing new security technology and reconfiguring terminals to accept the larger security screening devices have caused airport operators to shift money from other airport capital improvement projects, such as runway and taxiway maintenance and expansion, to security measures. Additionally, airport operators lost revenue-producing space to accommodate new Transportation Security Administration (TSA) equipment and personnel, and with the deployment of advanced imaging technology, the so-called "body imagers," airports have had to sacrifice even more space to make way for larger equipment and longer passenger screening lines.

The national airspace system is both economically and operationally fragile. A delay of 10 minutes can cost the airport and airlines significant money. Gate assignments at airports are often scheduled back to back, meaning that if one flight does not depart on time, the next flight will probably also depart late. This domino effect influences many operational considerations.

Airline flight delays significantly encumber the US air travel system and cost the airlines, passengers, and society billions of dollars each year. In 1 year alone, 2007, delays cost the airlines $8.3 billion dollars (increased expenses for fuel, crew, and maintenance); delays cost passengers $16.7 billion dollars from lost time due to delayed flights, cancellations, and missed connections, and the costs from lost demand[3] was calculated at $3.9 billion dollars, for a total of $32.9 billion in costs due to delays (Ball et al., 2010, p. vii). Weather and air-traffic-related delays are responsible for many flight delays, along with aircraft delayed due to having to wait for previously delayed aircraft (Ball et al., 2010, p. 1). However, while weather can be predicted to a certain extent, giving airlines enough time to reposition flights away from the storm, and rebook passengers in anticipation of delays and cancellations, and many air traffic delays currently in the system are supposed to improve with the integration of the Next Generation of Air Traffic Control (NextGen), a delay due to a security issue, by comparison, has a significant impact on the system. Security-related delays such as bomb threats, unruly passengers, or the massive shut down of the US aviation system on 9/11 can send costs into the billons and have ripple effects throughout the system that can last for days or weeks.

Commercial aviation is composed of a myriad of coupled systems (Fig. 1.3). When one part is affected, it forces change in many of the other systems. When

[3]Lost demand is an estimated cost associated with passengers who avoid air travel due to delays.

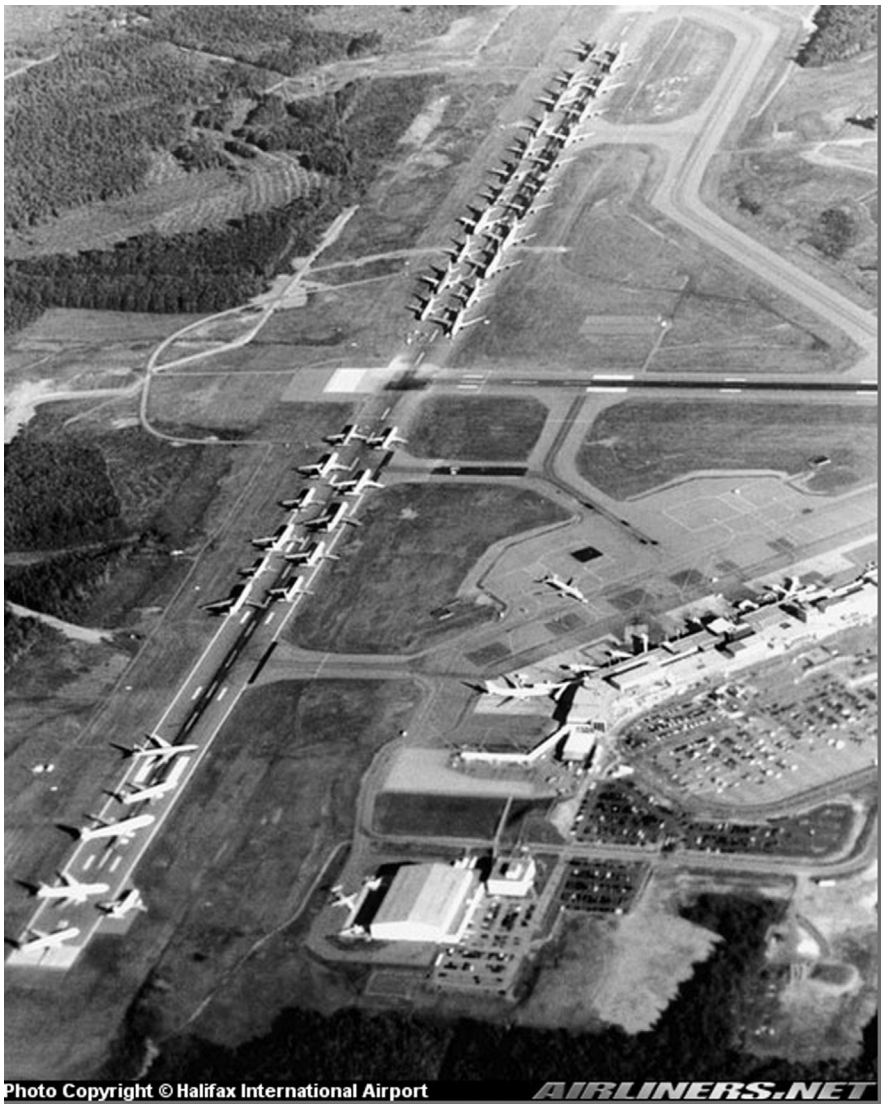

FIGURE 1.3

Dozens of aircraft are stranded in Halifax, Nova Scotia, during the shutdown of the US aviation system on 9/11.

airport flight operations shut down because of weather or aircraft have to be rerouted around bad weather, the entire national airspace system is impacted. When compared to criminal activity or terrorism, weather is relatively predictable and airport operators know how to adjust operations for the kinds of

weather in their region. More important, weather (with few exceptions) does not generally destroy essential components of the airport and scare the public from travel, as tends to happen with a terrorist attack.

The importance of protecting aviation as a driver of the global economy is clear. However, the various systems used to protect aviation can impede aviation's efficiencies. Security managers must balance their efforts to protect lives and infrastructure with policies and methods that enable aviation to provide commerce with efficient and reliable service. The goal in aviation security is to make security fit into aviation, not aviation fit into security. Efforts to change aviation operational practices to improve security effectiveness result in reducing the benefits of aviation.

AVIATION SECURITY FUNDING

A significant issue in aviation security is a reliable source to fund the elements of the system that must be implemented to consistently protect the system, while continually seeking additional funds to stop developing threats. The International Civil Aviation Organization (ICAO; see www.icao.int) recommends a reliable and consistent stream of monies to fund aviation security improvements and operations worldwide. In the United States, most commercial service airports receive revenue from multiple sources as outlined previously, and part of these monies fund aviation security at airports.

US airports spend billions of dollars to implement new security regulations. Airport operators have also had Airport Improvement Program (AIP) funding, usually earmarked for runway and facility improvements and upkeep, redirected toward security projects. This financial burden creates a situation where airport operators must sometimes decide between safety- or security-related projects. Local FAA airport district offices (ADOs) play a critical role in deciding which airports in each state are allocated federal funding. Some airports receive money through entitlement programs that designate specific funding regardless of capital improvement needs, and an airport listed in the National Plan of Integrated Airport Systems (NPIASs) is eligible for federal *discretionary funding*, an appropriation of federal dollars based on the discretion of the ADO. A complex planning process precedes the apportionment of discretionary monies, often involving airport operators, the state, the federal government, and the FAA. Since the FAA is now effectively out of the security business, but still controls the AIP revenue stream, some airport operators have complained that money is less available for security-related projects than for safety and airport development. The TSA does not have a federal apportionment through a trust fund, the way the FAA does, to provide money to airports for security improvements and technologies. Airport operators who use AIP funds have to balance the costs of security upgrades with other, capital-improvement projects that are often necessary for airfield safety and critical maintenance issues.

Many airports also receive capital monies through their state aviation offices, which may collect a percentage of receipts on aviation fuel sold within the state. State aviation/aeronautical offices work with the airports to coordinate 5- or 6-year capital improvement programs and then decide which airports in the state should receive the funds (in addition to federal AIP funding). Some states participate in the Code of Federal Regulations (CFR) Part 156 State Block Grant Program (see http://edocket.access.gpo.gov/cfr_2003/pdf/14cfr156.3.pdf). The Block Grant Program states have the sole responsibility for deciding the distribution of federal funds for improvement projects at GA and nonprimary (ie, very small) commercial service airports.

An important issue for airport operators has been the acquisition of explosive detection equipment and other federally mandated security upgrades. When a new explosive detection system (EDS) machine is installed for checked-baggage screening, the unit cost of the machine is not the only cost incurred. Facilities must often be redesigned to accommodate the additional weight and space of new detection equipment, and power requirements must be considered along with MTBF maintenance requirements. Since the initial deployment of these machines in the years following 9/11, airport operators are experiencing an entirely new dynamic as the machines are reaching their maximum effective operating life and must be replaced.

Aircraft operators have also been affected by aviation security mandates. For example, the required reinforcement of cockpit doors not only increases costs but also adds weight to the plane, thereby reducing the capacity for revenue-generating cargo and passengers. As a result, funding for aviation security requirements is now a significant part of airport and airline operating and capital budgets.

AIRCRAFT OPERATIONS: AN OVERVIEW

Aircraft operations encompass a wide range of flying categories—from personal travel and military flight to scheduled commercial airlines. An airline's purpose is to move people and goods from one place to another, safely and securely, while still making a profit. Airlines carry people, mail, and cargo and are essential to the US economy. Airlines also offer a variety of services, including private charter operations, carrying sports teams and rock stars (Fig. 1.4).

Aircraft operations are generally classified as commercial service, GA, or military operations. Regardless of the aircraft type, all aircraft may be used for each of these types of operations. The Boeing 737, for example, though most frequently used commercially for airlines, is also used by the military to train navigators, as well as by the private sector as a business jet. If aircraft are used in a commercial capacity for the transportation of passengers and cargo for pay, these operations are commonly referred to as *commercial aviation*.

Individuals or companies can use an aircraft owned by the company or rent an aircraft to facilitate business. For example, a salesperson may use his or her

FIGURE 1.4

A Ted B757 at the Las Vegas McCarron International Airport, one of the busiest airports in the world.

privately owned airplane to service accounts. These types of operations are GA. However, if the salesperson takes a passenger and charges a fee, it is now commercial aviation even though both operations use the same aircraft. These brief examples should highlight that an aircraft operation is determined by how an aircraft is used, not by the appearance or design of the aircraft.

Fig. 1.5 shows three aircraft—a Cessna 182 (foreground) used in flight training, a Cessna Citation used for business travel and charter operations, and a Boeing Business Jet (BBJ) used for private transportation by large corporations. The BBJ design is based on the Boeing 737 airframe and can easily be confused as a commercial airliner. It is not always possible through visual examination to determine whether an aircraft is being used for private transportation, as part of a public charter, or in commercial transportation. It is important to understand how an aircraft is being used, as various security measures are applied depending on the type of flight operation conducted.

Commercial service operations involve using aircraft to generate a profit. These are subclassified into scheduled service (the most common being airline operations) and public and private charter flights. *Scheduled aircraft operations* are similar to scheduled bus or train services; a person pays to occupy space or a seat for the purpose of transportation and schedules are published so the public

FIGURE 1.5

Cessna 182, Cessna Citation, and BBJ, each representing different types of aircraft used in general and commercial aviation, at Rocky Mountain Metropolitan Airport, CO, 2006.

can select which schedule most accommodates their needs. The company (an aircraft operator) provides the scheduled service to make a profit. In comparison, *public charter* also seeks a profit by offering transportation to the client, but departure and arrival times vary and are often based on client needs and the availability and capability of the aircraft. Public charters are often conducted using a scheduled-service air-carrier aircraft, which is leased to a private entity, such as a travel destination company. Passengers pay the travel or resort company a fee for the entire vacation package, of which the airfare is included, but the aircraft is not owned by the travel company. *Private charter* is analogous to renting a limousine in that the customer has purchased the exclusive use of the entire vehicle. In private charter, the purchaser pays for the right to his or her own transportation, to bring additional passengers or cargo, and to decide on the departure or arrival times.

Private operations are part of GA and may involve using an aircraft personally or as part of a business enterprise. In GA operations, aircraft are not *directly* used to generate profit but may enhance business opportunity as an efficient form of transportation. GA operations also include flight training, agricultural flying, soaring, experimental aircraft, and recreational flying—to name a few.

Military operations use aircraft to meet various needs specified by national governments. Military aircraft do not usually facilitate public or business transportation or generate profit, however, military aircraft frequently operate from commercial airports. In the following sections, we will focus on the most well-known type of aircraft operation: the commercial airline.

AIRLINE MANAGEMENT

Airline organizational structures vary depending on the size and history of the airline, its route structure (domestic or international), and the type of aircraft (regional or long haul). Air carriers are profit-making organizations typically owned by stockholders. The stockholders elect a board of directors, which designates a chairperson and outlines the goals and objectives for the airline. The board hires an administrative manager, a president, responsible for setting major policies and ultimately for the airline's success (Kane, 1998).

Within top-level airline management is the *aircraft operator security coordinator* (AOSC) who is the airline's key contact with the US TSA, the US Federal Bureau of Investigation (FBI), and other federal agencies. The AOSC oversees the implementation of security practices throughout the airline. Commercial service operators are regulated under US Transportation Security Regulations (TSRs; Title 49 CFR Part 1544).[4] US airlines must also adhere to the requirements in the *Aircraft Operator Standard Security Program*, a federally drafted document that outlines the practices airlines must follow to adhere to federal regulations.

An airline operations department is essential for managing effectiveness and efficiency. The operations department is responsible for delivering service to those demanding transportation or shipment of cargo. Within operations are the flight and ground operations departments. Flight and ground operations interact with the AOSC daily. The flight operations department is responsible for air carrier fleet safety, security, and efficiency. *Flight operations* consist of pilots, flight attendants, and dispatchers. Pilots directly operate the aircraft, whereas flight attendants provide essential safety and customer services on board the aircraft. Dispatchers generate the data needed before the flight, including weight and balance, weather, and safety and security information, and communicate with the pilots on company communication channels in flight. The *ground operations department* is responsible for maintenance and servicing of the aircraft. Through the ground operations department, the airline's ground security coordinators work with the flight department to disseminate pertinent security information.

[4]The TSA issues and administers TSRs, codified in Title 49 of the CFR, Chapter XII, parts 1500–1699.

AIRLINE ECONOMICS

Throughout the 1990s and into the 2000s, airlines operated on minimal profit margins, averaging from 1% to 2% compared to a US industry average of 5% (Kane, 1998, p. 413).[5] Airline revenues are seasonal, with most air travel occurring in the summer. Although more than 60% of air travelers fly for personal reasons, the majority of passenger revenue for many airlines comes from the 26% of those who are frequent business travelers. The number of airline operations also fluctuates throughout the day, with most travelers flying before 10:00 am or after 4:00 pm. The nature of passenger flow through an airport, based on time of day and time of year, relates directly to staffing security personnel and deploying required security-related equipment (Kane, 1998). However, the International Air Transport Association (IATA), a trade group for the airline industry, reported in 2015 that the industry would achieve a 4.0% profit margin, attributing the increase to a stronger global economy, record load factors, lower fuel prices and an appreciation of the US dollar (IATA, 2016). Despite the fact that US airline collected $6.16 billion in bag and reservation change fees in 2013 (Hetter, 2014), it still does not add up to more than an average profit of $8.27 for every passenger that boards a flight (Adamczyk, 2015).

The US airline industry has high capital and labor costs. Most airline equipment is financed through loans or stock rather than purchased. Airlines must generate a high cash flow to repay debt, buy fuel, service aircraft lease payments, and perform other operating expenses. More than a third of an airline's revenue is allocated to labor, with many airline workers unionized. As such, labor costs are among the highest of any industry. Airlines employ many highly specialized personnel including (Kane, 1998):

1. Pilots
2. Flight attendants
3. Reservation, ticket, gate, and cargo agents
4. Security personnel
5. Cooks
6. Administrative assistants
7. Revenue planners
8. Schedulers and dispatchers
9. Accountants
10. Lawyers
11. Human resource managers
12. Aircraft cleaners
13. Baggage handlers

[5]For a complete description of the financial measurements used in airline operations, see Kane (1998).

Airline bankruptcies are common. Airline profitability is often evaluated by the *load factor*, which is derived by dividing the number of seats generating revenue by the airline's available seats. On average, an airline needs to fill 70–80%[6] of its available seats on each flight (depending on the airline's particular expense structure) to generate a profit on that trip. The difference of just one or two seats filled by paying customers can be critical to an airline's ability to make a profit on a flight.

The cost of moving a passenger from point A to point B is often determined by calculating the cost per *revenue seat mile*. The cost per revenue seat mile represents the average cost to fly one full-fare-paying passenger occupying one seat a distance of one mile. For the "legacy carriers"[7] (eg, United Airlines, Delta, American Airlines, US Airways), this could be $0.10–0.14 per seat mile. In comparison, the costs for low-cost or discount air carriers (eg, Frontier Airlines, Southwest Airlines) range slightly less per seat mile. Factors contributing to higher costs include employee salaries, pensions, maintenance, in-flight food, airline ticket taxes, and the cost of aviation fuel.[8] An example of an airline cost factor related to security is a fee commercial-airline passengers pay as mandated in the Aviation and Transportation Security Act of 2001 (ATSA, 2001).

Airline cost structures are complex. Each airline monitors the rates of its competitors. When an airline increases its rates, other airlines may not increase theirs. By not responding with a rate increase, these airlines wait to see if the competing airline will lose profitability by increasing its fares, as there is usually an inverse correlation between airline ticket prices and passenger load factors. For example, if the cost of jet fuel increases and an airline raises its fares to compensate, other airline revenue managers may keep fares low (even with the same increased costs) in the hope that their own airlines will see higher load factors to make up for the higher fuel costs (Kane, 1998).

In relation to aviation security, if airlines raise fares to cover costs associated with new security requirements, then passenger load factors may also decrease. Because of small profit margins, the airline industry is watchful of security practices that may increase costs. In an attempt to help mitigate the impact of security concerns on cost, the ATSA 2001 created the *Registered Traveler Program*, designed to accommodate frequent airline travelers (usually business travelers) with a personal identity system, enabling those passengers rapid passage through airport screening.

The airline industry is sensitive to the fluctuations of the national economy. When the national economy declines, both business and leisure travel drop. This impact was discussed at an aviation security conference hosted by the American Association of Airport Executives (AAAE) (Fig. 1.6) in December 2001. At the

[6]These figures are dynamic, especially during periods of rapidly escalating fuel prices.

[7]Legacy carriers are commonly described as large airlines operating out of *hub-and-spoke* airports. A hub-and-spoke airport is usually a large airport that serves as a connecting hub for indirect flights to smaller airports.

[8]With the cost of fuel spiking to record levels in 2008, airlines have had to heavily revise their cost structures to make up for the added fuel expense.

FIGURE 1.6

Logo of the AAAE, the nation's largest airport management trade association.

conference, some participants warned that future attacks on aviation could trigger a "mode shift" to increased videoconferencing and online meetings. This shift in demand would affect not only airlines but hotel operators, rental car agencies, and airport financial models.

Functions within an airline have a tremendous interdependence; all departments are interrelated. When one component is impacted, the effects reverberate throughout the organization. For instance, when a flight is canceled or significantly delayed because of a bomb threat, many of the other flights for that airline are also affected. If flights were delayed or canceled each time a threat was issued (eg, phone or social media such as Twitter), one individual could call or Tweet several airlines and shut down the US aviation system. For this reason, bomb threats are vetted as thoroughly as possible before canceling or delaying a flight.

The national aviation airline route system is also highly sensitive—flight delays of just a few minutes can resound across the nation, multiplying the delay time for subsequent flights and even causing cancellations. Weather delays and temporary airport closures caused by security breaches can trigger the cancellation of dozens and sometimes hundreds of flights. A security breach at an airport can also have an economic impact by disrupting aviation operations. Approximately 40 million passengers a year pass through Denver International Airport (DIA). If an individual accidentally (without criminal intent) breaches security by entering a concourse without proper screening, the airport must temporarily close while the concourse is evacuated. In such a case, it takes security and other airport and airline personnel around 2 hours to conduct a *re-sterilization* procedure, which encompasses a search for the individual breaching security and any prohibited items he or she may have brought into secure areas. A major impact of a security breach is rerouting inbound

aircraft. This backs up aircraft movements across the country and may even affect inbound international flights. If an airport cannot accept an aircraft because of a security breach, the plane is held on the ground at its departure airport, slowed down en route, or placed into a costly holding pattern. During a breach, outbound aircraft are grounded and often evacuated and searched.

Approximately 800 commercial aircraft depart from DIA every day, and the average cost of a one-way flight is approximated at about $12,600 (depending on numerous variables—some costs can be as high as $23,000 or more for an intercontinental flight, or lower for regional aircraft operations). This cost represents the total average cost for the airline to fly an airplane from departure to destination. Using these numbers, the economic impact of a breach in security can be shown in the following example. A security breach occurs at noon, and concourse evacuation and resterilization begins. At least 390 flights are already affected, placing more than $4.9 million of revenue at risk. Assuming successful resterilization and the perpetrator is either found or the Federal Security Director determines there is no risk to reopening the airport, all flights resume with at least a 2-hour delay. If only half the original flights are canceled, the airport recognizes a net loss of $2.5 million. Across the United States, other airports are affected. By 5:00 pm, an additional 200 flights out of Chicago are affected, and by 9:00 pm, 800 total flights across the United States are affected.

Resterilization procedures result in long security screening lines, upset travelers, and lost revenue. There is also a loss of productivity as airport and airline personnel are called away from their primary job duties to assist in the resterilization process. Of course, the airlines lose significant revenue when security breaches occur.

AIRPORTS: AN OVERVIEW

Excluding military airports, approximately 20,000 GA, private, and commercial service airports operate in the United States. About 420 of these airports are classified by the FAA as commercial service but also host GA operations. Nearly 6000 airports are GA airports with approximately 300 of those hosting occasional small commercial service operations (Fig. 1.7). The remaining 11,000-plus airports are private airstrips scattered throughout the United States.

Airports support and provide a conduit to transportation. They also serve society in other ways. Sam Hoerter (2001), author of *The Airport Management Primer*, describes an airport as:

> *. . . a place where federal airspace and local roadways intersect. Think of it as a place where public infrastructure and private investment intersect. Think of an airport as a place where buyers and sellers meet in an open and ever-changing marketplace. In other words, think of it as a place forever caught between different worlds. Consequently, airport management requires a continuous effort to seek a balance among many competing forces. (p. 9)*

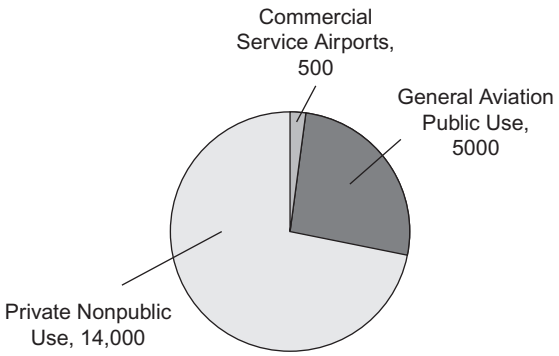

FIGURE 1.7

Approximate proportions of commercial service, GA, and private airports within the United States.

Airport Classifications		Hub Type: Percentage of Annual Passenger Boardings	Common Name
Commercial Service: Publicly owned airports that have at least 2500 passenger boardings each calendar year and receive scheduled passenger service **§47102(7)**	**Primary:** Have more than 10,000 passenger boardings each year **§47102(11)**	**Large:** 1% or more	**Large Hub**
		Medium: At least 0.25% but less than 1%	**Medium Hub**
		Small: At least 0.05% but less than 0.25%	**Small Hub**
		Nonhub: More than 10,000 but less than 0.05%	**Nonhub Primary**
	Nonprimary	**Nonhub:** At least 2500 and no more than 10,000	**Nonprimary Commercial Service**
Nonprimary (Except Commercial Service)		Not Applicable	**Reliever §47102(18)**

FIGURE 1.8

Airport categories.

From FAA.

Adding to the challenges for airports, as described by Hoerter (2001), is that airports must also operate safely and in a secure manner, while seeking to maintain balance between serving as a place to conduct commerce and public transportation and also complying with federal regulations.

The FAA classifies airports by categories of activities (Fig. 1.8). Commercial service airports have at least 2500 enplanements (passenger

boardings) per year. Commercial service airports may be primary or nonprimary. Primary commercial service airports have more than 10,000 annual enplanements. Nonprimary airports have at least 2500 but fewer than 10,000 enplanements. Cargo service airports host aircraft with a yearly average landed weight of more than 100 million pounds. Airports can operate both as commercial service and as cargo airports.

Reliever airports are GA airports designated by the FAA to relieve congestion at commercial service airports. These often serve as an outlet for GA traffic to avoid the congestion of the commercial service facility. Approximately 13,000 airports are GA and they constitute the largest subcategory of airports in the United States. They can be public or privately owned and operated and can have up to 2500 annual commercial service enplanements without being classified as a commercial service airport.

Commercial service airports are further classified by *hub* status.[9] Large-hub airports account for about 70% of the total annual passenger enplanements within the United States. Large-hub airports include Hartsfield–Jackson Atlanta International, Chicago O'Hare International, Los Angeles International, Dallas/Fort Worth International, and Denver International. There were 29 large-hub airports in the United States in 2010. Metropolitan Oakland International, Pittsburgh International, Portland International, Lambert–St. Louis International, and Cleveland Hopkins International airports are examples of medium-hub airports (37 in 2010). Small-hub airports (72 in 2010) include Louisville International (Kentucky), Will Rogers Field (Oklahoma), El Paso International (Texas), and Albany International (New York). Nonhub (nonprimary) airports make up the largest number of commercial service airports, totaling 244 in 2010. These include airports such as Mahlon Sweet Field (Oregon), Fort Wayne International (Indiana), Joe Foss Field (South Dakota), and Juneau International (Alaska) airports. An additional 121 airports are classified as nonhub airports servicing small numbers of commercial traffic at the rate of fewer than 2500 enplanements per year. Nonhub airports are predominantly GA operations (Table 1.1).

Civilian, commercial service airports may also be colocated with military airport facilities. Military airport facilities are not regulated by Federal Aviation Regulations (FARs; US 14 CFR Part 1-199) or TSRs (US Title 49 of the CFR, Chapter XII, Parts 1500–1699). Civilian airport operators with joint military operations must geographically separate the civilian and military areas. For example, Colorado Springs Regional Airport is located on the south side of its primary runway and shares the runway with Peterson Air Force Base, which is located on the north side of the airfield (Fig. 1.9). The areas are separated by the runway and by lines of demarcation painted on perimeter access roads.

[9]A *hub* is an airport with a high frequency of arriving and departing flights along with a relatively high rate of connecting traffic.

Table 1.1 Enplanements by Hub Type for 2000

Airport Type	Number of Airports	% of US Enplanements	Examples
Large Hub (>1.0% of all enplanements)	29	68.0%	Sea-Tac, Denver, Salt Lake City, LAX, DFW, Atlanta, etc.
Medium Hub (0.25–1.0% of all enplanements)	37	20.0%	Portland, Anchorage, Reno, Cleveland, etc.
Small Hub (0.05–0.25% of all enplanements)	72	8.0%	Colorado Springs, Billings, Boise, and Spokane
Nonhub (>10,000 enplanements, but <0.05% of all enplanements)	244	3.0%	Aspen, St. George, Cheyenne, Kalispell, and Hailey
Nonprimary Commercial Service (>2500 enplanements and scheduled service)	121	0.1%	Pueblo, Moab, Pendleton, Eastsound, etc.
Relievers (>100 based aircraft or 25,000 annual itinerant operations—other criteria apply as well)	269	0.0%	Centennial, South Valley Regional, Paine Field, etc.
GA	2560	0.0%	Aurora State, Arlington Municipal, and Nampa Municipal
Existing NPIAS airports	3332	99.1%	

Users of GA airports can include an eclectic mix of small training aircraft, experimental home-built planes, sailplane operations, helicopters, skydiving operations, and business jet air traffic. As mentioned, some GA airports host limited commercial service operations. These small airline operations are usually characterized by seasonal or periodic flights rather than daily scheduled service. Many GA airports are small, single-runway facilities, whereas others equal the size of large commercial aviation airports with multiple runways, hundreds of thousands of annual operations, and large jet aircraft.

Of the approximate 13,000 GA airports, about 3000 are part of the NPIAS (see www.faa.gov/airports_airtraffic/airports/planning_capacity/npias). NPIAS airports are designated as vital to the national airspace system and thus eligible for federal funding for airport safety, capital improvements, and security projects.

Private entities or individuals own, construct, and maintain private airports. Use of a private airport is generally restricted to the owner or those granted permission by the owner. However, in the United States, any aircraft in an emergency may use any airport, including private airports.

FIGURE 1.9

Peterson Air Force Base in Colorado Springs shares runways with the Colorado Springs Municipal Airport.

Title 14 CFR Part 139 Certification of Airports assigns a different classification for commercial service airports for the purpose of compliance with the Airport Certification Manual (ACM; see www.faa.gov/airports_airtraffic/airports/airport_safety/part139_cert/media/sample_ACM.pdf). The ACM outlines how the airport will comply with FARs to operate safely without specifically addressing security concerns. Under FAR Part 139, there are four classifications of commercial service airports: class I airports encompass most large-, medium-, and small-hub airports; class II airports encompass small scheduled service and large charter operations; class III airports encompass small scheduled service operations only; and class IV airports encompass large charter operations.

Security classifications for airports are established by the TSA and fall into three types: complete, supporting, and partial. The type of security program required at a particular commercial service airport depends on factors such as the scope of the airport's operation, the geography (ie, the airport is located near other critical infrastructure), the opinion of the TSA, and geopolitical circumstances. Complete security programs are generally required for large-, medium-, and small-hub airports. Supporting and partial security programs are generally required for nonhub airports.

AIRPORT OWNERSHIP AND OPERATION

Municipalities (eg, cities and counties) own and operate the majority of publicly available service airports in the United States. Exceptions to this form of ownership are Alaska, Hawaii, and Rhode Island, which own all the civil airports within their boundaries.

A common misconception is that the FAA operates US airports, as many airports have an FAA air traffic control tower (ATCT). ATCTs are staffed by FAA employees and coordinate the movement of aircraft in and around the runway of an airport. However, the movement of aircraft and ground vehicles within the "movement area" of an airport is generally the extent of the FAA's authority. The authority to close the airport, to open and close runways, and to manage other functions is generally under the purview of the airport owner or operator, which is usually a municipality or an appointed authority. The relationship between the airport owner or operator and the FAA at a particular airport is defined in a letter of agreement.

City and county airports can be owned and managed through a variety of arrangements. A municipally operated airport is typically owned by a city or county and run as a department or division within the municipality's organizational structure by its employees (Wells and Young, 2004). In contrast, an airport may be operated by an airport authority, which is an entity created by state legislation, usually at the will of a city or county, and which acts as a separate governmental agency (Hoerter, 2001). The city or county retains airport ownership, but much of the management and planning decisions are turned over to the airport authority. According to Hoerter, airport authorities are the preferred method of ownership, because "the leadership is more focused on airport issues, the airport staff is less subject to political interference, and a metropolitan community can be better represented by the authority's governing body" (2001, p. 12).

Al Graser, during his tenure as general manager of John F. Kennedy International Airport and former chair of the AAAE Transportation Security Policy Committee, agrees with Hoerter's viewpoint and adds to it a perspective related to security. Graser argues that airport directors working for an airport authority have the benefit of consistency, which gives them the ability to develop industry relationships needed to work with the TSA and other government agencies, particularly regarding security issues. Graser also claims that airport directors working directly for a city or county often campaign with the mayor or county commissioners for reelection, because if political situations change, the airport director is likely out of a job (Al Graser, personal communication, Dec. 2005).

Some airport authorities, such as the Los Angeles World Airports Authority (LAWAA), are responsible for entire aviation systems. The LAWAA oversees the management and operation of Los Angeles International Airport, Ontario International Airport, Van Nuys Regional Airport, and Palmdale Regional Airport.

The *port authority* is another form of airport management structure. A port authority is a legally chartered institution, with management responsibility

often extending beyond aviation and into several transportation modes. For example, the Port Authority of New York and New Jersey (PANY&NJ) represents John F. Kennedy International, LaGuardia International, Newark Liberty International, Stewart International Airport and Teterboro (a GA airport), Downtown Manhattan Heliport, and the New York seaport complex. PANY&NJ also manages various tunnels, bridges, bus terminals, the commuter ferry system, the AirTrain, and the PATH Rapid-Transit System commuter rail for New York and New Jersey.

AIRPORT SECURITY OPERATION

Airport directors or managers oversee airport operations. Airport staffing includes operations personnel responsible for managing airfield safety inspections and emergency response to incidents including compliance with the ACM, maintenance personnel who ensure the airfield lighting systems and other essential buildings, fleets, and field systems are operational; administrative personnel managing the budget, accounting, human resources, and information technology functions; public relations and marketing personnel; planning and engineering personnel; and security and law enforcement personnel who ensure compliance with the Airport Security Program (ASP).[10] A large airport may have hundreds or even thousands of employees. In contrast, only one individual may have management responsibility at a smaller GA airport.

Commercial service airports fall under Title 14 CFR Part 139, which requires an airport to meet a variety of standards related to airfield safety inspections, emergency response, wildlife management, public protection, and others. Flight operations at a commercial service airport are regulated under a variety of different regulations depending on the nature of the flight operation (scheduled air carrier, charter, private operation, etc.). Airports with 14 CFR Part 139 certificates are also required to adhere to Title 49 CFR Part 1542 Airport Security.

Most GA airports do not have specific federal regulations covering safety and security procedures; however, flight operations regardless of their location are regulated from a security perspective.[11] Three GA airports (College Park, Washington Executive/Hyde Field, and Potomac Airfield) have specific security regulations set forth by the federal government because of their proximity to Washington, DC. Some states have implemented their own regulations covering GA airports.

For many GA airports, the FAA provides funding in the form of federal grants for capital improvement projects. The FAA requires the recipient airport (known

[10]The ASP is a formalized plan required and approved by the TSA and used for implementing and managing security procedures at most US airports.

[11]Flight operations can be regulated under 14 CFR Parts 91, 121, 125, 127, or 135 and under Title 49 TSR CFR Parts 1544, 1546, 1548, or 1550.

as a *sponsor*) to adhere to *grant assurances*. Grant assurances require the airport operator to adhere to certain safety standards and management policies (see www.faa.gov/airports_airtraffic/airports/aip/grant_assurances). However, the FAA has not normally provided funding to GA airports for security projects.

Commercial service airport operators prepare an ACM to demonstrate how their airport will comply with Title 14 CFR Part 139. ASPs are drafted by commercial service airports to demonstrate how the airport will comply with Title 49 CFR Part 1542. Aircraft operators have similar security programs (under Title 49 CFR Part 1544) to demonstrate compliance with federal transportation regulations.

At each commercial service airport, the *airport security coordinator* (ASC), who usually operates a security department or division, oversees compliance with federal regulations and maintains compliance with the ASP. ASCs are charged with conducting security exercises, providing fingerprint-based criminal-history record checks, issuing identification badges (commonly referred to as access media or credentials), ensuring adequate law enforcement is present to respond to incidents, and assisting the TSA, FBI, airlines, and airport tenants with security matters.

AIRPORT FUNDING

Airports are funded by a variety of sources depending on the type of airport. Hoerter explains: "An airport can operate as a stand-alone enterprise because its revenues and expenses are related in a businesslike context; therefore, logical user fees can be charged for services rendered" (2001, p. 13). Commercial service airports are funded by leasing gates and administrative space to the airlines and other tenants, charging landing fees, and collecting passenger facility charges (PFCs), parking fees, and a percentage of concession sales. GA airports are primarily funded by leasing space to tenants and through the collection of a percentage of fuel sales. Understanding the revenue flows for an airport is important to planning and design decisions relating to security needs. Eliminating revenue-producing space to expand security checkpoints or include additional security equipment creates financial challenges for an airport, which must be offset with some other strategy.

An important revenue stream to airport operators is the PFC. The PFC is a charge that is collected (through the airline ticket) at an airport with the fee going to the airport operator. PFC money can supplement AIP monies and is often used for airfield safety and security improvements. However, the airline industry has traditionally fought against the collection of PFCs or the raising of PFC fees (A4A, 2015). A 2015 Government Accountability Office (GAO) report found that increasing the PFC cap could marginally slow passenger growth and therefore the growth in revenues to the airport Trust Fund (GAO, 2015). However, the GAO also noted that many passengers are not educated on reasons for PFC collection, and that depending on a variety of elements, an increased cap could reduce total revenues by 1%. Since 2000, PFCs have

been collected at the rate of $4.50 per passenger (lower than the current security fees collected by TSA), but airports have sought to raise the fee to $8.50. In an A4A poll conducted in 2015, survey respondents said they believe airports are already well funded and opposed another tax. However, PFC monies are considered a fee, not a tax, and go toward safety and security improvements, not to improve profitability for an airport, which are by and large government entities and strive to break-even. For commercial and GA airports, part of the annual capital improvement funding comes from the FAA's Aviation Trust Fund (ATF).[12] The US Congress reviews and approves airport funding through the AIP every few years (see www.faa.gov/airports_airtraffic/airports/aip). Additional funding is also derived through legislation for security programs and is generated by passenger fees. Several US airports receive funding from their city or county; however, the FAA generally encourages airports to be self-sufficient, generating enough of their own revenue to cover expenses.

AGENCIES AND ORGANIZATIONS

REGULATORY AGENCIES

In the United States, the primary regulating agency for aircraft and airport operations is the FAA, an administration of the US Department of Transportation. It oversees the management and enforcement of CFR Title 14 Aeronautics and Space, including the rules governing airport safety certification and air traffic control.

Commercial service airports fall under 14 CFR Part 139 Certification of Airports. Part 139 requires an airport to meet a variety of standards, such as airfield safety inspections, emergency response, wildlife management, and public protection. Flight operations at a commercial service airport are regulated under a variety of regulations depending on the nature of the flight operation. Airports operating under 14 CFR Part 139 Certificates[13] are also required to adhere to TSR Part 1542 Airport Security (see www.tsa.gov/research/laws/regs/editorial_1785.shtm).

Before 9/11, the FAA presided over the security regulations pertaining to airport and aircraft operations. After 9/11, this function transferred to the newly created US TSA. The TSA enforces the TSRs and is a division of the US Department of Homeland Security.

[12]The ATF was formally known as the FAA Airport and Airway Trust Fund and is designed to fund the nation's aviation system through various taxes (see www.faa.gov/airports_airtraffic/trust_fund).

[13]In general, 14 CFR Part 139 requires the FAA to issue airport operating certificates to airports that (1) serve scheduled and unscheduled air carrier aircraft with more than 30 seats, (2) serve scheduled air carrier operations in aircraft with more than 9 seats but fewer than 31 seats, or (3) the FAA administrator requires a certificate.

INDUSTRY TRADE ORGANIZATIONS

Industry trade organizations play a significant role in influencing public aviation safety and security policies through lobbying efforts and various membership services. These organizations often provide training and research on issues related to aviation security. Aviation-related trade organizations include the Airlines for American (formerly known as the Air Transport Association; see www.airlines.org), which represents commercial airlines; the IATA, which represents airlines throughout the world; the AAAE (see www.aaae.org), which represents airport operators; Airports Council International, which also represents airport interests; the Aircraft Owners and Pilots Association, which represents GA aircraft aviators; the National Business Aviation Association (see www.nbaa.org), which represents business aircraft operators; and the National Agricultural Aviation Association (see www.agaviation.org), which represents the operators of agricultural aircraft.

CONCLUSIONS

The aviation industry is essential to the viability of the US economy, which makes aviation a prime target for terrorists. The complexity and size of the industry also make it an attractive environment for crime. Understanding the tenuous financial structure of airlines, the aviation industry aids the security practitioner in applying appropriate and practical security measures. Aviation security practitioners must deploy systems, measures, and procedures to counteract both terrorist and criminal perpetrators. To meet these challenges, aviation security practitioners employ layered security systems that are symbiotic with the global aviation industry.

The US Congress establishes policy for protecting US aviation. Federal regulators convert these policies into regulations, which are therefore established as accepted industry practices. Federal regulators implement and supervise these policies and regulations across all aircraft operators and airports.

The 9/11 Commission was tasked with assessing facts surrounding the September 11, 2001, terrorist attacks. The 9/11 Commission analyzed and recommended new strategies for adoption within the United States. Because of the 9/11 Commission's work, the largest overhaul of aviation security in US history was implemented. However, to thwart or reduce the risk of crime or terrorist activity, the strategies recommended by the 9/11 Commission must remain flexible in evolution and application. The following chapters in this text will help aviation security practitioners or students build on the recommendations made by the 9/11 Commission. Readers of this text will be better prepared to understand, develop, and apply strategies, tactics, and methods that are appropriate and practical to the future needs of aviation security.

Aviation security practitioners or students of aviation security should have a solid understanding of the nature and contributing factors regarding the attacks of September 11, 2001. Therefore, it is strongly recommended that readers review the preceding case study on 9/11.

CASE STUDY: SEPTEMBER 11, 2001 (9/11) TERRORIST ATTACKS[14]

September 11, 2001

On September 11, 2001, Mohammed Atta checked in for his flight to Boston. Atta was preselected under the Computer-Assisted Passenger Prescreening System (CAPPS) to undergo additional security measures. These measures were to ensure that his baggage did not board the aircraft without him. The positive passenger–baggage matching (PPBM) program is designed to deter placement of an explosive device in checked baggage, but not to deter hijacking.[15]

Four other hijackers—Khalid al Mihdhar, Majed Moqed, Nawaf al Hazmi, and Salem al Hazmi—also checked in at the American Airlines ticket counter at Washington Dulles International Airport. These terrorists were also selected for additional scrutiny under CAPPS, but again, only to ensure they boarded assigned aircraft. One of the hijackers had neither photo ID nor understood English, and the ticket agent labeled the passengers as suspicious.

When the 9/11 Commission interviewed screeners at access points used by the hijackers, none reported anything unusual about the hijackers. At Dulles Airport, some hijackers activated walk-through metal detector alarms and were subjected to additional screening by hand wand. During subsequent reviews, a screening expert seeing the closed-circuit video of the screening process testified that the quality of the hand wand process was marginal. Additionally, one of the hijackers was seen on video with an unidentified object clipped to his belt. At Newark, NJ, the departure point of United Flight 93, one of the hijackers was preselected for additional scrutiny under CAPPS. As with Boston, Newark's screening checkpoints did not have closed-circuit television (CCTV) surveillance, so it is difficult to determine what took place at the screening checkpoints.[16]

Once hijackings began on 9/11, US agencies had a difficult time communicating with each other. Information from hijacked aircraft to the FAA and from airline headquarters to the FAA was nonexistent or ineffective because of cockpit takeovers by the terrorists. One method pilots use to notify the FAA of hijacking is to broadcast an emergency code via a transponder.[17] This code is published in the publicly sold *Aeronautical Information Manual* (FAA, 2008) and is taught in the most basic FAA pilot training curriculums. Because their flight training was conducted in the United States, the 9/11 hijackers would have known about the code and would have been familiar with the transponder. In three of the four hijacked aircraft, the transponders were turned off, making it difficult for the FAA to track the aircraft on radar.

The FAA and US military agencies were not in communication throughout the entire 9/11 attack sequence. Defending the United States during the attacks was a mission of North American Aerospace Defense Command (NORAD). NORAD's mission was to protect the United States from external threats. NORAD explored the threat of terrorists using aircraft as weapons of mass destruction, but the threat was based on speculation and not on developed intelligence.

The US government requires the FAA to work with the National Military Command Center (NMCC) in the Pentagon to manage hijackings in progress. Part of this process is to notify NORAD's Northeast Air Defense Sector (NEADS) in Rome, New York, to coordinate the intercept of hijacked aircraft by US military aircraft. However, during 9/11, both the FAA and the NMCC assumed that a hijacked aircraft would not attempt to disappear off radar, that there would be time to address the hijacking, and that a hijacking would follow a traditional form (land and

[14]The following case study is a synopsis of the key contributing factors and issues in aviation security management that were salient to the 9/11 attacks. Most of the content for this case was sourced from The 9/11 Commission Report (9/11 Commission, 2004).

[15]PPBM is also ineffective against suicide bombers, but for decades it had effectively deterred many non-suicide airline bombings.

[16]Although not mandated, CCTV monitoring of screening checkpoints is recommended by TSA and other aviation security experts.

[17]Referred to by pilots and air traffic controllers as "squawk 7500."

negotiate) rather than be enacted as a suicide mission. Communications between the FAA and NEADS were so inadequate that the military was using radar to search for American Airlines Flight 11 after the plane had struck the North Tower of the WTC. The first indication NEADS had of the second hijacked flight, United Airlines 175, came about the same time as that plane hit the South Tower of the WTC.

NEADS did send two F-15 fighter jets from Otis Air Force Base in Falmouth, MA, but without an assigned target because of communication problems, they were ordered in a holding pattern off the coast of Long Island. A National Guard C-130 cargo plane was also requested to search for American Airlines Flight 77 heading toward its Pentagon target. Because the C-130 was unarmed, the aircraft could only attempt to collide with American Airlines Flight 77 (if it had been granted that action by proper authority).

After 9/11, there was considerable discussion by US agencies and the federal government on who had authority to give an order to shoot down a commercial airliner. President Bush testified that he gave authorization to shoot down hijacked aircraft and that the order was passed to the vice president and through the NORAD command chain. This conversation between President George W. Bush and Vice President Dick Cheney took place between 10:10 am and 10:15 am Eastern Daylight Time on 9/11, just moments before United Airlines Flight 93 crashed in Shanksville, PA. The shoot-down order made its way through the NORAD command structure, and within 20 minutes flight controllers talking to interceptor aircraft had authorization. *The 9/11 Commission Report* (Fig. 1.10) outlines numerous other flaws in communication between the national military command authority and the FAA. The report stated:

> *The defense of U.S. airspace on 9/11 was not conducted in accord with preexisting training and protocols. It was improvised by civilians who had never handled a hijacked aircraft that attempted to disappear, and by a military unprepared for the transformation of commercial aircraft into weapons of mass destruction. As it turned out, the NEADS air defenders had nine minutes' notice on the first hijacked plane, no advance notice on the second, no advance notice on the third, and no advance notice on the fourth. (9/11 Commission, 2004, p. 31)*

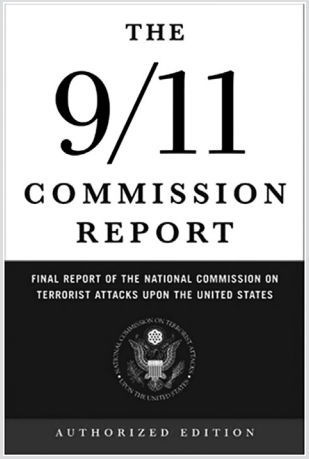

FIGURE 1.10

The 9/11 Commission Report outlined the structure and actions of the 9/11 attacks along with recommendations for improving aviation security.

Assumptions of what terrorists or criminals will do, based on a given situation and on the effectiveness of established communication protocols, are key concerns to aviation security practitioners. The assumptions made by stakeholders on 9/11 followed those of a "traditional hijacking," which proved fatal for thousands of US citizens.

The 9/11 Commission provided insights on the changing nature of the terrorist threat to aviation. The 9/11 Commission suggested that the failure of terrorists to destroy the WTC in 1993 and the quick success of investigators and prosecutors in bringing the perpetrators to justice might have contributed to a widespread underestimation of future terrorist threats by US officials and security personnel.

In addition to the notion of overconfidence by US officials and security practitioners, other failures contributed to the 9/11 attacks. Historically, aviation security professionals have been a consumer of intelligence information rather than a source. Therefore, aviation security practitioners rely on intelligence information gathered, disseminated, and analyzed by other agencies such as the FBI and, before 9/11, the FAA. However, as the 9/11 Commission pointed out, the FAA is also not a traditional source of intelligence information related to threats and is just as much a consumer of that information as airport and aircraft operators. Therefore, breakdowns in the dissemination of intelligence information to entities that can take action are of vital importance to the future of aviation security.

The 9/11 Commission Report noted that over the previous three decades, dissemination of intelligence information from federal agencies was ineffective. During that time, there had not been a domestic hijacking in more than 10 years, and the commercial aviation industry was more concerned with explosives than firearms or other weapons. The Presidential Commission on Aviation Security, chaired by Vice President Al Gore in 1997, focused nearly all of its recommendations on protecting civil aviation from bombings even though the number of attempted hijackings exceeded 600, whereas airline bombings numbered fewer than 100.

The 9/11 Commission stated that the existing layered security system intended to prevent hijackings was "seriously flawed" (9/11 Commission, 2004, p. 83). At the time of the 9/11 attacks, the FAA's *no-fly list* contained the names of only 12 individuals who were not allowed on board US civil aircraft. Furthermore, the security chief for the organization stated that he had not heard about the US State Department's tipoff list of known and suspected terrorists. Apparently, the FAA did have access to the tipoff data but found it too difficult to use. As consumers of intelligence data, the FAA also lacked awareness of developing threats.

Various hijackers on 9/11 had taken flight lessons within the United States. *The 9/11 Commission Report* states that in 2001, information about Middle Easterners taking flight lessons in the United States was not relayed to the FAA's 40-person intelligence unit. FAA Administrator Jane Garvey did not review daily intelligence information and was unaware of the hijacking threat information from her own intelligence unit.

Before 9/11, checkpoint screening was considered the most important layer of security. However, numerous GAO reports identified shortcomings in the screening process. Another security gap was the FAA's policy of allowing knives with blades shorter than 4 inches onto commercial aircraft. A 1993 proposal to ban knives was rejected because of projected increased congestion at checkpoints. Although continuous and random secondary screening using EDS and explosive trace detection technology was mandated after 1996, the policy was ignored to the point that it was operationally nonexistent. The report was further critical of airline opposition to procedures affecting the efficiency of flight operations.

Training and performance standards were part of the Gore Commission's recommendations, but not until the passage of the Airport Security Improvement Act of 2000 (ASIA 2000) were they placed into legislation. However, by 9/11 screener training and performance standards had still not been implemented. ASIA 2000 transferred the responsibility to the TSA, and screener training and performance standards are now required. Furthermore, the policy on prohibited items has changed. Knives shorter than 4 inches are no longer allowed on board commercial aircraft.

The final layer of airline security against hijackings used at the time of 9/11 was known as the Common Strategy, which instructed pilots and flight crews to cooperate with hijackers and land the plane as soon as possible, then let law enforcement take over to resolve the hijacking. The Common Strategy was not designed to counter suicide hijackings. This fundamental concept has changed to more active resistance against hijackers, as the assumption can no longer be made that future hijackers will follow traditional methods or purposes of hijacking.

Important lessons may be learned by analyzing the planning of the 9/11 attacks. Khalid Sheikh Mohammed (KSM; Fig. 1.11) began work on the future 9/11 attacks with Osama bin Laden in 1996. The two met in Afghanistan to discuss various attack methods against "potential economic and 'Jewish' targets in New York City" (9/9073511 Commission, 2004, p. 150). KSM had previously been involved in plots to assassinate President Clinton and to bomb US-bound air cargo carriers by smuggling nitrocellulose on board. At the 1996 meeting, initial planning of the 9/11 attacks was formulated as KSM and bin Laden discussed plans to train pilots to fly into US targets. New York and Los Angeles were identified as economic centers of the United States, which factored into the decision to target those cities. Other forms of attack were considered, including hijacking planes and then blowing them up in flight (similar to the Pan Am 103 bombing). However, KSM felt that explosives were too problematic and that a novel form of attack was required.

By 1999, the plot by KSM and bin Laden was moving forward with a list of targets including the White House, Pentagon, WTC, and US Capitol. Suicide operatives were recruited. A second attack was also planned, which resembled Yousef's Operation Bojinka plot. In this secondary plot, suicide bombers would board US aircraft on Pacific oceanic routes, possibly concealing bombs in their shoes. Both attacks (hijackings and airline bombings) were to be executed simultaneously, enhancing the psychological impact. This strategy is characteristic of the desire by terrorists for large physical and widespread psychological impact. However, by 2000, bin Laden canceled the second attack plan, declaring it too difficult to coordinate with the US hijack operation. In late 2000, the US National Security Council did warn the Justice Department about the second attack plan.

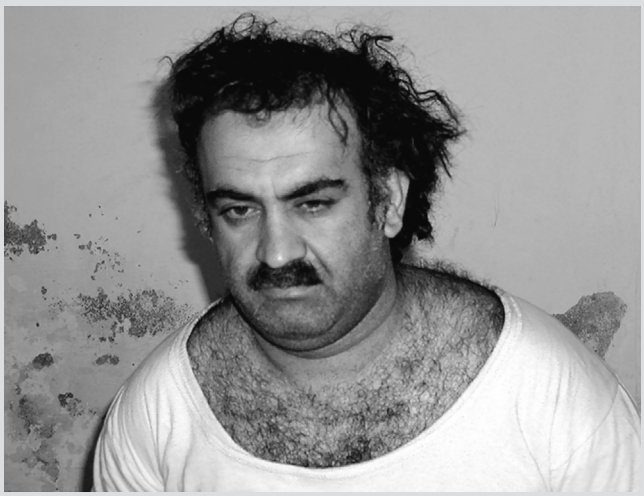

FIGURE 1.11

KSM worked with Osama bin Laden to plan the 9/11 attacks.

KSM spent much of 1999 training operatives on what he learned about the US aviation system. He searched the Internet, collecting brochures and information on US flight schools, reviewed airline timetables, bought movies depicting hijackings, and even purchased flight simulator software. Training also included lessons in English and how to read US phone books and airline timetables. Although most of this material is publicly available, it is interesting to note the extent to which the attacks were planned to give the terrorists insight into the intelligence-gathering process. Part of the advance surveillance process included observing flight crews in action, noting particularly when the cockpit doors were opened and processes that would take place when flight crewmembers used the lavatory and when food was served to the flight crew. Some operatives would test components of the aviation security system by intentionally bringing box cutters onto commercial flights and by removing box cutters and other items while in flight, then observing the reactions of passengers and flight attendants.

Flight Training Begins

Once training was completed in Afghanistan, the hijackers began their move to the United States and began efforts to appear less radical. The hijackers shaved their beards and wore Western clothing in efforts to blend into US society.

The 9/11 Commission outlined two abilities fundamental to the success of terrorist attacks: to travel and to transfer money. The plot required numerous international trips by planners and operators. Al-Qaeda hosted an office at the Kandahar Airport in Afghanistan that facilitated altering papers, visas, and passports. Operators were taught simple methods to alter their own passports and change documents while en route. It is estimated that $400,000 to $500,000 was spent to plan and carry out the 9/11 attacks. Al-Qaeda raised money through corrupt charities and donations from sympathizers in certain Gulf countries including Saudi Arabia, but it is not certain that all donors knew how their money was being used. The 19 hijackers were supported with funds wired from KSM, brought in as cash or held in foreign bank accounts that could be accessed from the United States. These findings of the 9/11 Commission highlight the importance of effective immigration and customs inspections as crucial components to national security that also affect aviation security. Although not part of the 9/11 attacks, the commission did note the importance of using fraudulent documents to facilitate an attack, when addressing the attempt by Ahmad Ressam (who used fraudulent documents) to attack Los Angeles International Airport in 2000.

Once in the United States, with their flight training started, the hijackers provided some interesting clues as to their intentions. A San Diego-based flight instructor of two of the operatives noted their unusual reaction when told they would have to start learning to fly in small aircraft. He believed they were joking when they requested to start their training in large planes, particularly Boeing-type aircraft. The instructor also noted that they were poor students and seemed more focused on learning how to operate the aircraft in flight rather than on how to land. A Florida flight instructor commented that two of the students, who were also hijackers, were rude and aggressive and at times fought with him over the controls. At one point, both those hijackers took the FAA exam to obtain the FAA instrument rating, and both failed. They were both very upset and stated that they had jobs waiting for them once flight training was complete.

Eventually, three of the hijackers learned to fly well enough to obtain the FAA commercial pilot certificate and began flying large-aircraft simulators. One pilot, Hani Hanjour, obtained his flight certificates in Arizona between 1996 and 1997. He was identified as a pilot by the background information he provided while at an al-Qaeda training camp and referred to KSM in 2000. Hanjour returned to Arizona for refresher training and to learn how to fly multiengine aircraft. Difficulties with English made learning how to fly the multiengine planes a challenge, and his flight instructor recommended him to discontinue. Hanjour then enrolled at the Pan Am International Flight Academy in Mesa, AZ, and began training on a Boeing 737 simulator.

A critical ingredient in the 9/11 attacks was the ability of the hijackers to fly the aircraft, which is why ATSA 2000 now places specific requirements on flight schools throughout the United States, now called the Alien Flight Training Program. Under the program, all flight students are now required to show proof of citizenship in the United States; legal aliens are required to have their fingerprints taken and their names checked against known terrorist watch lists.

In the early summer of 2001, the pilot hijackers began taking cross-country surveillance flights on US air carriers. Some also took additional flight training including flights along the Hudson Corridor, "a low-altitude hallway along the Hudson River that passes New York landmarks like the World Trade Center," as well as through the Washington, DC, airspace (9/11 Commission, 2004, p. 242).

At a meeting with an al-Qaeda facilitator in Spain in the summer of 2001, Mohammed Atta discussed details of the attack, including orders that if the pilots were unable to reach their objectives, they were to crash the planes. Atta considered targeting a nuclear facility, but the other pilots disliked the idea because of airspace restrictions, which would make reconnaissance around such sites difficult and increase the possibility of the planes being shot down. Al-Qaeda leaders determined that a nuclear strike would not have equal psychological value to attacking the WTC, as the center symbolized the economic strength of the United States. Atta further advised the following (9/11 Commission, 2004, p. 245):

1. On their surveillance flights, box cutters were not of concern to security screeners.
2. The best time to access the cockpit was 10–15 minutes into the flight when the cockpit doors were normally open. Atta discussed taking a hostage to compel the flight crew to open the doors but he felt this would not be necessary, as they should be open or unlocked anyway.
3. To use airplanes on long flights, as they would have more fuel on board.
4. To hijack Boeing aircraft because he believed Airbus aircraft had an autopilot feature that prevented planes from being crashed intentionally into the ground.
5. And the "muscle hijackers" had all arrived in the United States without incident.

Zacarias Moussaoui

KSM testified that a "second wave" of attacks, which included Zacarias Moussaoui, was planned (Fig. 1.12). However, during the summer of 2001, he was too busy with the 9/11 operation to put much effort into its planning. Moussaoui had taken flight lessons in Norman, OK, and asked about flight simulation materials for a Boeing 747. He also was moving forward with an application to Pan Am International Flight Academy, bought knives, and inquired about the use of portable global positioning system units for aviation (9/11 Commission, 2004, pp. 246–247).

Moussaoui's instructor at Pan Am notified authorities about his student's unusual behavior. Moussaoui paid the full balance of his Pan Am training in cash ($6800), and it seemed odd to his instructor that Moussaoui was learning to fly large jets without any intention of obtaining a pilot's license. Immigration authorities arrested Moussaoui on August 16, 2001. However, bin Laden and KSM did not learn of his arrest until after 9/11. KSM indicated that had they heard about the arrest they likely would not have gone forward with the attacks.[18] This is an important point, as it demonstrates how unplanned events can deter an attack in the planning stages. Another important point is the flight instructor's suspicions of his student and his actions to report those suspicions to authorities. This was information that could have led to discovery or mitigation of the plan to attack on 9/11.

[18]In 2006, Moussaoui plead guilty to six terrorism conspiracy charges and was sentenced to life in prison.

FIGURE 1.12

Zacarias Moussaoui took flight lessons in the United States in preparation for his role in the 9/11 attacks.

The System Is Flashing Red

During the summer of 2001, warning reports of planned terrorist attacks increased to their highest level since the millennium alert. In May 2001, the FAA was notified of a potential plot to hijack US aircraft to free incarcerated terrorists in the United States. The FAA issued an information circular to US air carriers warning of such attacks. During that same time, CIA Counterterrorist Chief Cofer Black warned National Security Adviser Condoleezza Rice that the current threat level was 7 on a scale of 1−10, as compared to an 8 during the millennium alert. In June, the CIA notified its station chiefs about intelligence, suggesting al-Qaeda was planning a possible suicide attack against a US target. The Department of State notified all its embassies of the terrorist threat. By late June, a terrorist threat advisory warned of near-term "spectacular" attacks resulting in numerous casualties (9/11 Commission, 2004, p. 257). US Central Command raised the force protection condition level for its troops to the highest level. By July, the FBI Counterterrorism Division issued a message to federal and state law enforcement agencies warning of increased threat reporting that indicated a potential attack against US targets, but also stated that there was no credible threat of a pending attack within the United States. Also, many warnings circulating within the federal government suggested an attack was imminent at locations other than within the United States.

In July 2001, an FBI agent in the Phoenix field office sent a memo warning of a coordinated effort by bin Laden to send students to US flight schools and recommended that specific actions be taken to further investigate this lead. The author of the memo stated that its subject was not related to suicide hijackings but more toward a potential bombing of US airliners. No one at FBI headquarters saw the memo before 9/11 and the NYC field office took no action.

The 9/11 Commission stated that if the memo had been read and followed up on, it may not have revealed the plot but may have made agents more sensitive to the threat when Moussaoui was arrested and therefore the matter taken more seriously.

By July 31, the FAA issued another information circular alerting aircraft operators of possible near-term terrorist operations in the Arabian Peninsula or Israel, but the circular also stated it had no credible evidence of specific plans to attack US civil aviation. Intelligence activity regarding potential attacks seemed to drop in August 2001. The intelligence community issued an advisory concluding that warnings of an al-Qaeda attack would continue indefinitely. From an intelligence perspective, although many were watching, few of the reported activities were correlated. This sentiment is embodied in the 9/11 Commission's comment, "The September 11 attacks fell into the void between the foreign and domestic threats" (9/11 Commission, 2004, p. 263).

In an attempt to prevent future intelligence failures, on December 17, 2004, President Bush signed the Intelligence Reform and Terrorist Prevention Act of 2004. The act created the position of Director of National Intelligence (DNI). The DNI is now the president's primary intelligence adviser with authority over budget and personnel decisions throughout the 15-member US intelligence community.

In the summer of 2001, the FAA did not issue any security directives that mandated increased security at checkpoints or on board aircraft. Mostly the FAA urged air carriers to "exercise prudence" and be alert. Before 9/11, the FAA presented a CD-ROM to air carriers and airport authorities describing the increased threat to civil aviation. The presentation mentioned the possibility of suicide hijackings but indicated that no known group was planning to implement this type of threat.

The FAA conducted 27 special security briefings for specific air carriers between May 1, 2001, and September 11, 2001. Two of these briefings discussed the hijacking threat overseas. None discussed the possibility of suicide hijackings or the use of aircraft as weapons. No new security measures were instituted.

Emergency Response

In describing the concept of emergency response, the 9/11 Commission (2004) stated:

> *Emergency response is a product of preparedness. On the morning of September 11, 2001, the last best hope for the community of people working in or visiting the World Trade Center rested not with national policymakers but with private firms and local public servants, especially the first responders: fire, police, emergency medical service, and building safety professionals. (p. 278)*

The 9/11 Commission Report touches on an important point of airport and aircraft operator security, which is the ability to both withstand an attack and recover from such an attack. The quicker an agency is able to recover from an attack, the less likely it is to be a target.

The WTC towers housed approximately 50,000 workers, and the entire complex exceeded the office space of downtown Atlanta, GA, and Miami, FL, combined (Fig. 1.13). The towers provided a variety of features to mitigate fire and smoke damage; however, there was not a rooftop evacuation plan. Both roofs were sloped and cluttered with radiation towers. There was a helipad on the South Tower, which did not meet FAA certification for use. During the building fires on 9/11, strong updrafts and a lack of visibility resulting from the rising smoke rendered helicopter rescues impossible. However, several rescues from the roof during the 1993 WTC bombing seemed to leave those who worked at the WTC with the impression that helicopter roof rescues were part of the evacuation plan—however, they were not.

In 1993, after a truck bomb exploded underneath the WTC towers in a parking garage, killing 6 and injuring more than 1000, the towers lost power and communications, including emergency communications. The 9-1-1 emergency call systems were flooded, and the ensuing evacuation took 4 hours. These were important lessons learned, and the PANY&NJ (the offices of which

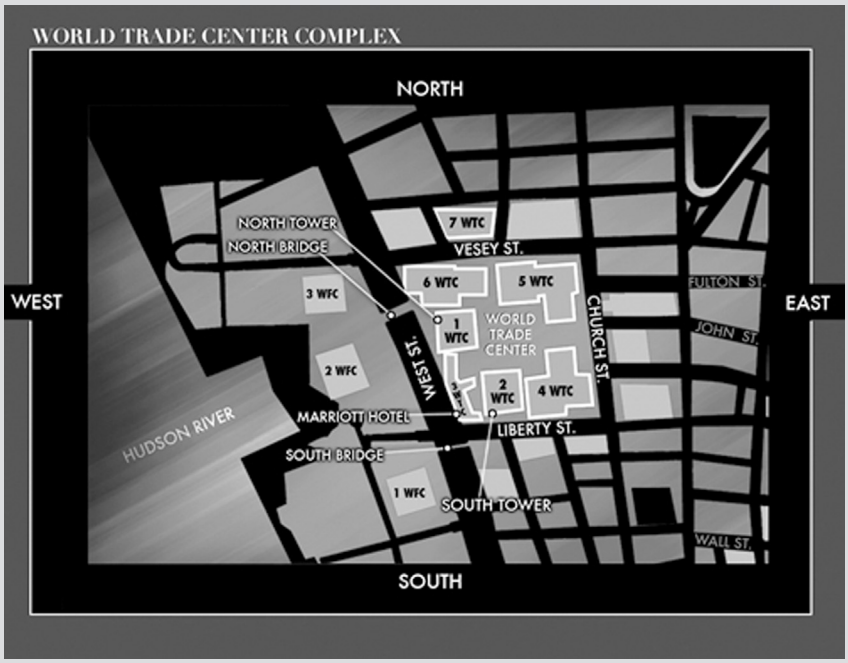

FIGURE 1.13

The WTC towers.

were located within the WTC) invested more than $100 million to make physical, structural, and technological improvements. The improvements included enhancements to power sources, emergency exits, a computerized fire alarm system, and the creation of a fire safety director position. Fire safety teams composed of office workers with fire wardens and searchers were created, along with twice-per-year fire drills. A radio repeater system was also installed in the towers to assist fire department personnel with radio communications. On 9/11, after both towers had been struck and response efforts were under way, the repeater system for the radios that was installed after the 1993 bombing worked only partially (in both towers) depending on the channel used and the particular radio broadcasting or receiving.

The 9/11 Commission noted that the fire drills conducted in the WTC were not comprehensive enough to address such a massive fire as that caused by the aircraft on 9/11, and that tenants were never advised that a roof rescue was not part of the evacuation plan. During evacuation drills, tenants were advised to evacuate only a few floors below the fire. Apparently, WTC tenants were not the only individuals not informed of the lack of a roof rescue contingency. After the WTC North Tower was struck, a team from the New York City Police Department's Emergency Services Unit (ESU) requested to be picked up at the Wall Street heliport to assist in a roof rescue. The team was advised that they could not land on the roof because of flames and heavy smoke. Regardless, ESU units and three New York Police Department (NYPD) helicopters remained ready to try a roof rescue if the conditions changed.