

13. LOSING FOCUS ON AVIATION SECURITY

Aviation security has improved dramatically since September 11, yet critical gaps remain. This chapter highlights the current state of aviation security and the most pressing deficits in the existing system and recommends a course of action for correcting those deficits. Six areas of aviation security are particularly important: passenger screening, checked baggage security, air cargo security, the shoulder-fired missile threat, in-flight and crew member security, and aviation worker screening.

WHERE WE ARE TODAY: THE CURRENT STATE OF AVIATION SECURITY

The events of September 11 demonstrated not only how vulnerable our air carriers were to a terrorist hijacking but also how vulnerable our economy is to shocks in the commercial airline industry. Commercial air carriers generate more than \$100 billion per year and support approximately 720,000 jobs.¹ The air traffic these carriers generate is even more impressive: Every day in the United States, 30,000 flights carrying 1.8 million passengers take off from more than 450 domestic commercial airports.²

In response to September 11, President Bush signed the Aviation and Transportation Security Act (ATSA) into law on November 19, 2001. ATSA endowed the newly created Transportation Security Administration (TSA) with responsibility for securing the commercial aviation system—previously the domain of the Federal Aviation Administration. TSA's mandate included overseeing security operations at over 450 commercial airports, which included passenger screening, checked baggage screening, and the procurement and installation of explosive detection

systems.³ By December 2002, the TSA was screening about 90 percent of checked baggage for explosives and had deployed a workforce of 65,000 screeners and federal air marshals.⁴

Since its inception, the TSA has received direction from congressional acts and commissions. In July 2004, the 9/11 Commission recommended the United States adopt a more robust “layered defense” strategy to address gaps in existing defenses.⁵ The Vision 100 Century of Aviation Reauthorization Act, enacted on December 12, 2003, addressed several aviation security concerns raised by the 9/11 Commission, and soon thereafter the National Intelligence Reform Act of 2004 built on the provisions of the Vision 100 legislation.

PASSENGER SCREENING

Effective passenger screening requires thorough prescreening operations. Since the Federal Aviation Reauthorization Act of 1996, the U.S. government has relied on the Computer-Assisted Passenger Prescreening System (CAPPS), or some version of it, to prescreen passengers.⁶ CAPPS was designed to distinguish low-threat passengers from high-threat passengers so that the luggage of high-threat passengers could receive more scrutiny for explosives. The events of September 11 revealed both the strengths and weaknesses of the CAPPS system. On the positive side, half of the September 11 hijackers were successfully selected by the CAPPS system for additional security screening, and, had the situation been handled properly from that point, the September 11 plot may have been severely disrupted. However, while additional screening procedures meant that the hijackers’ checked baggage was not loaded onto the airplane until the hijackers had boarded, it did not include increased scrutiny of the hijackers or their carry-on items.

When the TSA assumed the responsibility for aviation security it also assumed authority for managing and regulating CAPPS.⁷ In March 2003, the TSA began development of CAPPS II, which would have performed two functions. First, the passenger’s identity would have been authenticated using commercial databases and then the passenger’s name would be checked against terrorist watch lists maintained by the U.S. government. Once flagged, the passenger would be unable to board the flight or would be subjected to secondary screening.⁸ Due to privacy concerns

raised by the Government Accountability Office (GAO) and an internal review by the Department of Homeland Security (DHS), the CAPPS II program was cancelled in August 2004.⁹

As soon as CAPPS II was shot down, TSA announced the development of a prescreening system called Secure Flight. Secure Flight, now the most likely successor to CAPPS, has four main elements. First, the identity authentication process is scaled back. Second, the passenger names will be checked against a wider set of government-maintained watch lists, which are consolidated in the Terrorist Screening Database (TSDB). Third, passengers that are “selected” will be subjected to a more intensive screening and, fourth, passengers who have been misidentified may initiate an appeals process.¹⁰ Pursuant to the recommendations of the 9/11 Commission, the TSDB is a consolidation of “No Fly” and “Automatic Selectee” lists and is maintained by the FBI-administered Terrorist Screening Center. Additionally, TSA is responsible only for prescreening domestic flights under Secure Flight, with prescreening for international flights handled by Customs and Border Protection (CBP) personnel.¹¹

Once prescreening is completed, passengers along with their carry-on baggage are individually screened. This process constitutes the critical second screening function. TSA manages a workforce of approximately 60,000 people, most of whom work as explosives and weapons screeners at airports. Training and developing this workforce has presented a considerable challenge. TSA uses the Online Learning Center to train and retrain its screeners through self-guided courses on the Internet.¹² TSA also conducts unannounced, covert tests at airports to estimate screener performance and uses Threat Image Projection (TIP) software to keep screeners alert by periodically superimposing images of threat objects on X-ray scans.¹³ TSA has also pilot tested a biometric-based screening program called Registered Traveler, which would analyze physical characteristics of frequent passengers to expedite their screening.¹⁴

CHECKED BAGGAGE SECURITY

Prior to the passage of the November 2001 Aviation and Transportation Security Act (ATSA), commercial air carriers were responsible for screening checked baggage for explosives. The passage of ATSA gave TSA the mandate to screen 100 percent of checked bag-

gage by December 2002 using explosive detection machines (prior to ATSA, only a fraction of baggage was screened for explosives).¹⁵ As it became clear in 2002 that many airports would not meet this target, the Homeland Security Act of 2002 extended the deadline to December 2003 for noncompliant airports.¹⁶

Since November 2001, TSA has procured and deployed approximately 1,200 explosive detection system (EDS) machines and 6,000 explosives trace detection (ETD) machines at over 400 airports.¹⁷ The EDS uses computed tomography (CT scan) technology to generate a three-dimensional image of the contents of a bag in order to recognize the characteristic signatures of explosives.¹⁸ EDS machines cost about \$1 million each and are very large.¹⁹ ETD machines, which require a human operator to manually collect a sample from each bag with a swab, work by detecting the residues and vapors of explosives. Relative to EDS machines, ETD machines are \$40,000 less expensive per unit, but much more labor intensive, more vulnerable to human error, and less accurate in detecting explosives.²⁰ Currently, many of the EDS and ETD machines that the TSA has deployed have been placed in airport lobbies, in a “stand-alone” mode, rather than being integrated with baggage conveyor systems.²¹

The 9/11 Commission recommended in July 2004 that the integration of EDS machines “in-line” with baggage conveyor systems be expedited, and that the aviation industry pay some of the cost of installation.²² On October 18, 2005, Congress approved the DHS fiscal year 2006 budget, which allocates \$175 million for the procurement of EDS and ETD systems, as well as \$45 million to install this equipment in-line with baggage conveyors.

To supplement these systems, TSA has also deployed 345 explosives detection canine teams at 66 of the United States’s busiest airports. TSA plans to expand the program to 420 dog teams at 82 airports.²³

AIR CARGO SECURITY

The air cargo system consists of all the freight, express packages, and mail carried aboard cargo and passenger aircraft. These goods move from manufacturers to shippers to freight forwarders and finally

to airport cargo handling facilities where they are loaded onto aircraft.²⁴ With the increasing demand for air shipments over the past twenty-five years, the system is vast, complex, and growing.

In 2004, approximately 23 billion pounds of air cargo were shipped within the United States. Three-fourths of that was shipped on all-cargo aircraft and one-fourth was shipped on passenger aircraft. Typically about 50 percent of a passenger aircraft's capacity is taken up by air cargo, which remains a significant source of income for passenger air carriers.²⁵ It is estimated that by FY2015, domestic air cargo shipments will increase by 50 percent and international shipments by over 85 percent.²⁶

TSA has argued that air cargo is the primary aviation target for terrorists in the short term, and therefore one of the most vulnerable links in the aviation security chain.²⁷ As a result, TSA developed the Air Cargo Strategic Plan in November 2003 focusing on two threats to air cargo security: (1) preventing the introduction of explosives onto passenger aircraft via an air cargo package, and (2) preventing the hijacking of an all-cargo aircraft.²⁸ TSA hoped to address these threats by enhancing air cargo supply chain security, identifying elevated risk through prescreening, developing technology for screening risky cargo, and enhancing security for all-cargo operations. To some extent, TSA still relies on random inspections to evaluate cargo threats, though more comprehensive non-intrusive methods, such as X-ray scans, are being developed.²⁹

TSA is also using the Known Shipper Program to distinguish risky from non-risky cargo. Under the Known Shipper Program, individuals and businesses with an established history are not subject to the same degree of scrutiny as unknown shippers. In addition, unknown shippers are not allowed to ship their freight on passenger aircraft. TSA is in the process of expanding this program—currently only about one-third of air carriers utilize the voluntary central database of known shippers to vet their cargo.³⁰ Non-participating air carriers are using internal databases and security protocols approved by the TSA.

The DHS fiscal year 2006 allocation provides \$55 million for air cargo security. This includes funds to support air cargo inspectors, development and improvement of the Known Shipper Program, and expansion of the canine explosives detection program, among other measures.³¹

SHOULDER-FIRED MISSILE THREAT

Shoulder-fired missile systems, also referred to as man-portable air defense systems (MANPADS), may pose a serious risk to aviation security. These weapons are lethal against aircraft without countermeasures, relatively cheap (only \$5,000 in some markets), and readily available in the international arms bazaar—an estimated 700,000 MANPADS have been produced worldwide since the 1970s.³² In addition, such weapons are lightweight, small, and could be smuggled into the United States with relative ease. Most importantly, al Qaeda and other hostile groups possess and know how to operate MANPADS. In fact, during the recent operations in Afghanistan, numerous MANPADS were recovered from Taliban weapons caches.³³

The RAND Corporation has estimated that the direct cost of having an aircraft shot down would be about \$1 billion, which includes conventional economic valuations of the loss of life.³⁴ If air travel were shut down for one week following an incident, the economic cost would be about \$3 billion, and losses over the following month might bring the total cost to around \$15 billion.³⁵ The National Intelligence Reform Act of 2004 advised the president to vigorously pursue programs that limit the availability and proliferation of MANPADS worldwide. The act also requires that DHS report on the vulnerability of aircraft to MANPADS attacks and devise a plan for securing aircraft from this threat.³⁶ The DHS fiscal year 2006 allocation provides \$110 million for MANPADS countermeasures.

IN-FLIGHT AND CREW MEMBER SECURITY

In-flight security was a clear weakness prior to September 11. Since September 11, a number of security measures, such as hardening cockpit doors, have vastly improved crew member security. The Vision 100 Act required that air carriers provide security training for crew members and recommended arming all-cargo pilots in addition to passenger aircraft pilots.³⁷ The National Intelligence Reform Act

of 2004 called for strengthening initiatives that protect the anonymity of federal air marshals and providing counterterrorism and weapons training for law enforcement officials authorized to carry firearms on passenger aircraft.³⁸

The federal air marshals program is an important component of in-flight security. Originally called the “sky marshals program,” federal air marshals were given an expanded mandate following September 11, including a dramatic increase in the size of the workforce and mandatory deployment on all high-security-risk flights.³⁹ The DHS fiscal year 2006 budget allocation includes \$686 million for the federal air marshals program.

TSA has strengthened its review of crew member security training, including developing a standard form for TSA inspectors to use to document their review of crew member security training.⁴⁰

The recent rash of incidents involving lasers aimed at aircraft cockpits has raised concerns about terrorist use of commercially available lasers to disrupt aircraft operations. None of the 400 recorded incidents involving flight crew exposure to lasers over the past fifteen years were linked to terrorism, though terrorists could plausibly acquire higher powered lasers to incapacitate pilots. Indeed, DHS and the FBI issued a memo in December 2004 stating that terrorists had explored using lasers as weapons.⁴¹

AVIATION WORKER SCREENING

Currently, background checks and displayed identification serve as the primary means for screening aviation workers.⁴² This includes air cargo handlers and any other individuals with access to a passenger aircraft or airfields. The provisions of ATSA provide TSA with the authority to use biometric technology to enhance aviation worker screening procedures, though very few airports currently employ such technology.⁴³ TSA is developing a nationwide transportation workers identification card program, which would provide every aviation worker with a biometric ID card once his or her background check had been completed.

WHERE WE FALL SHORT

SECURITY DEFICITS IN THE CURRENT SYSTEM

PASSENGER SCREENING

There are a number of critical deficits in the current passenger prescreening process. In December 2005, the 9/11 Public Discourse Project gave passenger prescreening an “F” grade, citing delays in implementing the Secure Flight System’s consolidated “No Fly” lists.

The current system both misidentifies low-risk passengers (false positives) and fails to identify high-risk passengers (false negatives). According to one account, TSA was contacted by air carriers as many as 30 times per day with potential name matches. Assuming that a very small fraction of these passengers were actually on the terrorist watch list, false positives are clearly a problem—high-profile misidentifications included Senator Edward Kennedy and Representatives John Lewis and Don Young.⁴⁴ Should they persist, misidentification problems could continue to slow down operations and even undermine public confidence in aviation security measures.⁴⁵ Though cutting down on false positives may prove to be challenging, TSA is hoping that Secure Flight will at a minimum cut down on false negatives by using an expanded terrorist watch list.⁴⁶

The TSA anticipates that Secure Flight will significantly increase the prescreening workload, requiring increases in staff, space, and funding for support operations at the TSA. The TSA remains uncertain, however, about how much of a funding increase will be required to add Secure Flight to TSA regular operations.⁴⁷

Unfortunately, Secure Flight seems to have foundered on problems related to transparency and privacy, the same concerns that unraveled CAPPs II.⁴⁸ Specifically, private organizations and government auditors have raised concerns over widespread collection of passengers’ personal information without procedures for preventing misuse of, and unauthorized access to, that information. Until such issues are resolved, Secure Flight is unlikely to move forward.

The quality of passenger screeners is also a lingering deficiency in the current system. A DHS inspector general’s audit in March 2005

revealed poor screener performance among both federal and contract screeners during covert testing at screening checkpoints.⁴⁹ Part of the problem stems from TSA training policy. The TSA has no formal policies for monitoring the completion of screener training nor has it ensured that all Online Training Centers have the reliable high-speed Internet connections required for online training. As a result, many airports are finding it difficult to keep accurate and up-to-date training records.⁵⁰ Security auditors have also noted that due to insufficient staffing, screeners are not always able to meet the training needs within regular work hours.⁵¹

In addition, most passengers are screened by a metal detector but are not subjected to more thorough explosives detection methods. Only a fraction of passengers have their carry-on items and shoes screened for chemical traces.⁵² The 9/11 Public Discourse Project gave explosives screening at checkpoints a “C” grade, citing the lack of ETD systems at security checkpoints.

CHECKED BAGGAGE SECURITY

The key to improved checked baggage security is rapid deployment of explosive detection systems (EDS) and explosives trace detection (ETD) systems. Several barriers remain in the way of accomplishing this objective. First, given the increase in demand for air travel in the coming decade, the size of EDS acquisitions will need to double from the original estimate following September 11.⁵³

Second, how EDS and ETD equipment should be deployed continues to be debated. The 9/11 Public Discourse Project gave the effort to improve checked baggage screening a “D” grade as a result of delays in the in-line system installation. As of March 2005, TSA had not yet completed a systematic assessment of how to optimally deploy EDS and ETD equipment at over 400 U.S. airports.⁵⁴ Most agree that in-line EDS screening systems are necessary because the current practice of placing stand-alone EDS and ETD equipment in airport lobbies has resulted in crowding, which increases risks for passengers and airport workers.⁵⁵ The estimated cost of integrating EDS systems at all passenger airports is greater than \$4 billion, and installation would take several years to

complete at current funding levels.⁵⁶ Numerous problems exist for ETD systems as well. Relative to EDS machines, ETD machines are less reliable in detecting bombs, are more labor intensive, and have longer processing times per bag.⁵⁷

AIR CARGO SECURITY

As of October 2005, TSA had not yet completed a comprehensive assessment of the vulnerabilities of air cargo and other critical assets, including cargo facilities and cargo aircraft.⁵⁸ TSA has not adapted its vulnerability assessment tools for air cargo assessments nor has it declared when such tools would be ready.⁵⁹ Finally, TSA does not systematically collect information on air cargo security breaches, data that would help assess the system's most vulnerable points.

The Known Shipper Program has its fair share of challenges as well. The information in the known shipper database is submitted voluntarily and, as a result, is incomplete and potentially unreliable. TSA estimates that the database has information about 400,000 known shippers, or less than 30 percent of the estimated 1.5 million shippers.⁶⁰ Though TSA has declared that it plans to make the database mandatory, it has not yet done so. Furthermore, verification of data submitted by shippers has been inadequate. Currently, there is very little investigation of a shipper's credibility, and to what extent that shipper is using approved security measures to ensure the integrity of its freight.⁶¹

TSA is also struggling with the challenge of screening cargo containers and cargo unit loading devices (ULDs) reliably and rapidly. Under current technological constraints, it is not feasible to scan every container and ULD and retain the speed of shipment to which most commercial carriers are accustomed.⁶²

Hardened unit loading devices (HULDs) are also being considered as a means of mitigating the threat of a cargo-borne bomb. These containers must withstand an explosive blast without rupturing and must also self-extinguish any post-blast fire.⁶³ The drawbacks of using HULDs are numerous: increased weight affecting aircraft range and payload capacity, high procurement costs, and incompatibilities with current airframes, to name a few.⁶⁴ The 9/11 Commission recommended the

deployment of at least one hardened container on every passenger aircraft—on the Boeing 747, however, this accounts for less than 10 percent of available cargo storage area.⁶⁵

SHOULDER-FIRED MISSILE THREAT

Though every passenger aircraft in the United States is vulnerable to shoulder-fired missiles, we are still relatively far from installing countermeasures on aircraft. As with other areas of aviation security, a layered defense is required because no countermeasure will be 100 percent effective against MANPADS. A layered defense should include securing a perimeter around airports and improving an aircraft's ability to survive missile-induced fire damage.⁶⁶

IN-FLIGHT AND CREW MEMBER SECURITY

As of September 2005, the TSA had not yet established goals and performance measures for crew member security training, arguing that individual air carriers are responsible for setting their own goals and measuring performance.⁶⁷ The TSA is indisputably responsible for monitoring air carrier compliance with TSA-established training standards, but lacks the internal controls for regulating and reviewing air carrier compliance.⁶⁸ Observers of the current training system complain about the lack of recurrent, realistic training, and the instructors' lack of knowledge about the actual in-flight operating environment.⁶⁹

All-cargo aircraft also face important security challenges. Unlike passenger aircraft, all-cargo airplanes do not have hardened cockpit doors or federal marshals to thwart a hijacking attempt. Physical security and access control to cargo operations is also less strict than passenger aircraft security, making all-cargo aircraft an especially inviting target to terrorists.⁷⁰

Finally, the federal air marshals program has successfully expanded its mandate and operations, though it has failed to create a mechanism

for marshals to systematically document security incidents that occur during their missions.⁷¹ If federal air marshals do not adequately use, manage, and analyze mission reports, we may miss a valuable opportunity to detect terrorist mission planning and reconnaissance activity.

AVIATION WORKER SCREENING

A major concern for aviation worker screening is the possibility that unauthorized individuals could gain access to secure facilities with stolen or fraudulent identification. In addition, air cargo workers and cargo handlers do not receive formal security training for identification of suspicious activity or training in procedures to reduce physical security breaches.⁷²

RECOMMENDATIONS

The following section outlines how we can begin to address many of these security challenges.

13.1. PASSENGER SCREENING. The TSA needs to bring Secure Flight online as rapidly as possible. This will require addressing the privacy concerns raised over the government's collection of personal information. Most importantly, TSA must assure passengers that their personal information will be strictly safeguarded from unauthorized use, and will be used only for the purposes of distinguishing high-risk from low-risk passengers. In other words, for the limited personal information a passenger gives up, he or she gains volumes in aircraft security. The TSA may also consider segmenting the passenger population into travelers who are willing to give extra personal information for Secure Flight and those who are not willing to provide information. Those who are not willing may be subjected to extra prescreening and checkpoint screening as a result. It is plausible that many passengers will decide that their desire to save time outweighs their desire to remain anonymous.

Several technologies may potentially help to improve passenger screening at security checkpoints. One option is the multiview X-ray,

which provides screeners with much higher resolution images that can be rotated on the screening monitor in order to improve detection rates.⁷³ A second and more traditional option is to expand the canine explosive detection teams to operate at security checkpoints.

To keep screeners sharp and alert, the TSA should expand the use of the Threat Image Projection (TIP) program, wherein fictitious threat objects are superimposed on actual images of passenger bags. TIP is doubly effective as it can be used both to train and to evaluate screeners.⁷⁴ Airports should also be allowed to opt out of using federal screeners by hiring private contractor screeners if the airport determines that screening operations could be carried out more efficiently and effectively with private contractors.

Biometric identity verification is the obvious next step to enhancing screening effectiveness. The TSA's Registered Traveler pilot program, which uses iris and fingerprint verification, was completed on September 30, 2005, and seems to have been a widespread success. The TSA should aim for a quick review and expansion of this program to all major airports.

On a positive note, the TSA has indicated that it will soon vary its security checkpoint procedures on a regular basis in order to prevent terrorists from studying and exploiting weaknesses in the security protocols.⁷⁵ TSA should be sure, however, that variation in screening procedures doesn't result in a loss in screener capability.

13.2. CHECKED BAGGAGE SECURITY. TSA should develop a plan to rapidly deploy in-line EDS systems at the busiest passenger airports, and ultimately at all passenger airports. The current DHS fiscal year appropriation of \$175 million for acquiring EDS systems will provide for only a fraction of the systems that are required.

Screener training also needs improvement. Screeners should have access to ongoing training and every Online Training Center should be available by high-speed Internet so that trainers can access and complete training courses more rapidly. TSA should also systematically monitor and document the completion of required screener training.

13.3. AIR CARGO SECURITY. First and foremost, TSA should screen all of the cargo that travels by passenger aircraft with canine explosives detection teams and machines. Backscatter X-ray machines that emit low-dose X-rays are compact, lightweight, and reduce the need for

shielding of screeners.⁷⁶ Such devices can be mounted on moving platforms and used to scan over containers.

Cargo containers should also be sealed with tamper-evident tape, which offers a visual indication of tampering at a very low cost.⁷⁷ Such a measure would be easy to implement during packaging as well.

The use of HULDs should also be explored more vigorously. The National Intelligence Reform Act of 2004 required that the TSA test the use of HULDs for the purpose of determining the feasibility, cost, and logistical difficulties associated with an HULD system. The TSA has not yet released a final ruling on whether this option is feasible.

The TSA should make the Known Shipper Program mandatory for air carriers and known shippers—the current practice of voluntary participation has captured a meager one third of all known shippers. Importantly, the TSA must develop strict monitoring procedures to verify that shippers in the database are actually securing their cargo according to TSA standards. Without verifying shipper compliance, the Known Shipper Program could turn into a worthless investment.

13.4. SHOULDER-FIRED MISSILE THREAT. If a shoulder-fired missile system were used against a commercial aircraft the result would be catastrophic. The TSA should vigorously explore and test countermeasures for airlines against these weapons. Countermeasures should contribute to a layered defense, including securing a perimeter around airports that would prevent an attacker from firing within range of the missile system.⁷⁸

There are several countermeasure options available. Pyrophoric flares are relatively inexpensive, though their effectiveness during a MANPADS attack is not well established. Ground-based high-energy lasers (HELs) would be effective against MANPADS of any sophistication, but will not be available to deploy for several years. Laser jammers, which would be installed directly onto each aircraft, would be capable of defeating all MANPADS currently held by terrorists and are commercial available. RAND estimated that it would cost about \$11 billion to equip every aircraft in the U.S. fleet with a laser jammer. RAND further estimated that the full ten-year life-cycle costs of developing, installing, and maintaining laser jammers would be between \$20 billion and \$40 billion.⁷⁹

Unfortunately, time is not on our side with this problem. The TSA should settle on the superior alternative and accelerate development beyond the current pace.

13.5. IN-FLIGHT AND CREW MEMBER SECURITY. The first step toward improving in-flight security is for the TSA to fund and monitor mandatory self-defense and security training for flight crews rather than relying on air carriers to train their own flight crews according to varying standards.

Though the risk of high-powered lasers disrupting flight operations is relatively remote, the TSA should explore the development and installation of special visors on cockpit windows whose light-blocking properties would be activated only when a laser threat is detected—technology already in development by the Department of Defense.⁸⁰

The TSA should mandate that federal air marshals establish a standard procedure for compiling, analyzing, and responding to mission reports of security incidents.

13.6. AVIATION WORKER SCREENING. The key to protecting the air cargo system from attack is to develop higher standards of identity verification for security workers and higher standards of physical security at facilities in the cargo supply chain.

This begins with training air cargo workers to spot suspicious behavior and by screening them and their personal belongings when they enter secured airfield facilities—particularly when they have access to passenger aircraft. TSA should aggressively pursue development of biometric verification for all aviation workers. The Transportation Workers Identification Card is a good start and should be expanded to include all passenger airports and major air cargo shipping ports.

