

1.

AVIATION SECURITY

E. Marla Felcher

Adjunct Lecturer, John F. Kennedy School of Government, Harvard University

Five weeks after the September 11, 2001 attacks, President Bush signed the Aviation and Transportation Security Act (ATSA), creating the Transportation Security Administration (TSA). Housed within the Department of Transportation, TSA was responsible for protecting the nation's transportation systems, including aviation, waterways, rails, highways, public transit, and pipelines. Most of TSA's resources have gone toward securing the aviation system; \$4.5 billion of the agency's \$4.8 billion budget in fiscal year 2002 was spent on aviation security, as was \$6.1 billion of its \$7.1 billion budget in fiscal year 2003. TSA was transferred from the Department of Transportation to the Department of Homeland Security on March 1, 2003. (See appendix for a detailed timeline).

The nation's aviation system is undoubtedly more secure today than it was on September 11, 2001. During its first year, TSA made significant progress laying the groundwork for the nation's new security regimen. The agency hired tens of thousands of airport checkpoint screeners, whose job it was to prevent airline passengers from carrying dangerous weapons on board planes. After becoming a DHS agency, TSA completed background checks on all of these screeners, a measure intended to prevent non-U.S. citizens and people with criminal histories from holding the job.

TSA also made impressive progress installing equipment in airports to screen passengers' checked luggage. Now, 100 percent of all suitcases are screened for explosives, compared to 5 percent pre-TSA. Significant improvements have also been made to the federal air marshal program. Pre-TSA, the program employed just 33 agents; today between 4,000 and 6,000 undercover agents protect passengers on international and domestic flights. (Their exact number and the flights they are on are both closely guarded secrets.)

Still, much remains to be done. Questions have been raised concerning the adequacy of the checkpoint screeners' training and testing, as well as TSA's lack of screener performance data. While the agency keeps track of how many dangerous weapons the screeners are intercepting from passengers, it does not have a good handle on how many dangerous weapons screeners are failing to detect. In the past, government studies in which undercover agents attempted to smuggle simulated weapons through security checkpoints found alarmingly high successful infiltration rates; but a recent General Accounting Office report found that the TSA has done little to measure screener performance in detecting "threat objects." Undercover tests conducted by people outside TSA have demonstrated, however, that it is still possible for passengers to carry weapons onto planes.

TSA has also made some, but certainly not enough, progress on its passenger profiling system, CAPPS II, a computer program intended to identify terrorists after they buy an airplane ticket, but before they board a plane. After missing multiple deadlines, TSA estimates CAPPS II will be implemented in the fall of 2005. Another technologically sophisticated program, a Transportation Workers Identification Credential (TWIC), is still in development. TWIC cards will prevent unauthorized people from entering secure areas of airports.

Two important but largely neglected sectors of the aviation industry, air cargo and general aviation (private planes), remain as vulnerable to terrorist attack today as they were on September 11, 2001. Despite repeated warnings from the General Accounting Office, the Department of Transportation inspector general,

and members of Congress, TSA has taken few measures to secure these gaping holes in the aviation security system.

BACKGROUND: BUILDING THE POST–SEPTEMBER 11 AVIATION SECURITY REGIMEN

Congress initially allocated \$2.4 billion for TSA to get started, and President Bush was quick to appoint John Magaw, a former head of the Secret Service, as TSA's first leader.¹ The combination of the Aviation and Transportation Security Act's sweeping mandates, Congress's generous budget allocation, and Magaw's law enforcement background sent a strong message that the U.S. government was determined to thoroughly reform and augment aviation security.

Prior to the September 11, 2001 terrorist attacks, aviation security was the joint responsibility of the Federal Aviation Administration (FAA) and the airlines. The FAA (a Department of Transportation agency) provided oversight, and the airlines provided and paid for security. There was widespread agreement within the U.S. government that this arrangement had created a system that was not secure. (Poorly trained airport checkpoint screeners, many of whom were not U.S. citizens, were often paid less than workers at airport fast food restaurants). There was decidedly less agreement, however, on what it would take to secure the system. The Aviation and Transportation Security Act read like a laundry list of all the security measures Congress and the FAA had contemplated, yet failed to institute, over the past fifteen years.

Transportation Secretary Norman Mineta gave the job of transforming the Aviation and Transportation Security Act's mandates into specific security programs to his Deputy Secretary Michael Jackson. Jackson viewed aviation security as a ring of protective layers around an aircraft that would protect it from

¹ Schneider, Greg and Sara Kehaulani Goo, "Twin Missions Overwhelmed TSA," *Washington Post*, September 3, 2002, p. A1.

terrorist attack.² Individual security programs would not necessarily keep a terrorist from hijacking or blowing up a plane, but cumulatively the layers would provide adequate protection. Some of TSA's security programs would keep dangerous *objects* off planes—a new workforce of stringently trained airport checkpoint workers would screen passengers and their carry-on bags, and high-tech explosives-detection systems would scan passengers' checked luggage for bombs. Other measures would keep dangerous *people* away from planes—criminal background checks for airport screeners, an airline passenger profiling system capable of flagging terrorists after they bought an airplane ticket but before they boarded a plane, and airport access controls that would keep unauthorized people from entering an airport's secure areas, such as airfields and baggage handling rooms. The innermost layer of protection, undercover air marshals positioned in First Class seats, would be a last-ditch effort to protect the aircraft's passengers and crew if the outermost layers failed.

The Aviation and Transportation Security Act set forth unambiguous, quantifiable goals for the two layers of the new security regimen Congress deemed most urgent—passenger and luggage screening. Specifically, TSA was to:

- Hire, train, and deploy a new federal workforce of airport checkpoint screeners to all of the nation's (429) commercial airports by November 19, 2002, and
- Purchase and install explosives-detection systems to scan passengers' checked luggage in all of the nation's (429) commercial airports by December 31, 2002.

Congressional staffers estimated TSA would need to hire a workforce of 28,000 airport checkpoint screeners and purchase about 1,000 explosives-detection systems (costing about \$1 million each). TSA's ability to complete this

² Brill, p. 105.

work within the time frame specified by Congress would become the metric by which its oversight committees, and the American people, would judge its efficacy.

RECOVERING FROM THE SCREENER DEPLOYMENT DEBACLE

TSA chief John Magaw struggled in his new job. When it became clear, very early on, that Congress had grossly underestimated the number of screeners needed to secure airport checkpoints, Magaw appeared before TSA's House appropriations subcommittee to ask for more money. Chairman Harold Rogers (R-KY), who had been opposed to federalizing aviation security from the start, set the tone for this and many of the agency's hearings to come. Rogers, along with a number of his Democratic and Republican colleagues in both the House and Senate, chastised Magaw for hiring too many people and running through his budget too quickly.³ Many feared that TSA was becoming a bloated government bureaucracy, incapable of meeting its goals.

Six months into his deadline, John Magaw had not deployed federal screeners to a single airport.⁴ The TSA chief insisted he would meet his goals, but many in Congress and the White House were pessimistic. At the same time, airline passengers were losing patience with the interim, private-workforce screeners who, in their efforts to provide more thorough security, were creating long lines and hour-long waits at airport checkpoints. The airline industry complained that TSA's first leader was taking the new security drill too far. President Bush did not ignore these concerns; he fired John Magaw in July 2002.⁵

Less than four months later, on November 19, 2002, DOT Secretary Norman Mineta and Admiral James Loy, Magaw's replacement, announced that

³ *FDCH Political Transcripts*, "U.S. Representative Harold Rogers (R-KY) Holds Hearing on Transportation Security," June 20, 2002.

⁴ Schneider, Greg and Sara Kehaulani Goo, "Screening Deadline Worries Grow," *Washington Post*, June 14, 2002, p. A9.

⁵ *Ibid.*

TSA had met Congress's deadline and deployed federal screeners to all 429 airports.⁶ 44,000 screeners had been hired. It would take another six months for Congress to fully understand the downside of their myopic focus on TSA's ability to meet hastily formulated benchmarks.

The Aviation and Transportation Security Act required the new federal screeners to undergo background checks to ensure that TSA employees were not, themselves, criminals or security threats.⁷ Yet, during the first six months of 2003, airline passengers had filed more than 6,700 complaints accusing TSA employees of stealing cash, jewelry and computers.⁸ New York City police had arrested multiple TSA screeners for offenses that included possession of drugs and an illegal Mach Ten machine gun. Twelve screeners at the Los Angeles International Airport, who had badges giving them access to secure areas of the airport, were found to have criminal records related to "the unlawful use, sale, distribution or manufacture of an explosive or weapon."⁹ By the end of 2003, TSA had fired more than 1,900 airport workers nationwide, at least 500 of whom had been arrested or convicted of crimes (including rape, manslaughter, and burglary) and others who had lied on their job applications.¹⁰

The problem was that criminal background checks were a more complex, time-consuming process than Congress had anticipated. The tens of thousands of applicants who had applied for TSA screener jobs had been given English-language competency, medical, object-recognition, and baggage-lifting tests. Passing these tests *initiated* the background checks, a process that required the coordination of multiple government agencies, including the FBI, Immigration and Naturalization Service (INS), the Department of Defense, and the Office of

⁶ "Federal Security Screeners Successfully Deployed at All U.S. Airports," TSA Press Release, November 18, 2002, www.tsa.gov.

⁷ *GAO Report 02-971T*, "Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges," July 25, 2002.

⁸ Goo, Sara Kehaulani, "TSA Under Pressure to Stop Baggage Theft," *Washington Post*, June 29, 2003, p. A1.

⁹ Goo, Sara Kehaulani, "Airport Finds That More Screeners are Questionable," June 12, 2003, p. A3.

¹⁰ *FDCH Political Transcripts*, "U.S. Representative Christopher Cox (R-CA) Holds Hearing on Homeland Security Progress," May 20, 2003, p. 12, and, "Shenon, Philip, "Report Faults Lax Controls on Screeners at Airports," *The New York Times*, February 6, 2004.

Personnel Management. As of the summer of 2003, the *majority* of TSA's checkpoint screeners, 30,000 employees, had not completed this process.¹¹ Yet many had been working in airport jobs for seven months. If TSA had waited for the background checks to be completed, the agency would have missed Congress's screener deployment deadline.

Background checks were not the only task TSA officials let fall by the wayside in their rush to deploy tens of thousands of new workers to airports within a year. In September 2003, the General Accounting Office released a report describing TSA's screener training program as "remedial."¹² A month later, the TSA inspector general reported that most of the questions on the screeners' written test had been rehearsed with the applicants immediately before the exam and that many of the "simplistic" questions were "phrased so as to provide an obvious clue to the correct answer."¹³ After reading the exam questions, Senator Charles E. Schumer (NY), head of a Democratic task force on Homeland Security, said, "When you read the test, you'd think it was written by [comedian] Jay Leno's scriptwriters rather than by a testing agency."¹⁴

Despite the deficiencies in the screeners' training and testing, it is nonetheless possible that the new TSA employees would have been capable of performing the job they had been hired to do: keeping passengers from carrying dangerous objects onto planes. Ultimately, this is the only screener performance measure that matters. Press releases issued by TSA suggest that the screeners are in fact passing this on-the-job test with flying colors. During its first year in business, TSA reported, checkpoint screeners intercepted more than 4.8 million prohibited items, including 1,101 firearms, nearly 1.4 million knives, 2.4 million

¹¹ *Federal News Service*, "Hiring Practices for the Transportation Security Administration's (TSA) Screener Workforce," Hearing of the Homeland Security Subcommittee of the House Appropriations Committee, June 3, 2003.

¹² *GAO Report 03-1173*, "Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining," September 24, 2003.

¹³ Wald, Matthew L., "Official Says Airport Trainees Knew Questions Before Test," *New York Times*, October 8, 2003.

¹⁴ Wald, Matthew L., "Official Says Airport Trainees Knew Questions Before Tests," *The New York Times*, October 9, 2003.

sharp objects, 40,000 box cutters, 125,000 flammable objects, and 15,700 clubs.¹⁵ In August 2003, TSA lauded its screeners for confiscating “artfully concealed items,” including a handgun stuffed inside a plush teddy bear, a child’s car seat that was used to conceal a knife, and a “statue artifact” concealing a sword.¹⁶

There is no doubt that air travel is safer when vigilant screeners prevent passengers from boarding planes with handguns, knives, and swords. But the measure offered by TSA—the number of prohibited items screeners have detected—tells just part of the story. Assessing the extent to which TSA screeners have improved aviation security requires the agency to answer one more question: *How many dangerous objects are screeners failing to detect and intercept?* The answer to this question, according to the September 2003 General Accounting Office report, is: *No one knows.*¹⁷ “TSA currently collects little information,” the GAO said, “to measure screener performance in detecting threat objects.”¹⁸

While there may be a dearth of screener performance data *within* TSA, multiple news organizations, and at least one private citizen, have conducted their own screener tests. The results are not encouraging. On Labor Day weekend 2002, a team of *New York Daily News* reporters got carry-on bags packed with pepper spray, rubber-handled razor knives, box cutters, and razor blades onto planes in eleven airports.¹⁹ In July 2003, *WBNS News* in Ohio hired former FAA undercover agent Steve Elson to see if he could get lead-lined film bags through airport security.²⁰ The lead lining, intended to protect film from being damaged by x-ray machines, also shields the bags’ contents from screeners. Because a weapon concealed in such a bag would appear as a big black blob, screeners are instructed

¹⁵ “Air Travelers’ Security Enhanced as TSA Intercepts Over 4.8 Million Prohibited Items in First Year, Including 1,101 Firearms,” TSA press release, March 10, 2003, www.tsa.gov.

¹⁶ “Artfully Concealed Items Confiscated by TSA Screeners,” TSA press release, August 25, 2003, www.tsa.gov.

¹⁷ “Air Travelers’ Security Enhanced as TSA Intercepts Over 4.8 Million Prohibited Items in First Year, Including 1,101 Firearms,” TSA Press Release, March 10, 2003, www.tsa.gov.

¹⁸ *GAO Report 03-1173*, September 24, 2003.

¹⁹ Becker, Makki and Greg Gittrich, “Weapons Still Fly at Airports,” *Daily News*, September 4, 2002, p. 7.

²⁰ McCoy, Roger, “Airport Security Test Finds Faulty Screenings,” *Columbus Dispatch*, July 29, 2003, p. 4B.

to search these carry-on bags by hand. The first time Elson passed through security, the TSA screener correctly followed protocol: he opened the bag, hand-searched its contents, and sent it through the x-ray machine twice. Yet subsequent tests were disappointing; at three different checkpoints screeners failed to inspect the lead-lined bags by hand. Then, in October 2003, a college student stashed box cutters and other dangerous items on four Southwest Airlines planes, where they sat for weeks before they were discovered. The student claimed his goal was to bring public attention to what he perceived to be ongoing lapses in security.²¹

TSA officials described the media tests as “unrealistic” and “alarmist” and denied that they are an accurate measure of screener performance. In response to the college student’s actions, TSA deputy administrator Steven McHale said, “Amateur testing like this does not in any way assist us or show us where we have flaws in our system.”²² The agency announced, however, that it has recently completed a “screener performance improvement study” and is “taking steps to address (performance measurement) deficiencies identified” by the General Accounting Office.²³

CONTRACTOR OVERSIGHT AND COST CONTROLS: CLAIMS OF IMPROVEMENT AFTER A BAD START

As a brand new agency, TSA did not have an adequate workforce in place to simultaneously build an organization *and* implement a host of new aviation security programs. Some employees had been transferred to TSA from the Federal Aviation Administration, but there were still hundreds of staff jobs to be filled and tens of thousands of airport workers to hire. The only chance the new agency had of meeting Congress’s deadlines was to rely heavily on private sector contractors to do the bulk of TSA’s early work. The Department of Transportation awarded

²¹ Goo, Sara Kehulani, “TSA to Check Plane Inspections,” *Washington Post*, October 22, 2003, p. A10.

²² No byline, “Holes in TSA’s Screens,” *Washington Post*, October 22, 2003, p. A28.

²³ *GAO Report 03-1173*, September 24, 2003.

\$8.5 billion to contractors in 2002, among them, Lockheed Martin (\$370 million for checkpoint “lane reconfiguration”), VF Solutions (\$17 million for TSA screener uniforms), Boeing (\$508 million for explosives-detection machines), Accenture (\$215 million for ongoing human resources support), and NCS Pearson (\$103 million to recruit the TSA screeners).²⁴ The combination of TSA’s tight deadlines, Congress’s initially generous budget allocation, and lax contractor oversight became a recipe for wasteful spending and contractor billing abuses.

During the first few months when TSA was getting organized, FAA legal and purchasing staff helped TSA award contracts to the interim screening companies that would provide screeners between November 2001, when the Aviation and Transportation Security Act became law, and November 2002, when TSA had hired its own screener workforce. During this time, FAA entered into agreements with 74 companies, obligating TSA to \$1 billion.²⁵ Rushing to get the job done, FAA staff didn’t have time to negotiate the contracts. Instead, they issued “letter contracts” stipulating that the contractors would bill the TSA about what they had charged the airlines for screeners in 2000. Yet, half of the contractors reneged on this promise and ultimately charged TSA between 50 and 100 percent more than the amount they had charged the airlines a year earlier, accounting for at least \$300 million in overcharges.²⁶

TSA also was overcharged by the contractor responsible for hiring the TSA screener workforce, NCS Pearson. One of the factors contributing to the delay in screener background checks was NCS Person’s sudden departure after the company’s initial \$103.4 million contract had ballooned inexplicably to \$700 million.²⁷ Government auditors eventually learned that Pearson had billed TSA more than \$5 million for New York-area screeners to live for up to six months in

²⁴ *FDCH Political Transcripts*, “Hearing on Aviation Security,” Senate Commerce Committee, Aviation Subcommittee, February 5, 2003; www.tsa.gov.

²⁵ Letter from J. M. Loy, ADM, Under Secretary of Transportation for Security, to Kenneth M. Mead, inspector general, “Oversight of Security Contracts,” January 21, 2003.

²⁶ Letter from Alexis M. Stefani, Principal Assistant Inspector General for Auditing and Evaluation, to J.M. Loy, Under Secretary of Transportation for Security, February 28, 2003.

²⁷ *FDCH Political Transcripts*, “U.S. Representative Christopher Cox (R-CA) Holds Hearing on Homeland Security Progress,” May 20, 2003, p. 12.

hotels and for recruiters to stay for multi-week stretches at luxury resort hotels in Florida, the Virgin Islands, Colorado, and Hawaii.²⁸

In the summer of 2003, TSA chief Loy reported that TSA had made considerable progress creating the systems it needs to monitor the costs and performance of its contractors and that the situation would continue to improve.²⁹

PROGRESS ON INSPECTING CHECKED LUGGAGE

Congress mandated TSA to install explosives-detection systems in every U.S. airport to screen every piece of checked baggage by December 2002. The agency made an impressive effort to meet this deadline but was ultimately unable to do so. The major hurdles were funding and space; Congress did not allocate enough money for airports to integrate the explosives-detection systems into their baggage-handling systems, and many airports did not have anywhere to put the minivan-sized machines. The Homeland Security Act extended TSA's baggage screening deadline and gave the agency the authority to implement "alternate screening methods" for up to another year. Among the methods that TSA approved to replace the explosives-detection systems were trace-detection machines (a cotton swab is run across the outside of luggage and tested for traces of explosive chemicals), explosives-sniffing dogs, and physical hand searches.³⁰ TSA came close to making the extended December 2003 deadline but missed that one as well; explosives-detection systems are still not installed in five airports.³¹

Airport operators continue to complain that their efforts to integrate explosives-detection systems equipment into baggage handling systems are being

²⁸ Fiandaca, Cheryl, "Airport Screeners Live it Up at Taxpayer Expense," www.abclocal.go.com, May 7, 2003; Ramstack, Tom, "Investigators Audit Expenses of Arlington, VA Airport Security Contractor," *Washington Times*, July 17, 2003; Miller, Leslie, "Perks of Air Screeners' Trainers Probed," *Washington Post*, July 16, 2003.

²⁹ Barr, Stephen, "A Vow to Closely Oversee Personnel Management Contracts," *Washington Post*, July 31, 2003, p. B2.

³⁰ Goo, Sara Kehaulani, "Large, Small Airports to Use Different Security Systems," *Washington Post*, March 28, 2002, p. A5.

³¹ *GAO-04-285T*, "Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs," November 20, 2003.

thwarted by Congress's reluctance to allocate enough money for them to get the job done. Many of the machines remain in airport lobbies, thus requiring multiple screeners to take the checked luggage from passengers, run the suitcases through the explosives-detection machines, and then transport them to baggage handling rooms. What prevents this labor-intensive process from being mechanized is money; it will cost airports between \$1 and 3 million to integrate each explosives-detection machine into their baggage handling systems. So far, TSA has promised seven airports a total of \$700 million to get the job done and has identified another 25 to 35 airports as candidates for integration. But until Congress authorizes the funding, which has not yet occurred, the work cannot begin and the machines will remain in airport lobbies.

Despite these infrastructure problems, there is good news: According to a recent Department of Transportation inspector general investigation, all checked bags are now being screened for explosives in some way.³² This is an impressive accomplishment for TSA, given that before the agency existed, only 5 percent of checked luggage was inspected.

IMPROVEMENTS IN THE OUTER- AND INNER-MOST LAYERS OF SECURITY

The TSA deserves additional credit for making some limited progress on several other realms, including passenger profiling, air marshals, and airport perimeter and access controls:

Computer-Assisted Passenger Prescreening System: CAPPS II

TSA's passenger profiling system, Computer-Assisted Passenger Prescreening (CAPPS II), is considered by many security experts to be the most important layer

³² Ibid.

of its “system of systems.” CAPPS II will integrate vast amounts of information on every airline passenger, including demographic data (e.g., name, date of birth, address) and information held by other government agencies such as INS and the FBI, to compute a passenger “risk score.” Airport screeners will use the score to determine the level of scrutiny to which each passenger will be subjected before being allowed to board a plane.

The CAPPS II deadline, originally set to be June 2004, has been moved to the fall of 2005, due in large part to the unexpected level of public criticism over personal privacy concerns prompted by TSA’s ambitious data collection efforts. An early prototype of the CAPPS II program gave TSA access to what was considered by some to be *too much* personal information, including where passengers had lived in the past, who their neighbors had been, the charities to which they had donated money, to whom they had been married and for how long, and details of their health and financial histories. The American Civil Liberties Union and the National Association for the Advancement of Colored People were among the many organizations objecting to the scope of the information to be collected by TSA, how long it would be stored in government computers, and who would get to see it.³³

In response, TSA scaled back its data collection plans. In September 2003, the agency announced that financial and health information will not be part of the profiling database, as was TSA’s original plan. The agency also promised that passenger data will be purged within a few days of the flight being finished, and that private companies involved in the data collection process will be prohibited from retaining the output in a “commercially usable form.”³⁴ The original CAPPS II plan would have allowed TSA to keep some information for up to 50 years.

Privacy advocates were cautiously optimistic after TSA announced these safeguards. But in September 2003, a blunder by three-year-old discount airline JetBlueAirways demonstrated that airline passengers had a right to be concerned

³³ O’Harrow, Robert Jr., “TSA Modifies Screening Plan,” *Washington Post*, June 14, 2003, p. E1.

³⁴ Loy, James M., “Privacy Will be Protected,” *USA Today*, March 12, 2003, p. 12A and O’Harrow, Robert, Jr., *Washington Post*, June 14, 2003.

about losing control of their personal data. The airline acknowledged that it had given the Pentagon information on five million of its passengers, without their consent, including their names, addresses, and phone numbers.³⁵ The Pentagon, in turn, passed the information to a private sector contractor who had used it to identify passengers' Social Security numbers, occupation, income, home- and car-ownership history, as well as the number of adults and children living in the passenger's household. The Pentagon intended to use the data for research on its own "airline passenger risk assessment" system.³⁶ The airline's indiscretion rekindled an intense level of public outrage, including multiple class action lawsuits filed against JetBlue on behalf of its passengers.

JetBlue had shared its data with the Pentagon, not with TSA. But *which* federal agency was responsible was of little concern to those who felt their privacy had been invaded. This point did not go unnoticed by the airlines, whose participation TSA very much needs to continue testing CAPPs II. As of the end of 2003, the agency had not been able to convince a single airline to hand over its passenger data for a CAPPs II pilot program.³⁷ The debate over passenger privacy was ratcheted up another notch in January 2004, when Northwest Airlines acknowledged that it had provided the National Aeronautics and Space Administration three months of its passengers' reservation information shortly after the September 11 attacks, despite the airline's previous claims that it had never given such information to anyone.³⁸

Acting TSA Administrator David M. Stone has the authority to *force* the airlines give him their data by issuing a security directive, similar to orders the agency issues to airports and airlines when security is heightened. Stone says this

³⁵ Power, Stephen, "TSA Chief Pushes Screening System," *Wall Street Journal Abstracts*, September 29, 2003, p. A12.

³⁶ Shenon, Philip, "Airline Gave Defense Firm Passenger Files," *New York Times*, September 20, 2003, p. A1.

³⁷ Goo, Sara Kehaulani, "TSA May Try to Force Airlines to Share Data," *Washington Post*, September 27, 2003, p. A11.

³⁸ Goo, Sara Kehaulani, "Northwest Gave U.S. Data on Passengers: Airline Had Denied Sharing Information for Security Effort," *Washington Post*, January 18, 2004, p. A1.

is exactly what he intends to do if the airlines do not agree to participate voluntarily.³⁹

In November 2003, the General Accounting Office's director of Homeland Security and Justice, Cathleen A. Berrick, testified before the House Committee on Government Reform on the state of the CAPPS II system. Berrick⁴⁰ reported that the many challenges TSA is currently facing with CAPPS II—how to ensure the accuracy of CAPPS II data, the ability of TSA to redress erroneous information, and how to prevent a “high-risk” person from stealing the identity of a “low-risk” person and subsequently boarding a plane—may in fact significantly impede the agency's ability to implement the system. The GAO is in the midst of an extensive CAPPS II investigation and expects to release its findings in 2004.

Federal Air Marshals

On September 11, 2001, the U.S. federal air marshal program employed just 33 undercover agents, whose job it was to prevent hijackings on U.S. commercial aircraft. The program's budget, about \$4 million a year, covered only a handful of international flights; the 20,000 domestic flights that took off from domestic airports each day were unprotected by the highly trained agents.⁴¹

By the summer of 2002 TSA had hired between four and six thousand new undercover air marshals (the exact number is classified information), who were to guard the cockpits of both international and domestic flights, typically from First Class seats.⁴² Congress had given TSA \$1 billion to resuscitate the program.

³⁹ TSA Administrator James Loy was appointed Deputy Secretary at the Department of Homeland Security on October 23, 2003. Rear Admiral David M. Stone replaced Loy on December 4, 2004, as TSA's Acting Administrator.

⁴⁰ Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs. GAO-04-285T November 20, 2003

⁴¹ Schiavo, Mary, *Flying Blind, Flying Safe*, Avon Books, New York, New York, 1997.

⁴² The exact number of air marshals is classified information. However, in an August 15, 2002 article, *USA Today* reporter Blake Morrison wrote, “Although the precise number of marshals is classified, sources say about 6,000 have been hired since Sept. 11,” p. 1A. Another story, run four months later, put the air marshal force at “more than 4,000.” No byline, “Air Marshals Reveal Security Lapses,” *USA Today*, December 24, 2002, p. 11A.

Although the program had been well funded, there were still problems. Lured from jobs with police departments, U.S. Customs and Border Patrol, the new agents found that the reality of their workday fell short of what TSA recruiters had promised. The program was disorganized, many marshals complained, the training was inadequate, and 12- and 16-hour workdays sitting on planes were simultaneously monotonous and exhausting. During one 18-day period in the summer of 2002, 1,250 unhappy marshals called in sick. By the end of the month, at least 250 had quit.⁴³

TSA chief Loy worked with Department of Homeland Security officials to find a solution. By September 2003, they had settled on a plan: air marshals were to be transferred out of TSA and into the Bureau of Immigration and Customs Enforcement, a new Department of Homeland Security agency.⁴⁴ Immigration agents, customs officers, and air marshals would be cross-trained to perform all three jobs. The move would more than double the number of air marshals to 11,000 by creating a system of “reserve” agents who would be placed on planes only when the Department of Homeland Security perceived an increased threat to aviation security. The new plan was a positive step toward improving air marshal morale. But the move had broader long-term implications: transferring the air marshal program out of TSA demonstrated the Department of Homeland Security’s ability to respond to a difficult problem quickly and to implement a solution that resulted in a more efficient use of agency resources.

Airport Perimeters and Access Controls

The Aviation and Transportation Security Act required airports to strengthen the security of their perimeters, airfields, jetways, and baggage handling rooms. TSA

⁴³ Schneider, Greg and Sara Kehaulani Goo, “For Air Marshals, A Steep Takeoff,” *Washington Post*, January 2, 2003, p. A1; Morrison, Blake, “Air Marshals’ Resignations Flood TSA, Managers Say,” *USA Today*, August 29, 2002, p. 1A; Morrison, Blake, “Air Marshal Program in Disarray, Insiders Say,” *USA Today*, August 15, 2002, p. A1.

⁴⁴ Goo, Sara Kehaulani, “Customs Agents to Be Marshals,” *Washington Post*, September 3, 2003, p. A6.

has made some progress in this area; airports have decreased the number of perimeter access points, individuals and vehicles are randomly stopped and searched at entry points, and criminal history checks have been completed for most airport workers. In October 2003, the agency awarded a contract to Unisys to test and evaluate multiple technologies TSA is considering for a Transportation Workers Identification Card. The card will use biometric (biologic) technologies, possibly fingerprints and retinal (iris) scans, to identify airport employees and keep unauthorized people out of airports' secure areas. The card will serve as a common credential for the 12 million workers in the nation's transportation systems.

Yet, as airports continue to improve the security of their "sterile" areas, new security vulnerabilities continue to surface. In November 2002, terrorists believed to be associated with al-Qaeda shot two SA-7 shoulder-fired missiles at an Israeli passenger jet shortly after it took off from Mombasa, Kenya. The missiles narrowly missed hitting the plane but raised concerns within the U.S. that the weapons would someday be used against an American target. Airport officials have become increasingly worried about the highly portable missiles being launched from locations near or in airports. Airport directors report that they have increased their surveillance of perimeters but continue to voice concerns to TSA about their inability to completely guard against this threat. Motion detectors, closed-circuit televisions, and barriers are among the measures that are available but have not yet been used to better secure and monitor airport perimeters. The problem is money: Congress has failed to adequately fund programs that would improve airport perimeter security. While TSA continues to study alternative solutions, the question, "Who will pay?" remains unanswered.

GAPING HOLES THAT REMAIN IN THE NATION'S AVIATION SECURITY NET: GENERAL AVIATION AND AIR CARGO

General Aviation: Private Planes

There are about 219,000 privately owned planes in the U.S. general aviation fleet, ranging from two-seaters to 737 jets.⁴⁵ Recreational flyers, sports teams, crop dusters, banner advertisers, aerial sightseeing companies, and corporate executives are among the diverse users of general aviation planes. Single-engine propeller planes account for about 70 percent of the fleet. These small planes can take off and land anywhere, including the nation's commercial airports and an additional 2,500 public-use airports designated specifically for general aviation. Private plane pilots can also fly from their own private airstrips, built on farms and even in backyards. On any given day in the U.S., there are about 132,000 general aviation flights in the sky.

Private pilot and security consultant Joseph A. Kinney wrote in a *Washington Post* editorial⁴⁶ shortly after the 9/11 attacks that anyone who has visited a general aviation facility knows that security ranges between poor and non-existent. It took a suicidal teenager, 14-year-old Charles J. Bishop, to point up just how easy it is, even in post-9/11 America, to steal a small plane. On January 5, 2002, Bishop flew a 4-seat Cessna into the 28th floor of the 42-story Bank of America building in Tampa, Florida, killing himself but injuring no one else.⁴⁷

Two years after Bishop's crash, TSA has taken little action to improve general aviation security. General aviation pilots are still not required to pass through airport security screening, nor are their passengers, suitcases, or cargo.

⁴⁵ *GAO Report 01-916*, "General Aviation: Status of Industry, Related Infrastructure, and Safety Issues," August, 2001.

⁴⁶ Kinney, Joseph A., "Clamp Down on General Aviation," *Washington Post*, September 25, 2001, p. A23

⁴⁷ Koch, Kathleen, "Police: Tampa Pilot Voiced Support for bin Laden," www.cnn.com/U.S., January 7, 2002.

That is why the General Accounting Office concluded in April 2003, and again the following November, that general aviation is far more vulnerable than commercial aviation to terrorist attack.⁴⁸ Yet, neither Congress nor TSA has imposed any regulations on private planes that would prevent a terrorist from replicating Bishop's flight, this time with a plane loaded with explosives. TSA officials, who have referred to the general aviation industry as "unregulated," report that the agency does not plan to impose any mandatory rules on private planes in the foreseeable future.⁴⁹

The Aircraft Operators and Pilots Association, a lobbying group representing about 398,000 private plane owners and pilots, applauds Congress's and TSA's hands-off stance.⁵⁰ The organization has many Congressional allies and benefactors, chief among them, Representative James L. Oberstar (D-MN), who counts the lobbying group among his top campaign contributors.⁵¹ In March 2003, Representative Oberstar introduced a House proposal to commend the organization on its "proactive commitment to the security of general aviation."⁵² In fact, the association has battled regulators on most general aviation security measures considered after 9/11, including airspace restrictions over major cities during heightened terrorist alerts, the ban of small planes at Washington, D.C.'s National airport, restrictions on banner-towing advertising over stadiums, a law requiring general aviation pilots to pass criminal background checks, and another requiring FBI checks for flight school operators.⁵³

General aviation industry officials maintain that there has never been a terrorist attack involving a private plane, therefore it is unnecessary for the

⁴⁸ Griffin, Greg, "Flight Risks? Little Has Been Done to Boost Security at the Nation's General Aviation Airports," *The Denver Post*, August 17, 2003, p. K1.

⁴⁹ Ibid.

⁵⁰ www.aopa.org.

⁵¹ www.opensecrets.org; Thirteen organizations gave \$10,000 or more to Oberstar's 2002 campaign: National Air Traffic Controllers, Airline Pilots Association, Aircraft Owners and Pilots Association (AOPA), Amalgamated Transit Union, FedEx, Machinist/Aerospace Workers Union, Professional Airways Systems Specialists, Teamsters, Transportation Communication Union, UPS, United Transportation Union, Laborers Union and AFSCME.

⁵² Oberstar, Jim, House Resolution 120, 108th Congress, 1st Session, March 4, 2003.

⁵³ www.aopa.org.

government to impose new security regulations on the general aviation industry. For now, Congress and TSA agree.

Air Cargo

Last year, more than 12 million tons of cargo and mail were transported by air in the U.S. About 75 percent of air cargo is shipped on cargo-only planes. The rest, about 3 million tons annually, flies on commercial flights, in the holds of planes along with passengers' suitcases.⁵⁴ TSA estimates there is a 35 to 65 percent chance that terrorists are planning to place a bomb in the cargo of a U.S. passenger plane. Yet, only about 5 percent of air cargo is screened, even if it is transported on passenger planes.⁵⁵ Congress did not legislate new security initiatives for the air cargo industry in the Aviation and Transportation Security Act. Instead, they mandated TSA only to "ensure the adequacy of security measures for the transportation of cargo," stopping short of specifying how cargo should be inspected, and holding TSA to no firm deadline. The result: Cargo that is carried aboard cargo-only as well as on commercial passenger flights, reported the General Accounting Office in November 2003, continues to be highly vulnerable to terrorists' bombs.⁵⁶

Industry executives are pessimistic about the government's ability to come up with an effective air cargo security plan, largely because of the degree to which their business relies on speed. The success of air cargo companies is closely tied to their ability to move highly perishable and valuable goods across the world at a moment's notice. Enhanced security can only slow down companies' tightly scheduled operations.

Some members of Congress have attempted to fill in the air cargo security gap, while others are intent on making sure the industry is not saddled with any

⁵⁴ *GAO Report 03-344*, "Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System," December 2002.

⁵⁵ Morgan, Hudson, "Shipping News," *The New Republic*, July 7-14, 2003, p. 10.

⁵⁶ *GAO-04-285T*, November 20, 2003.

new regulations. Senators Kay Bailey Hutchison (R-TX) and Diane Feinstein (D-CA) introduced the Air Cargo Security bill in January 2003, which was passed by the Senate in May 2003.⁵⁷ The bill calls for the TSA to create a system for the regular inspection of air cargo facilities, and for every cargo shipper to develop a security plan, subject to TSA approval. The Hutchison-Feinstein bill has moved to the House, but Representative Don Young (R-AK), chairman of the Transportation and Infrastructure committee, has refused to mark it up. Young has come up with a competing bill that calls only for TSA to create a cargo screening pilot program that assesses “the capabilities of the private sector.”⁵⁸

In September 2003, House and Senate negotiators rejected a spending bill provision that would have required TSA to develop a plan for screening air cargo carried aboard passenger planes. The reason, said an Appropriations Committee spokesman, was that screening technology does not yet exist. Representative Edward J. Markey (D-MA) disagreed, and blamed Congressional Republicans for eliminating the provision because the air cargo industry opposed it.⁵⁹

TSA chief James Loy had the authority to mandate airlines and air cargo companies to institute specific security measures, just as he had the authority to force the airlines to hand over their passengers’ personal data for CAPPS II. But he refused to do so. Instead, Loy passed the issue to the Aviation Security Advisory Committee, a group of government and industry representatives pulled together by the FAA in 1989 (in the wake of the Pan Am 103 bombing) to advise regulators on security-related issues. While under the jurisdiction of the FAA, the Advisory Security Committee, dominated by the aviation industry, had a 13-year history of stalling or thwarting every security-related regulation the airlines opposed.⁶⁰

⁵⁷ Hutchison, Kay Bailey, “Air Cargo Security Improvement Act,” *Congressional Record*, Proceedings and Debates of the 108th Congress, First Session, May 8, 2003, p. S5932.

⁵⁸ Morgan, Hudson, *The New Republic*, July 7, 2003.

⁵⁹ No Byline, “Security Risks in the Air,” *Columbus Dispatch*, September 19, 2003, p. 14A.

⁶⁰ For detailed history of the Aviation Security Advisory Committee see: Felcher, E. Marla, *U.S. Domestic Aviation Security Before and After the 9/11/2001 Terrorist Attacks*, The Century Foundation, in press.

TSA's Aviation Security Advisory Committee met in October 2003 to make their cargo security recommendations.⁶¹ The next step is for TSA to turn these suggestions into a proposed regulation. Industry then will have an opportunity to comment on TSA's proposal, a process that can take months. It will be up to TSA staff to decide how to integrate industry's ideas and concerns into the final cargo security regulation—a process that often took *years* at the FAA. TSA has set no firm deadline for when a new regulation is likely to go into effect. This is the same course followed by most security regulations FAA considered pre-2001, a script that ultimately resulted in the promulgation of few security regulations and an aviation system highly vulnerable to terrorist attack.

THE FUTURE OF U.S. DOMESTIC AVIATION SECURITY

On September 11, 1989, security expert Robert Kupperman of the Center for Strategic International Studies addressed the Senate Governmental Affairs committee.

“The problem with terrorism is its episodic nature,” Kupperman said. “During the periods of relative calm, terrorism is viewed by large governments, including our own, as a minor annoyance...and it is difficult to get the policy levels of government focused on the problem at all. But when an incident occurs, particularly one dominated by media coverage, terrorism takes on a virtual strategic significance. When terrorists strike, governments go on hold, paralyzed by an unfolding human drama, which is televised for all to see.”⁶² After an attack, Kupperman told the group of senators, there is a groundswell of support for measures that would prevent it from occurring again but ultimately this enthusiasm dissipates and little changes.

⁶¹ www.tsa.gov, “New Regulations to Contribute to Improved Security in Air Cargo,” October 1, 2003.

⁶² Kupperman, Robert, “Responses to Terrorism,” Hearing of the Senate Governmental Affairs Committee, *Federal News Service*, September 11, 1989.

Kupperman's observations were a prescient description of the "aviation disaster script" that played out in the wake of pre-2001 airline disasters, specifically, the 1988 bombing of a Pan Am 747 and the 1996 explosion of a TWA 747 off the coast of New York.⁶³ The script's actors—FAA staff and officials, the Department of Transportation inspector general, government task forces, Congressional oversight committees, White House commissions, and the General Accounting Office—identified, investigated, documented, and offered solutions intended to prevent the disaster from occurring again. Between 1988 and 2001, the GAO issued more than forty reports warning that lax security in the nation's airports left our airports and planes highly vulnerable to terrorist attack. The Department of Transportation inspector general's office issued dozens more reports, all saying essentially the same thing. Two presidents, the first Bush and Clinton, convened blue-ribbon commissions to study the problem. Both groups seconded the opinions of the General Accounting Office and Department of Transportation inspector general that security was abysmal. These investigations and reports culminated with interminable Congressional hearings, much passing of the buck, and few security enhancements.

That Congress refused to take any action to improve aviation security, in light of indisputable evidence that U.S. aircraft were an easy target for terrorists, was due primarily to the airlines' tenacious efforts to delay, dilute, or defeat every measure that threatened their short-term pecuniary interests. Security was viewed as an expense, not a revenue-generating line item, and they didn't want to spend the money. Therefore, each time Congress even considered security-related legislation, the aviation industry would respond by dispatching its representatives to Capitol Hill. Reinforcing the lobbyists' efforts were the airlines' open checkbooks; between 1990 and 2000 the air transport industry donated over \$67 million to politicians' campaigns.⁶⁴

⁶³ The cause of the TWA explosion, while initially considered to be the work of terrorists, was ultimately ruled, five year after the crash, to be mechanical.

⁶⁴ Center for Responsive Politics, www.opensecrets.org.

WHY SECURITY IS BETTER TODAY THAN IT WAS ON SEPTEMBER 11, 2001

The September 11 terrorists finally motivated Congress to do what no previous terrorists or government reports had prompted them to do in the past: enact legislation that improved the nation's aviation security. That the government would be picking up the tab for aviation security quelled the airlines' objections, at least temporarily. The result: aviation security is stronger now than it has ever been in the nation's history. There are more screeners stationed at airport checkpoints than ever before, and they are better paid and more experienced than their private sector predecessors; screeners' annual attrition rate has dropped to about 14 percent, from between 100 and 400 percent when they were considered by the airlines to be little more than a line-item expense. While the adequacy of the screeners' training and testing has been rightly questioned, the overall caliber of the workforce certainly has been raised. All of the incomplete screener background checks pending as of the summer of 2003 have been completed, and screeners with questionable backgrounds have been fired.⁶⁵ Backing up the screeners' efforts are the 1,060 explosives-detection systems and 5,300 electronic trace-detectors that scan 100 percent of passengers' luggage for explosives.

Two innermost layers of the "system of systems" now decrease the probability of a terrorist gaining control of a plane in mid-air: airport cockpit doors have been reinforced to prevent intruders from gaining access to the flight deck, and thousands of undercover air marshals fly on tens of thousands of domestic and international flights each month to protect the planes' passengers and crew.

Although a final version of CAPPs II has not been implemented, TSA has joined efforts with U.S. and international intelligence agencies to do a better job of flagging suspected terrorists at airports. In August 2003, airline ticket agents at

⁶⁵ www.tsa.gov, "TSA Screener Background Checks Fact Sheet," September 29, 2003.

the Seattle-Tacoma airport alerted police after the names of two passengers appeared on a “no-fly” list TSA had circulated to the airlines. This would not have occurred pre-TSA. In fact, on September 11, 2001, the FAA’s “no-fly” list was 300 names long and contained the names of two of the hijackers. But the FAA had not circulated the list to the airlines, because, according to one FAA official, “We just never got around to setting up a protocol for who would control the list and how we would get the airlines to implement it.”⁶⁶

In FY 2001, the FAA spent \$160.4 million on aviation security; the TSA spent \$4.5 billion on aviation security in FY 2002 and will spend at least \$6.1 billion more in FY 2003. While Congress and TSA have allowed two enormous security holes to remain, air cargo and general aviation, most of the holes that existed in the system two years ago have been made significantly smaller.

THE TRADE-OFFS CONNECTED TO SECURITY

Despite these improvements, there is a limit to how far TSA can be expected to raise the bar, given that the Aviation and Transportation Security Act did not get at the root of the aviation security problem—our government’s reluctance to view security along a continuum, rather than as an absolute. Each point along the continuum represents a series of tradeoffs, factors affected by the level of security our leaders choose for the country, including aviation industry profitability, costs to the government, passenger convenience, and passenger privacy. Pre-TSA, the aviation system operated on the far left side of this continuum, “low security,” as Congress hesitated to mandate any security enhancement that would saddle either the U.S. government or the airlines with millions of dollars of new expenses. Refusing to act, Congress tried to wish away the risk of a terrorist attack on America’s aviation system.

⁶⁶ Brill, Steven, *After: How America Confronted the September 12 Era*, Simon & Schuster, New York, New York, 2003.

This trade had advantages for passengers as well as the government and the airlines. Travelers moved freely throughout airports, checkpoint lines remained short, invasive searches of our bodies and luggage were rare, airline tickets remained free of security taxes, and, in the absence of a profiling system like CAPPS II, privacy remained intact. For many years, the interests of airline passengers, Congress, and the airline industry appeared to be aligned under this “no-security” policy.

Then, in a flash, the 2001 attacks jolted us to the opposite end of the security continuum, far to the right. Suddenly, we demanded high levels of security, at the expense of everything else. In response, Congress enacted sweeping legislation in record time, allocating an unprecedented amount of money for TSA to fix what was now an obviously broken system. In an abrupt about-face, our leaders adopted a “zero-risk” mentality, promising to spare no expense to do all that was necessary to secure our planes. No public official would have dared to explain that, while the nation’s new security regimen was capable of decreasing the probability of another attack, it would certainly not decrease the risk to zero. The public needed to be assured that it was safe to fly, and promises of zero-risk policies were what they needed to get back in the air. “Public support is much greater, no matter how unrealistic, when there are promises that the risk will be completely eliminated,” wrote Harvard University economists Kip Viscusi and Richard Zeckhauser.⁶⁷ Cadres of professionally uniformed TSA screeners who combed through our carry-on bags with a level of vigor we had never before witnessed went far to reinforce the position that it was once again safe to fly.

This zero-risk mentality is as unsustainable as our pre-September 11 no-security policy. Eventually, Congress and the American public will be forced to confront the fact that there simply isn’t enough money to fund every security program, nor is it possible to completely eliminate the risk of another terrorist

⁶⁷ Zeckhauser, Richard and Kip Viscusi, “Sacrificing Civil Liberties,” *Journal of Risk and Uncertainty*, in press.

attack. This is the point at which TSA finds itself today. Until now, the agency has directed most of its energy toward tactical issues. The first year was devoted to creating itself, hiring, training and deploying tens of thousands of new employees to airports, and purchasing and installing explosives-detection systems. The second year was spent largely on refining what was already in motion (e.g., the air marshal program), cleaning up what had gone wrong (e.g., airport screener background checks and contractor oversight), and making headway on non-deadline programs (e.g., CAPPs II and airport perimeter controls). Now that TSA is in its third year, TSA, Congress, and the American people must wrestle with a question of longer-term, strategic importance, namely, *how much security do we need, and what are we willing to give up to have it?*

Before our abrupt quest for tight security, many Americans were not even aware of what they “getting” in return for lax security. It was not until airport checkpoint lines curled around corners and extended out airport doors, guards with machine guns patrolled airport lounges, a security tax appeared on airline tickets, and our privacy was threatened that we even considered the costs associated with heightened security. Legislators’ enthusiasm for aviation security had always fizzled long before such changes occurred. The Aviation and Transportation Security Act ensured that these changes would occur. Now, for the first time in history, Americans are aware of what we must give up to have an aviation system terrorists cannot easily penetrate.

In May 2003, Department of Transportation inspector general Ken Mead testified before the National Commission on Terrorist Attacks Upon the U.S. “The new security model is much more likely to ensure strong aviation security than its predecessor,” Mead concluded after detailing the progress TSA had made over the past eighteen months. “However, a cautionary note is in order. The sense of vigilance for a priority attached to tight security can dissipate with the passage of time,” the inspector general warned, just as security expert Robert Kupperman had warned in 1989, “which in turn may lead to a sense of complacency as well as

pressures to relax security.”⁶⁸ The Aviation and Transportation Security Act ensured that security would improve in the U.S., but as Ken Mead pointed out, it did not ensure that the momentum initiated by the legislation will continue in the absence of another terrorist attack. And it certainly did not eliminate the source that is mostly likely to apply intense “pressures to relax security”—the airline industry. Aviation security is still very much a work-in-progress, TSA’s to-do list an open invitation for the agency’s most powerful stakeholder, the airlines, to have a say in the agency’s policies.

When President Eisenhower signed the Federal Aviation Act in 1958, creating the FAA, the agency’s dual mission was explicit: *ensure aviation safety and promote the aviation industry*. At the time, few questions were asked about the ability of a single agency to carry out two missions that could easily collide. Over the next four decades plenty of questions were asked, particularly in the wake of high-profile plane crashes that killed many people. The FAA was stripped of its explicit mandate to promote the aviation industry in 1996, under the Clinton administration. But as long as commercial aviation occupies a central role in the U.S. economy, generating hundreds of billions of dollars annually and accounting for hundreds of thousands of jobs, the issue will not disappear.

Congress’s obstinate ambivalence on the security-commerce issue is apparent in TSA’s mission statement today:

The Transportation Security Administration protects the Nation’s transportation systems to ensure freedom of movement for people and commerce.⁶⁹

⁶⁸ Mead, The Honorable Kenneth M., Statement Before the National Commission on Terrorist Attacks Upon the United States on Aviation Security,” May 22, 2003, www.ignnet.gov.

⁶⁹ www.tsa.gov.

Going forward, it will be up to TSA's leaders, Congress, and the American people to calibrate just how freely people and commerce should move and the costs they are willing to incur for this freedom.

APPENDIX

TIMELINE OF SIGNIFICANT EVENTS IN TSA'S HISTORY

November 19, 2001	President Bush signs Aviation and Transportation Security Act into law
December 10, 2001	President Bush nominates John M. Magaw as Undersecretary of Transportation Security
April 30, 2002	Transportation Security Administration deploys first 200 checkpoint screeners to Baltimore-Washington International Airport
July 1, 2002	TSA deploys thousands of new federal air marshals to fly on U.S. planes
July 18, 2002	John M. Magaw resigns, replaced by James M. Loy
August 7, 2002	DOT inspector general testifies to House that TSA is having difficulty hiring enough checkpoint screeners
November 18, 2002	TSA meets Congress's screener deployment deadline
December 20, 2002	GAO issues report describing air cargo as vulnerable to terrorist attack

December 31, 2002	TSA meets deadline to screen all checked luggage for explosives*
February 28, 2003	DOT inspector general audit finds that TSA contractors overcharged agency by millions of dollars
March 1, 2003	TSA moved to Department of Homeland Security
April 9, 2003	Airlines complete reinforcement of all aircraft cockpit doors
May 22, 2003	DOT inspector general urges TSA to improve air cargo security and to measure screener performance
July 7, 2003	DHS allocates total of \$350 million to 3 airports for integration of EDS into baggage-handling systems
September 2, 2003	Federal air marshal program moved to Bureau of Customs and Immigration Enforcement
September 2, 2003	DHS allocates total of \$425 million to 3 more airports for integration of explosives-detection machines into baggage-handling systems

* While Admiral James Loy announced that TSA had met its Congressional deadline to screen all checked baggage for explosives, this was technically not true. The Aviation and Transportation Security Act mandated TSA to screen suitcases with electronic explosives-detection systems, yet TSA was not able to buy and install all of the equipment by December 31, 2002. A few months earlier, when it had become clear that TSA would not be able to meet this deadline, Congress had extended it and approved other screening technologies to be used in the interim, including trace-detection machines and bomb-sniffing dogs.

September 24, 2003	TSA approves total of \$100 million to reimburse 58 carriers for reinforcing cockpit doors
October 1, 2003	TSA completes all outstanding background checks on airport checkpoint screeners
October 1, 2003	TSA's Aviation Security Advisory Committee offers 40 recommendations on how to improve air cargo security
October 16, 2003	TSA awards contract for pilot project to strengthen secure-area access controls at 20 airports
October 23, 2003	TSA Administrator James Loy nominated as Deputy Secretary at Department of Homeland Security
November 17, 2003	TSA releases Air Cargo Strategic Plan
December 4, 2004	Rear Admiral David M. Stone appointed Acting Administrator of TSA