United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Aviation, Committee on Commerce, Science, and Transportation, U.S. Senate

For Release on Delivery
Expected at
10:00 a.m. EDT
Thursday,
April 6, 2000

AVIATION SECURITY

Vulnerabilities Still Exist in the Aviation Security System

Statement of Gerald L. Dillingham,
Associate Director, Transportation Issues,
Resources, Community, and Economic
Development Division

GAO/T-RCED/AIMD-00-142

Mr. Chairman and Members of the Subcommittee:

We appreciate the opportunity to be here today to discuss the security of the nation's air transport system. The air transport system is vital to our nation's prosperity, and protecting this system from terrorist attacks or other dangerous acts remains an important national issue. Events over the past decade have shown that the threat of terrorism against the United States is an ever-present danger and, coupled with the fact that aviation is an attractive target for terrorists, indicate that the security of the air transport system remains at risk. Protecting this system demands a high level of vigilance because a single lapse in aviation security can result in hundreds of deaths, destroy equipment worth hundreds of millions of dollars, and have immeasurable negative impacts on the economy and the public's confidence in air travel.

Our testimony today discusses the Federal Aviation Administration's (FAA) efforts to implement and improve security in two key areas: air traffic control computer systems and airport passenger screening checkpoints. Computer systems—and the information within—are the crucial link for providing information to air traffic controllers and aircraft flight crews to ensure the safe and expeditious movement of aircraft. Screening checkpoints and the screeners who operate them provide the means to ensure that passengers and others do not bring dangerous items aboard aircraft. Our testimony is based on issued reports on computer security and on work that we have under way on checkpoint screeners that we are conducting at this Subcommittee's request. Our report on checkpoint screeners will be issued shortly.

In summary, Mr. Chairman, our work has identified security problems in both the air traffic control computer systems and in the performance of checkpoint screeners:

- A report we issued in 1998 detailed weaknesses in critical computer security areas, including the physical security at facilities that house air traffic control systems and the management of security for operational computer systems. For example, FAA had not assessed the physical security at a large portion of its air traffic control

facilities and had not performed the necessary threat analyses for 87 of its 90 operational air traffic control computer systems in the 5 years prior to our review. FAA has since initiated actions to resolve the problems we identified in these instances; however, in December 1999, we reported that FAA was still not following its own security requirements as it failed to conduct the required background searches on contractor employees reviewing and repairing critical computer system software.

- FAA and the airline industry have made little progress in improving the effectiveness of airport checkpoint screeners. Screeners are not adequately detecting dangerous objects, and long-standing problems affecting screeners' performance remain, such as the rapid screener turnover and the inattention to screener training. FAA's efforts to address these problems are behind schedule. For example, FAA is 2 years behind schedule in issuing a regulation that would implement a congressionally mandated requirement to certify screening companies and improve the training and testing of screeners. Partially as a consequence of its delays, FAA has not attained its fiscal year 1999 Government Performance and Results Act goals for improving screener performance. Five countries we visited had different screening practices and significantly lower screener turnover and may have better screener performance. One country's screeners detected over twice as many test objects in a joint testing program that it conducted with FAA.

The security problems we have found would by themselves be cause for concern. Unfortunately, Mr. Chairman, the problems we have identified are not unique. Problems identified by others, such as the Department of Transportation's Inspector General, point out weaknesses in a number of other key aviation protection measures. Taken together, these problems show the chain of security protecting our aviation system has not one but several weak links. It must be recognized that the responsibility for these problems does not fall on the shoulders of FAA alone. The aviation industry is responsible for undertaking the security measures at airports and many of the problems identified—such as rapid screener turnover—more appropriately rest with it.

The fact that there have been no major security incidents in recent years—such as the 1988 bombing of Pan Am Flight 103—could breed an attitude of complacency. Maintaining or improving aviation security in such an environment is more challenging. However, serious vulnerabilities in our aviation security system exist and must be adequately addressed. We expressed concern 2 years ago that the momentum of aviation security improvements must not be lost, and we express that concern again today. Continual congressional oversight will be needed to hold the aviation community accountable for establishing and achieving specific improvement goals and changes.

Background

Before I discuss these issues in greater detail, it is important to place some perspective on the nation's aviation security system. Providing security to the nation's aviation system is a complex and difficult task because of the size of the U.S. system, the differences among airlines and airports, and the unpredictable nature of terrorism or criminal acts. The U.S. civil aviation system comprises hundreds of commercial airports, thousands of aircraft, and tens of thousands of flights each day that transport over 2 million passengers. FAA has hundreds of facilities throughout the country that monitor and direct the flow of aircraft to ensure they arrive safely at their intended destination. Providing security to such a vast and diverse system can be a daunting challenge.

Yet the need for strong aviation security grows every day. The threat of terrorism against the United States remains high and, as evidenced by the 1995 discovery of a plot to bomb as many as 11 U.S. airliners, civil aviation is an attractive target. More recent events such as the December 1999 apprehension at the Canadian border of a suspected terrorist with bomb components, including some small enough to be brought onto an aircraft, reaffirm the need for concern. Other threats such as "air rage"—those hostile or possibly criminal acts that occur onboard aircraft—are on the increase and could be potentially catastrophic if dangerous objects, such as weapons, were to be involved. In

the past month alone, there have been two such incidents in which passengers attacked pilots in the cabins of airborne flights. Finally, a growing threat—computer hackers—has evolved that could threaten the security of aircraft or the entire national airspace system. If hackers are able to penetrate the air traffic control system, they could attack the computer systems used to communicate with and control aircraft, potentially causing significant economic problems and placing aircraft at risk.

The threat of terrorist or other acts against aircraft have led to numerous calls for improvements that address the vulnerabilities in the aviation system. During the last decade, two presidential commissions have reviewed and reported on problems with various aspects of aviation security, and two major laws have been enacted that required actions to improve security measures. Additionally, the Congress provided about $1 billion to FAA over the last 4 fiscal years to carry out its civil aviation security program, including over $340 million for the purchase and deployment of security equipment at U.S. airports.

ATC Computer Security

Securing the air traffic control (ATC) computer systems that provide information to controllers and flight crews is critical to the safe and expeditious movement of aircraft. Failure to adequately protect these systems, as well as the facilities that house them, could cause nationwide disruption of air traffic or even loss of life. Moreover, malicious attacks on computer systems are becoming an increasing threat, and it is essential that FAA ensure the integrity and availability of the ATC computer systems and protect them from unauthorized access. Numerous laws as well as FAA's policy require that these systems be adequately protected.

However, as we reported in May 1998, FAA had been ineffective in four critical computer security areas we reviewed.[1] The first of these areas was physical security at

[1] *Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety* (GAO/AIMD-98-155, May 18, 1998).

key ATC facilities, such as towers and en route centers, where known weaknesses existed. For example, contractor employees were given unrestricted access to sensitive areas without required background investigations. In addition, at many facilities, the extent of weaknesses was unknown because FAA did not follow its own security policy and did not conduct the required physical security assessments from 1993 to 1998 at a large portion of its ATC facilities.

Second, FAA had not ensured the security of operational ATC systems. FAA's policy requires that all ATC systems be assessed for risk, certified that they comply with FAA's requirements, and accredited by FAA management once the appropriate security safeguards have been implemented. However, of 90 operational ATC systems, only 3—less than 4 percent—were certified and none was accredited. Additionally, security assessments for ATC telecommunications systems were similarly lacking. Eight of nine telecommunications systems were not assessed despite the fact that FAA's 1994 Telecommunications Strategic Plan stated that "vulnerabilities that can be exploited in aeronautical telecommunications potentially threaten property and public safety."

Third, FAA was not adequately managing security for new ATC systems. Because FAA had no security architecture, security concept of operations, or security standards, the implementation of security requirements for ATC development efforts were ad hoc and sporadic. Of the six system development efforts we reviewed, only four had security requirements, and of these, only two were based on risk assessments. Without security requirements based on sound risk assessments, FAA lacks assurance that future ATC systems will be protected from attack.

Fourth, FAA's management structure was not effectively implementing and enforcing computer security policy. Responsible offices did not adequately implement and enforce security policy, and FAA lacked a central point for enforcing security. In particular, FAA did not have a Chief Information Officer (CIO) reporting directly to the FAA Administrator, a management structure consistent with Clinger-Cohen Act requirements.

As a result of our work, FAA has initiated efforts to address all four computer security problem areas. For example, it has inspected the facilities it had not assessed since 1993, and it has established a CIO position with responsibility for developing, implementing, and enforcing the agency's security policy. Nevertheless, weaknesses continue in FAA's efforts to maintain effective computer security. In December 1999, we reported that FAA was still not following its own security requirements.[2] We found FAA used contractor employees to make Year 2000 repairs to mission-critical ATC systems and to review these systems' software without the required background searches being performed. In one case, we found that no background searches were performed on 36 foreign nationals who had access to copies of critical ATC systems' source code. As a result of not following its own security requirements, FAA increased the risk of inappropriate individuals gaining access to, and knowledge of, its facilities, information, and resources. Consequently, the ATC system may now be more susceptible to intrusion and malicious attacks. We are currently following up on the status of FAA's efforts to resolve the computer security problems we identified as part of an ongoing computer security review.

Checkpoint Screeners

Not only have we found security problems at air traffic control facilities, but more significantly, we have found problems at the screening checkpoints at airports. The screening checkpoints and the screeners who operate them are a key line of defense against the introduction of dangerous objects into the aviation system. All passengers and their baggage must be checked for weapons, explosives, or other dangerous articles that could pose a threat to the safety of an aircraft and those aboard it. FAA and the air carriers share this responsibility. FAA prescribes the screening regulations and establishes the basic standards for the screeners, the equipment, and the procedures to be used, and the air carriers are responsible for screening passengers and their baggage

[2] *Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software* (GAO/AIMD-00-55, Dec. 23, 1999).

before they are permitted into the secure areas of an airport or onto an aircraft. Air carriers can use their own employees to conduct screening activities, but for the most part, air carriers hire security companies to do the screening.

The screeners detect thousands of dangerous objects each year. Over the past 5 years, they detected nearly 10,000 firearms being carried through checkpoints, according to FAA. Nevertheless, the screeners do not identify all threats, and instances occur each year in which weapons are discovered to have passed through a checkpoint. We found a number of cases in which passengers passed through checkpoints on the first flight of their trips and were subsequently found to have loaded guns at screening checkpoints prior to boarding connecting flights. Similarly, we are aware of two instances in which simulated explosive devices used for testing screeners passed through screening checkpoints and were placed aboard aircraft.

Concerns have been raised for many years by us and by others about the effectiveness of the screeners and the need to improve their performance. In 1978, the screeners were not detecting 13 percent of the potentially dangerous objects FAA agents carried through checkpoints during tests—a level that was considered "significant and alarming." In 1987, we found that screeners were not detecting 20 percent of the objects during FAA's tests.[3] Two presidential commissions—established after the bombing of Pan Am Flight 103 in 1988 and the then-unexplained crash of TWA Flight 800 in 1996—as well as numerous reports by GAO and the Department of Transportation's Inspector General have highlighted problems with screening and the need for improvements. To rectify some of these problems, the Federal Aviation Reauthorization Act of 1996 mandated that FAA certify screening companies, improve the training and testing of the screeners, and develop performance standards. However, Mr. Chairman, problems with the screeners' performance remain a serious concern. Data on FAA's test results can

[3]*Aviation Security: FAA Needs Preboard Passenger Screening Performance Standards* (GAO/RCED-87-182, July 24, 1987).

not be released publicly, but our research shows that the screeners' ability to detect objects during the agency's tests is not improving, and in some cases is worsening.

Screeners' Performance Problems Are Attributed to Rapid Turnover and Inattention to Human Factors

There is no single reason why screeners fail to identify dangerous objects. Two conditions—rapid screener turnover and inadequate attention to human factors—are believed to be important causes. The rapid turnover among screeners has been a long-standing problem, having been singled out as a concern in FAA and GAO reports dating back to at least 1979. We reported in 1987 that turnover among screeners was about 100 percent a year at some airports, and today, the turnover is considerably higher.[4] From May 1998 through April 1999, turnover averaged 126 percent among screeners at 19 large airports, with 5 airports reporting turnover of 200 percent or more and 1 reporting turnover of 416 percent. At one airport we visited, of the 993 screeners trained there over about a 1-year period, only 142, or 14 percent, were still employed at the end of that year. Such rapid turnover can seriously affect the level of experience among the screeners operating a checkpoint. Appendix I lists the turnover rates for screeners at 19 large airports.

Both FAA and the aviation industry attribute the rapid turnover to the low wages the screeners receive, the minimal benefits, and the daily stress of the job. Generally, screeners get paid at or near the minimum wage. We found that some of the screening companies at many of the nation's largest airports paid screeners a starting salary of $6 an hour or less, and at some airports the starting salary was the minimum wage—$5.15 an hour. It is common for the starting wages at airport fast-food restaurants to be higher than the wages the screeners receive. For instance, at one airport we visited, the screeners' wages started as low as $6.25 an hour, whereas the starting wage at one of the airport's fast-food restaurants was $7 an hour.

[4]GAO/RCED-87-182, July 24, 1987.

The human factors associated with screening—those work-related issues that are influenced by human capabilities and constraints—have also been noted by FAA as problems affecting performance for over 20 years. Screening duties require repetitive tasks as well as intense monitoring for the very rare event when a dangerous object might be observed. Too little attention has been given to factors such as (1) individuals' aptitudes for effectively performing screening duties, (2) the sufficiency of the training provided to the screeners and how well they comprehend it, and (3) the monotony of the job and the distractions that reduce the screeners' vigilance. As a result, screeners are being placed on the job who do not have the necessary abilities or adequate knowledge to effectively perform the work and who then find the duties tedious and unstimulating.

FAA Is Making Efforts to Address Causes of Screeners' Performance Problems, but Progress Has Been Slow

FAA has demonstrated that it is aware of the need to improve the screeners' performance by conducting efforts intended to address the turnover and human factors problems and by establishing goals with which to measure the agency's success in improving performance. The efforts include establishing a threat image projection system to keep screeners alert and to monitor their performance; a screening company certification program; and screener selection tests, computer-based training, and readiness tests. FAA's implementation of these efforts, however, has encountered substantial delays and is behind schedule. I would like to focus on two key efforts, the threat image projection system and the screening company certification program, and then discuss FAA's progress in achieving its goals for improved screener performance.

The Threat Image Projection System

FAA is deploying an enhancement to the X-ray machines used at the checkpoints called the threat image projection (TIP) system. As screeners routinely scan passengers' carry-on bags, TIP occasionally projects images of dangerous objects like guns and

explosives on the X-ray machines' screens. The screeners are expected to spot the objects and signal for the bags to be manually searched. Once prompted, TIP indicates whether an image is of an actual object in a bag or was generated by the system and also records the screeners' responses, providing a measure of their performance while keeping them more alert. By frequently exposing screeners to what dangerous objects look like on screen, TIP will also provide continuous on-the-job training.

FAA is behind schedule in deploying this system. It had planned to begin deploying 284 units to 19 large airports in April 1998. But as a result of hardware and software problems, FAA dropped its plans to install the units on existing X-ray machines nationwide. Instead, in mid-2000, it will begin purchasing and deploying 1,380 new X-ray machines already equipped with the TIP system. FAA expects to have the system in place at the largest airports by the end of fiscal year 2001 and at all airports by the end of fiscal 2003.

Unfortunately, the delays in the TIP system's deployment have impeded another key initiative to improve the screeners' performance: the certification of screening companies.

The Certification of Screening Companies

In response to a mandate in the Federal Aviation Reauthorization Act of 1996 and a recommendation from the 1997 White House Commission on Aviation Safety and Security, FAA is creating a program to certify the security companies that staff the screening checkpoints. The agency plans to establish performance standards—an action we recommended in 1987[5]—that the screening companies will have to meet to earn and retain certification. It will also require that all screeners pass automated readiness tests after training and that all air carriers have TIP units on the X-ray machines at their checkpoints so that the screeners' performance can be measured to ensure FAA's standards are met. FAA believes that the need to meet certification

[5]GAO/RCED-87-182, July 24, 1987.

standards will give the security companies a greater incentive to retain their best screeners longer and so will indirectly reduce turnover by raising the screeners' wages and improving training. Most of the air carrier, screening company, and airport representatives we contacted said they believe certification has the potential to improve the screeners' performance.

FAA plans to use data from the TIP system to guide it in setting its performance standards, but because the system will not be at all airports before the end of fiscal year 2003, the agency is having to explore additional ways to set standards. FAA plans to issue the regulation establishing the certification program by May 2001, over 2 years later than its earlier estimated issue date of March 1999. According to FAA, it has needed more time to develop performance standards and to develop and process a very complex regulation. The first certification of screening companies is expected to take place in 2002.

FAA's Goals for Screeners' Performance

As required by the Government Performance and Results Act, FAA established goals in 1998 for improving screeners' detection of test objects carried through metal detectors and concealed in carry-on baggage. FAA views specific data relating to these goals, as well as other information relating to screeners' detection rates, to be too sensitive to release publicly. However, it can be said that, in part because of the delays in implementing its screener improvement efforts, the agency did not meet its first-year goals for improving screener performance. FAA acknowledged that it did not meet its fiscal year 1999 improvement goal for detecting dangerous objects carried through metal detectors, but it believed that it had nearly met its goal for improving their detection in carry-on baggage. However, we found flaws in FAA's methodology for computing detection rates, and that, in fact, the goal was not met. We have discussed our findings with FAA, and as result of our findings and the delays in its initiatives, the agency is revising its goals.

We are encouraged that FAA is currently developing an integrated checkpoint screening management plan to better focus its efforts and meet its goals for improving the screeners' performance. According to FAA officials, the plan, which is still in draft form, will (1) incorporate FAA's goals for improving the screeners' performance and detail how its efforts relate to the achievement of the goals; (2) identify and prioritize checkpoint and human factors problems that need to be resolved; and (3) provide measures for addressing the performance problems, including related milestone and budget information. Moreover, the draft plan will consolidate the responsibility for screening checkpoint improvements under a single program manager, who will oversee and coordinate efforts at FAA headquarters, field locations, and the agency's Technical Center in Atlantic City, New Jersey. FAA expects the plan to be completed in April 2000 and to be continuously updated based on its progress.

Screening Practices in Five Other Countries Differ From U.S. Practices

To identify screening practices that differ from those in the United States, we visited five countries—Belgium, Canada, France, the Netherlands, and the United Kingdom—viewed by FAA and the aviation industry as having effective screening operations. These countries also have significantly lower screener turnover than the United States—about 50 percent or lower. We found some significant differences in four areas: screening operations, screeners' qualifications, screeners' pay and benefits, and institutional responsibility for screening.

First, screening operations in some countries are more stringent. For example, Belgium, the Netherlands, and the United Kingdom routinely touch or "pat down" passengers in response to metal detector alarms. Additionally, all five countries allow only ticketed passengers through the screening checkpoints, thereby allowing the screeners to more thoroughly check fewer people. Some countries also have a greater police or military presence near checkpoints. In the United Kingdom, for example, security forces—often armed with automatic weapons—patrol at or near checkpoints.

At Belgium's main airport, a constant police presence is maintained at one of two glass-enclosed rooms directly behind the checkpoints.

Second, the screeners' qualifications are usually more extensive. For example, in contrast to the United States, Belgium requires screeners to be citizens, while France requires screeners to be citizens of a European Union country. In the Netherlands, screeners do not have to be citizens, but they must have been residents of the country for 5 years. Moreover, while FAA requires that screeners in this country have 12 hours of classroom training, Belgium, Canada, France, and the Netherlands require more. France requires 60 hours of training, and Belgium requires at least 40 hours with an additional 16 to 24 hours for each activity, such as X-ray machine operations, the screener will conduct.

Third, the screeners receive relatively better pay and benefits in most of these countries. While in the United States screeners receive wages that are at or slightly above minimum wage, screeners in some countries receive wages that they view as being "middle income." In the Netherlands, for example, screeners receive at least the equivalent of about $7.50 per hour. This wage is about 30 percent higher than wages at fast-food restaurants. In Belgium, screeners receive about $14 per hour. Screeners in some countries also receive some benefits, such as health care or vacations, as required under the laws of these countries.

Finally, the responsibility for screening in most of these countries is placed with the airport or with the government, not with the air carriers as it is in the United States. In Belgium, France, and the United Kingdom, the responsibility for screening has been placed with the airports, which either hire screening companies to conduct the screening operations or, as at some airports in the United Kingdom, hire screeners or manage the checkpoints themselves. In the Netherlands, the government is responsible for passenger screening and hires a screening company to conduct checkpoint operations, which are overseen by a Dutch police force.

Because each country follows its own unique set of screening practices, and because data on screener performance in each country were not available to us, it is difficult to measure the impact of these different practices, either individually or jointly, on improving screeners' performance. Nevertheless, there are indications that in at least one country, the practices may help to improve the screeners' performance. This country conducted a testing program jointly with FAA that showed that the other country's screeners detected over twice as many test objects as did the screeners in the United States.

We note that practices similar to those in other countries have been proposed in the United States. The Chicago Department of Aviation, which operates Chicago-O'Hare International Airport, has advocated moving the responsibility for screening to airports, hiring screening companies under a model similar to that used by the General Services Administration to contract for security services, and having universities conduct more extensive and independent screener training programs. In response to a requirement of the Federal Aviation Reauthorization Act of 1996, FAA did evaluate options for moving screening responsibilities to airports or the federal government. The agency said that it found no consensus for moving these responsibilities to other parties, and consequently the responsibility for screening remains with the air carriers.

Summary

Many vulnerable areas in the aviation system need strong protection. Unfortunately, Mr. Chairman, the problems we have identified in two of these areas are not unique. Others such as the Department of Transportation's Inspector General and the National Research Council have identified other problems with the security controls in and around airports, the implementation of security procedures, and the use and effectiveness of new equipment intended to better assist in identifying threats. Taken together, these problems point out that effective security for our nation's aviation system has not yet been achieved. It is often said that a chain is only as strong as its weakest link; in the case of aviation security, there are still many weak links. It must be

recognized that these weak links are not the responsibility of FAA alone. The responsibility for certain conditions, such as the rapid screener turnover, more appropriately rests with the air carriers and screening companies. It will, therefore, take the cooperation of the aviation industry to put into place the actions needed to improve security.

In closing, Mr. Chairman, the fact that there has been no major security incident in the United States or involving a U.S. airliner in nearly a decade could breed an attitude of complacency in improving aviation security. Improving security in such an environment is more challenging and difficult. Two years ago, in another testimony before the Congress, we expressed a similar concern in stressing that the momentum of aviation security improvements must not be lost. Given the extent of the problems, we must reiterate this concern and believe that continuing congressional oversight in holding FAA and the aviation industry accountable for improving the aviation security will be critical to the full achievement of a safe and secure air transportation system.

- - - - -

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions that you or Members of the Subcommittee may have.

Contacts and Acknowledgments

For more information, please contact Gerald L. Dillingham at (202) 512-2834.
Individuals making key contributions to this testimony included Leslie D. Albin, J. Michael Bollinger, Barry R. Kime, John R. Schulze, and Daniel J. Semick.

Appendix I

SCREENER TURNOVER RATES AT 19 LARGE AIRPORTS, MAY 1998-APRIL 1999

City (airport)	Annual turnover rate (percentage)
Atlanta (Hartsfield Atlanta International)	375
Baltimore (Baltimore-Washington International)	155
Boston (Logan International)	207
Chicago (Chicago-O'Hare International)	200
Dallas-Ft. Worth (Dallas/Ft. Worth International)	156
Denver (Denver International)	193
Detroit (Detroit Metro Wayne County)	79
Honolulu (Honolulu International)	37
Houston (Houston Intercontinental)	237
Los Angeles (Los Angeles International)	88
Miami (Miami International)	64
New York (John F. Kennedy International)	53
Orlando (Orlando International)	100
San Francisco (San Francisco International)	110
San Juan (Luis Munoz Marin International)	70
Seattle (Seattle-Tacoma International)	140
St. Louis (Lambert St. Louis International)	416
Washington (Washington-Dulles International)	90
Washington (Ronald Reagan Washington National)	47
Average turnover	**126**

Source: FAA.

(348227)

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to

info@www.gao.gov

or visit GAO's World Wide Web home page at

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: 1-800-424-5454