United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
10:00 a.m. EDT
Thursday,
September 20, 2001

AVIATION SECURITY

Terrorist Acts Demonstrate Urgent Need to Improve Security at the Nation's Airports

Statement of Gerald L. Dillingham,
Director, Physical Infrastructure Issues

GAO
Accountability * Integrity * Reliability

GAO-01-1162T

Mr. Chairman and Members of the Committee:

A safe and secure civil aviation system is a critical component of the nation's overall security, physical infrastructure, and economic foundation. Billions of dollars and a myriad of programs and policies have been devoted to achieving such a system. Although it is not fully known at this time what actually occurred or what all the weaknesses in the nation's aviation security apparatus are that contributed to the horrendous events of last week, it is clear that serious weaknesses exist in our aviation security system and that their impact can be far more devastating than previously imagined.

We are here today to discuss the vulnerabilities that we have identified throughout the nation's aviation system. Our testimony is based on our prior work and includes assessments of security concerns with (1) aviation-related computer systems, (2) airport access controls, and (3) passenger and carry-on baggage screening, including how the United States and selected other countries differ in their screening practices. Our testimony will also offer some observations about improving aviation security in these various areas.

In summary:

- As we reported last year, our reviews of the Federal Aviation Administration's (FAA) oversight of air traffic control (ATC) computer systems showed that FAA had not followed some critical aspects of its own security requirements. Specifically, FAA had not ensured that ATC buildings and facilities were secure, that the systems themselves were protected, and that the contractors who access these systems had undergone background checks. As a result, the ATC system was susceptible to intrusion and malicious attacks. FAA is making some progress in addressing the 22 recommendations we made to improve computer security, but most have yet to be completed.
- Controls for limiting access to secure areas, including aircraft, have not always worked as intended. As we reported in May 2000, our special agents used fictitious law enforcement badges and credentials to gain access to secure areas, bypass security checkpoints at two airports, and walk unescorted to aircraft departure gates. The agents, who had been issued tickets and boarding passes, could have carried weapons, explosives, or other dangerous objects onto aircraft. FAA is acting on the weaknesses we identified and is implementing improvements to more closely check the credentials of law enforcement officers. The Department of Transportation's Inspector General has also documented numerous

problems with airport access controls, and in one series of tests, the Inspector General's staff successfully gained access to secure areas 68 percent of the time.

- As we reported in June 2000, tests of screeners revealed significant weaknesses as measured in their ability to detect threat objects located on passengers or contained in their carry-on luggage. In 1987, screeners missed 20 percent of the potentially dangerous objects used by FAA in its tests. At that time, FAA characterized this level of performance as unsatisfactory. More recent results have shown that as testing gets more realistic—that is, as tests more closely approximate how a terrorist might attempt to penetrate a checkpoint—screeners' performance declines significantly. A principal cause of screeners' performance problems is the rapid turnover among screeners. Turnover exceeded over 100 percent a year at most large airports, leaving few skilled and experienced screeners, primarily because of the low wages, limited benefits, and repetitive, monotonous nature of their work. Additionally, too little attention has been given to factors such as the sufficiency of the training given to screeners. FAA's efforts to address these problems have been slow. We recommended that FAA develop an integrated plan to focus its efforts, set priorities, and measure progress in improving screening. FAA is addressing these recommendations, but progress on one key effort—the certification of screening companies—is still not complete because the implementing regulation has not been issued. It is now nearly 2 ½ years since FAA originally planned to implement the regulation.
- Screening operations in Belgium, Canada, France, the Netherlands, and the United Kingdom—countries whose systems we have examined—differ from this country's in some significant ways. Their screening operations require more extensive qualifications and training for screeners, include higher pay and better benefits, and often include different screening techniques, such as "pat-downs" of some passengers. Another significant difference is that most of these countries place responsibility for screening with airport authorities or the government instead of air carriers. The countries we visited had significantly lower screener turnover, and there is some evidence they may have better screener performance; for example, one country's screeners detected over twice as many test objects as did U.S. screeners in a 1998 joint screener testing program conducted with FAA.

The events of September 11, 2001, have changed the way this country looks at aviation security. Last week, FAA and the air carriers implemented new controls that promise a greater sense of security. We support these actions. Yet, to further minimize the vulnerabilities in our aviation security system, more needs to be done. Additional

considerations for the immediate future could include prioritizing outstanding recommendations that address security, developing a strategic plan to address the recommendations, assigning specific executive responsibility for carrying out this plan, and identifying the sources and amounts of funding needed. In establishing priorities, a key action needed is to complete the promulgation of the screening company certification regulation, which also implements the requirements of the Airport Security Improvement Act of 2000, enacted by the Congress last November. The Congress also needs to reconsider whether airlines should continue to bear primary responsibility for screening operations at the nation's airports. Aviation security has truly become a national security issue, and responsibility for screening may no longer appropriately rest with air carriers. Consideration of the role of air carriers in conducting passenger screening could be examined as part of the ongoing effort to identify and structure mechanisms to provide financial and other assistance to help the aviation industry emerge from the current crisis.

Mr. Chairman, it has been observed that previous tragedies have resulted in congressional hearings, studies, recommendations, and debates, but little long-term resolve to correct flaws in the system as the memory of the crisis recedes. The future of aviation security hinges in large part on overcoming this cycle of limited action that has too often characterized the response to aviation security concerns.

Background

Some context for my remarks is appropriate. The threat of terrorism was significant throughout the 1990s; a plot to destroy 12 U.S. airliners was discovered and thwarted in 1995, for instance. Yet the task of providing security to the nation's aviation system is unquestionably daunting, and we must reluctantly acknowledge that any form of travel can never be made totally secure. The enormous size of U.S. airspace alone defies easy protection. Furthermore, given this country's hundreds of airports, thousands of planes, tens of thousands of daily flights, and the seemingly limitless ways terrorists or criminals can devise to attack the system, aviation security must be enforced on several fronts. Safeguarding airplanes and passengers requires, at the least, ensuring that perpetrators are kept from breaching security checkpoints and gaining access to secure airport areas or to aircraft. Additionally, vigilance is required to prevent attacks against the extensive computer networks that FAA uses to guide thousands of flights safely through U.S. airspace. FAA has developed several mechanisms to prevent criminal acts against aircraft, such as adopting technology to detect explosives and establishing procedures to ensure that passengers are positively identified before boarding a flight.

Still, in recent years, we and others have often demonstrated that significant weaknesses continue to plague the nation's aviation security.

Potential for Unauthorized Access to Aviation Computer Systems

Our work has identified numerous problems with aspects of aviation security in recent years. One such problems is FAA's computer-based air traffic control system. The ATC system is an enormous, complex collection of interrelated systems, including navigation, surveillance, weather, and automated information processing and display systems that link hundreds of ATC facilities and provide information to air traffic controllers and pilots. Failure to adequately protect these systems could increase the risk of regional or nationwide disruption of air traffic—or even collisions.

In five reports issued from 1998 through 2000, we pointed out numerous weaknesses in FAA's computer security.[1] FAA had not (1) completed background checks on thousands of contractor employees, (2) assessed and accredited as secure many of its ATC facilities, (3) performed appropriate risk assessments to determine the vulnerability of the majority of its ATC systems, (4) established a comprehensive security program, (5) developed service continuity controls to ensure that critical operations continue without undue interruption when unexpected events occur, and (6) fully implemented an intrusion detection capability to detect and respond to malicious intrusions. Some of these weaknesses could have led to serious problems. For example, as part of its Year 2000 readiness efforts, FAA allowed 36 mainland Chinese nationals who had not undergone required background checks to review the computer source code for eight mission-critical systems.

To date, we have made nearly 22 recommendations to improve FAA's computer security. FAA has worked to address these recommendations, but most of them have yet to be completed. For example, it is making progress in obtaining background checks on contractors and accrediting

[1] *Aviation Security: Weak Computer Security Practices Jeopardize Flight Safety* (GAO/AIMD-98-155, May 18, 1998), *Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software* (GAO/AIMD-00-55, Dec. 23, 1999), *Computer Security: FAA is Addressing Personnel Weaknesses, But Further Action Is Required* (GAO/AIMD-00-169, May 31, 2000), *FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses* (GAO/AIMD-00-252, Aug. 16, 2000), and *FAA Computer Security: Recommendations to Address Continuing Weaknesses* (GAO-01-171, Dec. 6, 2000).

facilities and systems as secure. However, it will take time to complete these efforts.

Weaknesses in Airport Access Controls

Control of access to aircraft, airfields, and certain airport facilities is another component of aviation security. Among the access controls in place are requirements intended to prevent unauthorized individuals from using forged, stolen, or outdated identification or their familiarity with airport procedures to gain access to secured areas. In May 2000, we reported that our special agents, in an undercover capacity, obtained access to secure areas of two airports by using counterfeit law enforcement credentials and badges.[2] At these airports, our agents declared themselves as armed law enforcement officers, displayed simulated badges and credentials created from commercially available software packages or downloaded from the Internet, and were issued "law enforcement" boarding passes. They were then waved around the screening checkpoints without being screened. Our agents could thus have carried weapons, explosives, chemical/biological agents, or other dangerous objects onto aircraft. In response to our findings, FAA now requires that each airport's law enforcement officers examine the badges and credentials of any individual seeking to bypass passenger screening. FAA is also working on a "smart card" computer system that would verify law enforcement officers' identity and authorization for bypassing passenger screening.

The Department of Transportation's Inspector General has also uncovered problems with access controls at airports. The Inspector General's staff conducted testing in 1998 and 1999 of the access controls at eight major airports and succeeded in gaining access to secure areas in 68 percent of the tests; they were able to board aircraft 117 times. After the release of its report describing its successes in breaching security,[3] the Inspector General conducted additional testing between December 1999 and March 2000 and found that, although improvements had been made, access to secure areas was still gained more than 30 percent of the time.

[2] *Security: Breaches at Federal Agencies and Airports* (GAO/T-OSI-00-10, May 25, 2000).

[3] *Airport Access Control* (AV-2000-017, Nov. 18, 1999).

Inadequate Detection of Dangerous Objects by Screeners

Screening checkpoints and the screeners who operate them are a key line of defense against the introduction of dangerous objects into the aviation system. Over 2 million passengers and their baggage must be checked each day for articles that could pose threats to the safety of an aircraft and those aboard it. The air carriers are responsible for screening passengers and their baggage 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 mostly air carriers hire security companies to do the screening. Currently, multiple carriers and screening companies are responsible for screening at some of the nation's larger airports.

Concerns have long existed over screeners' ability to detect and prevent dangerous objects from entering secure areas. Each year, weapons were discovered to have passed through one checkpoint and have later been found during screening for a subsequent flight. FAA monitors the performance of screeners by periodically testing their ability to detect potentially dangerous objects carried by FAA special agents posing as passengers. In 1978, screeners failed to detect 13 percent of the objects during FAA tests. In 1987, screeners missed 20 percent of the objects during the same type of test. Test data for the 1991 to 1999 period show that the declining trend in detection rates continues.[4] Furthermore, the recent tests show that as tests become more realistic and more closely approximate how a terrorist might attempt to penetrate a checkpoint, screeners' ability to detect dangerous objects declines even further.

As we reported last year, there is no single reason why screeners fail to identify dangerous objects.[5] Two conditions—rapid screener turnover and inadequate attention to human factors—are believed to be important causes. Rapid turnover among screeners has been a long-standing problem, having been identified as a concern by FAA and by us in 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 according to our more recent work, the turnover is considerably higher.[6] From May

[4]Information on FAA tests results is now designated as sensitive security information and cannot be publicly released. Consequently, we cannot discuss the actual detection rates for the 1991-99 period.

[5]*Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance* (GAO/RCED-00-75, June 28, 2000).

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

1998 through April 1999, screener turnover averaged 126 percent at the nation's 19 largest airports; 5 of these airports reported turnover of 200 percent or more, and one reported turnover of 416 percent. At one airport we visited, of the 993 screeners trained at that airport 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 limit the level of experience among screeners operating a checkpoint.

Both FAA and the aviation industry attribute the rapid turnover to the low wages and minimal benefits screeners receive, along with the daily stress of the job. Generally, screeners are paid at or near the minimum wage. We reported last year that some of the screening companies at 14 of the nation's 19 largest airports paid screeners a starting salary of $6.00 an hour or less and, at 5 of these airports, the starting salary was the then-minimum wage—$5.15 an hour. It is common for the starting wages at airport fast-food restaurants to be higher than the wages screeners receive. For instance, at one airport we visited, 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.

The demands of the job also affect performance. 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) improving individuals' aptitudes for effectively performing screener duties, (2) the sufficiency of the training provided to screeners and how well they comprehend it, and (3) the monotony of the job and the distractions that reduce screeners' vigilance. As a result, screeners are being placed on the job who do not have the necessary aptitudes, nor the adequate knowledge to effectively perform the work, and who then find the duties tedious and dull.

We reported in June 2000 that FAA was implementing a number of actions to improve screeners' performance. However, FAA did not have an integrated management plan for these efforts that would identify and prioritize checkpoint and human factors problems that needed to be resolved, and identify measures—and related milestone and funding information—for addressing the performance problems. Additionally, FAA did not have adequate goals by which to measure and report its progress in improving screeners' performance.

FAA is implementing our recommendations. However, two key actions to improving screeners' performance are still not complete. These actions are the deployment of threat image projection systems—which place images

of dangerous objects on the monitors of X-ray machines to keep screeners alert and monitor their performance—and a certification program to make screening companies accountable for the training and performance of the screeners they employ. Threat image projection systems are expected to keep screeners alert by periodically imposing the image of a dangerous object on the X-ray screen. They also are used to measure how well screeners perform in detecting these objects. Additionally, the systems serve as a device to train screeners to become more adept at identifying harder-to-spot objects. FAA is currently deploying the threat image projections systems and expects to have them deployed at all airports by 2003.

The screening company certification program, required by the Federal Aviation Reauthorization Act of 1996, will establish performance, training, and equipment standards that screening companies will have to meet to earn and retain certification. However, FAA has still not issued its final regulation establishing the certification program. This regulation is particularly significant because it is to include requirements mandated by the Airport Security Improvement Act of 2000 to increase screener training—from 12 hours to 40 hours—as well as expand background check requirements. FAA had been expecting to issue the final regulation this month, 2 ½ years later than it originally planned.

Differences in the Screening Practices of Five Other Countries and the United States

We visited five countries—Belgium, Canada, France, the Netherlands, and the United Kingdom—viewed by FAA and the civil aviation industry as having effective screening operations to identify screening practices that differ from those in the United States. We found that some significant differences exist in four areas: screening operations, screener qualifications, screener pay and benefits, and institutional responsibility for screening.

First, screening operations in some of the countries we visited 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 in Brussels, a constant police presence is maintained at one of two glass-enclosed rooms directly behind the checkpoints.

Second, screeners' qualifications are usually more extensive. In contrast to the United States, Belgium requires screeners to be citizens; 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. Training requirements for screeners were also greater in four of the countries we visited than in the United States. While FAA requires that screeners in this country have 12 hours of classroom training before they can begin work, Belgium, Canada, France, and the Netherlands require more. For example, France requires 60 hours of training and Belgium requires at least 40 hours of training with an additional 16 to 24 hours for each activity, such as X-ray machine operations, that the screener will conduct.

Third, screeners receive relatively better pay and benefits in most of these countries. Whereas screeners in the United States receive wages that are at or slightly above minimum wage, screeners in some countries receive wages that are viewed as being at the "middle income" level in those countries. In the Netherlands, for example, screeners received at least the equivalent of about $7.50 per hour. This wage was about 30 percent higher than the wages at fast-food restaurants in that country. In Belgium, screeners received the equivalent of about $14 per hour. Not only is pay higher, but the screeners in some countries receive benefits, such as health care or vacations—in large part because these benefits are required under the laws of these countries. These countries also have significantly lower screener turnover than the United States: turnover rates were about 50 percent or lower in these countries.

Finally, the responsibility for screening in most of these countries is placed with the airport authority 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 and 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. We note that, worldwide, of 102 other countries with international airports, 100 have placed screening responsibility with the airports or the government; only 2 other countries—Canada and Bermuda—place screening responsibility with air carriers.

Because each country follows its own unique set of screening practices, and because data on screeners' performance in each country were not

available to us, it is difficult to measure the impact of these different practices on improving screeners' performance. Nevertheless, there are indications that for least one country, practices may help to improve screeners' performance. This country conducted a screener testing program jointly with FAA that showed that its screeners detected over twice as many test objects as did screeners in the United States.

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions that you or Members of the Committee 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 Bonnie Beckett, J. Michael Bollinger, Colin J. Fallon, John R. Schulze, and Daniel J. Semick.

Related GAO Products

Responses of Federal Agencies and Airports We Surveyed About Access Security Improvements (GAO-01-1069R, Aug. 31, 2001).

Aviation Security: Additional Controls Needed to Address Weaknesses in Carriage of Weapons Regulations (GAO/RCED-00-181, Sept. 29, 2000).

FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations (GAO/T-AIMD-00-330, Sept. 27, 2000).

FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses (GAO/AIMD-00-252, Aug. 16, 2000).

Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance (GAO/RCED-00-75, June 28, 2000).

Computer Security: FAA Is Addressing Personnel Weaknesses, But Further Action Is Required (GAO/AIMD-00-169, May 31, 2000).

Security: Breaches at Federal Agencies and Airports (GAO-OSI-00-10, May 25, 2000).

Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism (GAO/NSIAD-00-85, Apr. 7, 2000).

Aviation Security: Vulnerabilities Still Exist in the Aviation Security System (GAO/T-RCED/AIMD-00-142, Apr. 6, 2000).

Aviation Security: Slow Progress in Addressing Long-Standing Screener Performance Problems (GAO/T-RCED-00-125, Mar. 16, 2000).

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

FBI: Delivery of ATF Report on TWA Flight 800 Crash (GAO/OSI-99-18R, Aug. 13, 1999).

Aviation Security: FAA's Actions to Study Responsibilities and Funding for Airport Security and to Certify Screening Companies (GAO/RCED-99-53, Feb. 25, 1999).

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

Aviation Security: Progress Being Made, but Long-Term Attention Is Needed (GAO/T-RCED-98-190, May 14, 1998).

Aviation Security: Implementation of Recommendations Is Under Way, but Completion Will Take Several Years (GAO/RCED-98-102, Apr. 24, 1998).

Combating Terrorism: *Observations on Crosscutting Issues* (T-NSIAD-98-164, Apr. 23, 1998).

Aviation Safety: Weaknesses in Inspection and Enforcement Limit FAA in Identifying and Responding to Risks (GAO/RCED-98-6, Feb. 27, 1998).

Aviation Security: FAA's Procurement of Explosives Detection Devices (GAO/RCED-97-111R, May 1, 1997).

Aviation Security: Commercially Available Advanced Explosives Detection Devices (GAO/RCED-97-ll9R, Apr. 24, 1997).

Aviation Security: Posting Notices at Domestic Airports (GAO/RCED-97-88R, Mar. 25, 1997).

Aviation Safety and Security: Challenges to Implementing the Recommendations of the White House Commission on Aviation Safety and Security (GAO/T-RCED-97-90, Mar. 5, 1997).

Aviation Security: Technology's Role in Addressing Vulnerabilities (GAO/T-RCED/NSIAD-96-262, Sept. 19, 1996).

Aviation Security: Urgent Issues Need to Be Addressed (GAO/T-RCED/NSIAD-96-251, Sept. 11, 1996).

Terrorism and Drug Trafficking: Technologies for Detecting Explosives and Narcotics (GAO/NSIAD/RCED-96-252, Sept. 4, 1996).

Aviation Security: Immediate Action Needed to Improve Security (GAO/T-RCED/NSIAD-96-237, Aug. 1, 1996).

Terrorism and Drug Trafficking: Threats and Roles of Explosives and Narcotics Detection Technology (GAO/NSIAD/RCED-96-76BR, Mar. 27, 1996).

Aviation Security: FAA Can Help Ensure that Airport's Access Control Systems are Cost Effective (GAO/RCED-95-25, Mar. 1, 1995).

Aviation Security: Development of New Security Technology Has Not Met Expectations (GAO/RCED-94-142, May 19, 1994).

Aviation Security: Additional Actions Needed to Meet Domestic and International Challenges (GAO/RCED-94-38, Jan. 27, 1994).