Office of Inspector General

Aviation Security

Federal Aviation Administration

Report Number: AV-2000-070
Date Issued: March 23, 2000

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: **INFORMATION**: Aviation Security, Federal Aviation Administration AV-2000-070

Date: March 23, 2000

From: Alexis M. Stefani
Assistant Inspector General for Auditing

Reply to Attn of: JA-10:60500

To: Federal Aviation Administrator

On March 16, 2000, at a hearing before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, U.S. House of Representatives, we provided testimony on aviation security. Our testimony addressed the reliance of aviation security on each employee in the aviation system doing his or her part, and what needs to be done to ensure that these employees are well-trained, trustworthy and held accountable for compliance with security requirements. We also addressed the need for FAA to have an integrated strategic plan to guide its efforts and prioritize funding needs. A copy of our statement is attached for your information.

Specifically, we testified on (1) implementing and deploying technology that enhances screener performance, (2) strengthening background investigation requirements for granting access to secure areas of the airport, (3) controlling access to secure airport areas and holding employees accountable for access control requirements, and (4) establishing a strategic plan that integrates employees and technology into a comprehensive, seamless security program.

We are not making specific recommendations in this report. Later this year, we will issue separate reports with recommendations on the results of our audits of Controls Over Airport Identification Media, and Followup on Deployment of Explosives Detection Equipment.

The Office of Inspector General will continue to monitor FAA's progress in improving aviation security. If I can answer any questions or be of further assistance, please contact me at (202) 366-1992, or David A. Dobbs, Deputy Assistant Inspector General for Aviation, at (202) 366-0500.

Attachment

#

R/SF/Testify/Transmittal.doc

Before the Subcommittee on Aviation,
Committee on Transportation and Infrastructure,
U.S. House of Representatives

For Release on Delivery
Expected at
10:00 a.m. EST
Thursday
March 16, 2000
Report Number: AV-2000-070

Aviation Security
Federal Aviation Administration

Statement of
Alexis M. Stefani
Assistant Inspector General for Auditing
U.S. Department of Transportation

Mr. Chairman and Members of the Subcommittee:

We appreciate the opportunity to discuss aviation security. One of the Department of Transportation's (DOT) five strategic goals is National Security. Likewise, FAA has as a strategic goal the prevention of security incidents in the aviation system. Security of the Nation's aviation, surface, and marine transportation systems is one of the 12 management issues we have identified for DOT this year.

Aviation security is a layered system of systems that is dependent on the coordination of airport and air carrier security operations and the integration of people and technology. Perhaps the most important factor in an effective security program is well-trained, alert screeners, baggage handlers, and other employees processing passengers or having access to secure areas of the airport. Aviation security relies heavily on each employee in the aviation system doing his or her part.

Today we would like to discuss four issues: (1) implementing and deploying technology that enhances screener performance, (2) strengthening background investigation requirements for granting access to secure areas of the airport, (3) controlling unauthorized access to secure airport areas and holding employees accountable for access control requirements, and (4) establishing a strategic plan that integrates employees and technology into a comprehensive, seamless security program.

- **First**, in fiscal years (FY) 1997 through 2000, Congress authorized more than $350 million for the deployment of advanced security technologies. FAA has used these funds to deploy FAA-certified[1] and non-certified bulk explosives detection machines, explosives trace detection devices, Computer-Based Training platforms, and Computer-Assisted Passenger Prescreening Systems. FAA plans to continue deploying many of these same technologies in the future, as well as deploying new screening checkpoint x-rays machines. Although advanced security technologies are effective in detecting explosives, each one is ultimately dependent on the human operator.

  FAA believes - and we agree - that operators of advanced security equipment are critical in improving security. FAA test results indicate that new technologies to detect explosives in passenger baggage can correctly identify a potential threat but a screener can make a wrong decision and "clear" the bag.

[1] FAA's standards for certifying explosives detection systems for screening checked baggage are classified. The certification standard sets criteria for detection, false alarm, and baggage processing rates.

Screeners who operate security equipment must be carefully selected, monitored, and trained.

In September 1996, the White House Commission on Aviation Safety and Security (Gore Commission) recommended that FAA certify screening companies and improve screener performance. In May 2001, FAA expects to issue a final rule establishing training requirements for screeners and requiring screening companies to be certified. To achieve this, FAA needs to have a means to measure screener performance, and methods of providing initial and recurrent screener training as well as ensuring that the screeners maintain their proficiency through actual experience with the machines in the airport environment.

FAA will rely on Threat Image Projection (TIP) to measure the performance of individual screeners and certify screening companies. TIP is a computer software program, which projects fictitious images on to bags or an entire fictitious bag containing a threat. TIP is intended to keep equipment operators alert, provide real world conditions, and measure performance in identifying the fictitious items or bags. TIP is installed on the actual equipment the screener uses each day to screen passenger baggage. TIP has been installed on all CTX[2] machines used to screen checked baggage. FAA is currently testing TIP equipped x-ray machines used to screen carry-on items. FAA plans to purchase more than 1,200 new TIP equipped x-ray machines for screening checkpoints by the end of FY 2003.

Another needed technology is Computer-Based Training (CBT), an intensive course of self-paced, realistic learning using computer workstations. It is used to select, train, evaluate, and monitor the performance of employees who operate x-ray machines at passenger screening checkpoints. Although FAA began deploying CBT in April 1997, as of March 1999 FAA has only 38 CBT platforms[3] installed at 37 airports. However, there has not been any increase during the last year in the number of deployed CBT platforms and some are being used infrequently. To complete deployment to all 79 large airports an additional 42 platforms need to be installed.

Explosives detection equipment such as the CTX machine was developed to assist screeners in identifying threat items in passenger baggage. However, CTX machines are still underused, and screeners' performance needs

[2] The InVision Technologies CTX 5500 machines are the only FAA-certified bulk explosives detection devices currently deployed at U.S. airports.

[3] A CBT Platform consists of a network server with installed software, and networked computer terminals (workstations).

improvement. Our recent audit work found that over 50 percent of the deployed CTX machines still screen fewer than 225 **bags per day**, on average, compared to a certified rate of 225 **bags per hour**.

According to a recent report by the National Research Council, "Underutilization poses a potential problem for the maintenance of operator skills, particularly the skills required for resolving alarms, because underpracticed skills often deteriorate." Recent testing by FAA showed a significant number of failures by CTX operators. FAA concluded that a major factor in the test failures appeared to be the performance of CTX operators, and not the CTX machine itself. In response to our 1998 report on the deployment of explosives detection equipment, FAA agreed to conduct a study to determine the minimum CTX daily processing rates needed to ensure operator proficiency, and use the results to establish minimum daily use rates. To date, no study has been conducted.

- **Second**, actions are needed to improve the process used to ensure that employees with access to secure areas of an airport are trustworthy.

  Our recent review of industry's compliance with FAA's background investigation requirements at six U.S. airports found that the requirements were ineffective, and airport operators, air carriers and airport users[4] frequently did not comply with these requirements. For example, Federal Bureau of Investigation (FBI) criminal checks[5] are currently only required in certain cases, such as when there is an unexplained gap of employment of 12 months or more. However, according to the U.S. Department of Justice 43 percent of violent felony convictions resulted in probation or an average jail time of just 7 months.

  When the current requirements were proposed in 1992, processing fingerprints and performing the criminal check took up to 90 days. Today, technology allows this process to be completed in only a few days, and airport operators and FAA both agree the requirements need to be revised.

  Although the background investigation requirements need to be revised, it is important that airport operators, air carriers and airport users comply with existing background investigation requirements as well as requirements to

[4] Airport users include foreign air carriers, non-air-carrier airport tenants, and companies that do not have offices at the airport, but require access to the secure airport areas.

[5] A comparison of the individual's fingerprints to the FBI's database of individuals convicted of crimes in the United States. The FBI returns a complete criminal history if there is a fingerprint match.

account for airport identification (ID). Our recent audit found that for 35 percent of the employee files reviewed there was no evidence that a 5-year history verification was conducted, the verification was incomplete, or no file was available for review. In addition, 9 percent of the active airport IDs we reviewed were issued to employees who no longer needed access to secure areas.

- **Third,** once hired, employees must be held accountable for compliance with airport access control requirements. Airport access control has been, and continues to be, an area of great concern due to increased threat to U.S. airport facilities and aircraft. During late 1998 and early 1999, we successfully accessed secure areas[6] in 68 percent of our tests at eight major U.S. airports. Once we entered secure areas, we boarded aircraft 117 times. The majority of our aircraft boardings would not have occurred if employees had taken the prescribed steps, such as making sure doors closed behind them.

  Recent FAA results demonstrate that compliance can improve with continuous oversight, but testing is not the only answer. During testing in December 1999 and January 2000 at 10 airports, FAA successfully accessed secure areas 40 percent of the time without being challenged by employees. In February 2000, FAA expanded its testing to 80 airports, and as of February 23, 2000, FAA was successful in accessing secure areas 32 percent of the time without being challenged by airport personnel. When noncompliance was found, FAA took actions to correct the problem, such as requiring guards on doors to ensure only authorized employees accessed the secure area.

  In June 2000, FAA plans to issue regulations making individuals directly accountable to FAA for noncompliance with access control requirements. This will permit FAA to take enforcement action against the employee instead of the air carrier or airport when an employee does not follow access control requirements.

- **Finally,** FAA has made significant progress in deploying existing advanced security technologies; however, it continues to focus on the acquisition and deployment process, rather than on the necessary transition to integrating all the various assets into a comprehensive, seamless security program. From FYs 1997 through 2000, Congress has authorized $200 million in Research, Engineering, and Development funds, and over $350 million in Facilities and Equipment funds for various security efforts. FAA is approximately at the

[6] OIG uses the term **secure area** to define the area of an airport where each person is required to display airport-approved identification. Each airport defines this area, which may be the entire Air Operations Area or may be limited to a smaller, more restrictive area.

halfway point in the effort started by the Gore Commission. FAA expects to spend an additional $600 million on aviation security through FY 2004.

To meet current and future threats to aviation security, FAA needs an integrated strategic plan to guide its efforts and prioritize funding needs. Concentration on deployment (what to buy, when to buy it, and where to put it) is not the complete solution. This plan should include a balanced approach covering basic research, equipment deployment and use, certification and operator testing processes, data collection and analysis on actual equipment and operator performance, and regulation and enforcement. Although we recommended such a plan in 1998, FAA has made little progress in developing this strategic plan.

BACKGROUND

The responsibility for aviation security is shared between FAA, the airlines, airports, and employees. FAA sets guidelines, establishes policies and procedures, and makes judgments on how to meet threats to aviation based on information from the intelligence community. FAA then tests the aviation industry to ensure they are complying with the many security requirements. FAA also sponsors the development, purchase, and deployment of new security technology, such as explosives detection equipment, for industry use. Airports are responsible for the security of the airport environment. Airlines are responsible for screening baggage, passengers, and cargo. Until recently, airlines and airports have been responsible for purchasing security equipment and systems.

The July 1996 crash of TWA Flight 800 was the catalyst for important advances in aviation security. Although the FBI and the National Transportation Safety Board have ruled out terrorist activity as a potential cause of the crash, the crash prompted the August 1996 creation of the White House Commission on Aviation Safety and Security (known as the Gore Commission). Its September 1996 and February 1997 reports addressed safety, security, and air traffic control modernization. The Gore Commission made 31 recommendations regarding

aviation security, including recommendations that FAA: (1) certify screening companies and improve screener performance; (2) require FBI criminal checks for all airport and air carrier employees with access to secure areas, no later than mid-1999; (3) develop comprehensive and effective means to control unauthorized access to aircraft and secure airport areas; and (4) deploy new explosives detection equipment.

Since 1997, Congress has provided over $350 million for deployment of advanced security technology, and $200 million in aviation security Research, Engineering and Development including about $21 million for human factors research. As of February 11, 2000, FAA has installed new security technologies, including 92 FAA-certified explosives detection machines at 35 airports, and 553 explosives trace detection devices at 84 U.S. and foreign airports. For FY 2001, FAA has requested $98 million to continue the deployment and $49 million for aviation security research, engineering, and development.

SECURITY SCREENER PERSONNEL

The Gore Commission recognized that it is critical to ensure that those charged with providing security for over 500 million passengers a year in the United States are the best qualified and trained in the industry. The Gore Commission further recognized that better selection, training, and testing of the people who work at airport x-ray machines would result in a significant boost in security. Therefore, in September 1996, the Commission recommended that FAA certify screening companies and improve screener performance. In October 1996, the President signed the Federal Aviation Reauthorization Act of 1996 (Public Law 104-264), which requires FAA to certify companies providing security screening, and to improve the training and testing of security screeners through development of uniform performance standards.

In February 1997, the Gore Commission recommended that FAA work with the private sector and other Federal agencies to promote the professionalism of security personnel through a program that would include performance standards that reflect best practices, and adequate, common, and recurrent training that considers human factors.

TIP Must Be Properly Deployed Before Screening Companies Can Be Certified. In response to the Gore Commission recommendation and the direction contained in Public Law 104-264, FAA published an advance notice of proposed rulemaking on the certification of screening companies in March 1997, but withdrew it in May 1998 because there was no reliable and consistent way to measure screeners' performance at the time. In January 2000, FAA again published a notice of proposed rulemaking that would require screening companies to be certified by FAA. The comment period for this proposed rule ends on May 4, 2000.

TIP is the system that FAA will rely on to provide uniform data regarding screener performance, and thus use to evaluate and certify screening companies under the proposed rule. The TIP systems use two different methods of projection. One method, used with screening checkpoint x-ray machines, superimposes the image of a threat item onto the x-ray image of the actual passenger baggage being screened. The other method, used with CTX machines, projects a prefabricated image of an entire threat bag onto the monitor.

FAA has only recently established procedures and controls for implementing and using the TIP program that has been installed on deployed CTX 5500 machines for almost a year. In response to our October 1999 audit report,[7] FAA issued new

[7] Follow-up Audit of Deployment of Explosives Detection Equipment, Federal Aviation Administration (Report No AV-2000-002, October 21, 1999).

guidance to air carriers in November 1999 that standardizes frequency of threat image presentation, provides better control over passwords, and requires that TIP be activated for each screening session. This should result in more consistent data on CTX screener performance.

The TIP program is not as fully developed for use on screening checkpoint x-ray machines, which are used to screen carry-on items. FAA is currently evaluating the TIP program for checkpoint x-ray machines in an operational airport environment. When this evaluation is complete, FAA intends to purchase and deploy 390 TIP-configured x-ray machines in FY 2000 for $24.26 million. FAA expects to begin this deployment next month. FAA must complete a successful field evaluation and ensure that management controls are in place prior to beginning the planned large-scale acquisition and deployment of this technology. FAA plans to purchase a total of more than 1,200 TIP-equipped x-ray machines by the end of FY 2003.

FAA Has Been Slow in Deploying Systems Needed to Train Screening Company Employees. CBT, a system that provides initial and recurrent training to screeners, is one of the technologies FAA is developing and deploying to improve screener performance. CBT offers an intensive course of realistic learning using computer workstations. It is used to select, train, evaluate, and monitor the performance of employees who operate screening checkpoint x-ray machines to screen carry-on items. The potential benefits of CBT are self-paced learning, enhanced opportunities for realistic practice, combined training and performance testing, and instruction that is uniform across the country.

Despite the potential benefits of CBT, its deployment and implementation has been slow. Deployment of CBT platforms to the 19 Category X[8] airports began in April 1997 and was completed in March 1999. The deployment of CBT platforms to 18 Category I[9] airports was completed in October 1998.

In March 1999, FAA reported that 42 additional platforms would be required to complete deployment to the remaining 60 Category I airports. Now, a year later there has been no change in the number of CBT platforms or the airports to which they had been deployed above what was reported last March.

In addition, some air carrier representatives told us that they were not using CBT. At five airports, they told us they are not using CBT primarily because of an inadequate number of available workstations installed at their airports and the inconvenient location of the installed workstations. For example, at Ronald Reagan Washington National Airport, the CBT workstations are located away from the new main terminal building in a maintenance hangar. However, at Honolulu International Airport, the screening company that provides all security screening services at the main terminal was very pleased with both the location of the CBT workstations and the quality and effectiveness of the CBT software, and used CBT frequently.

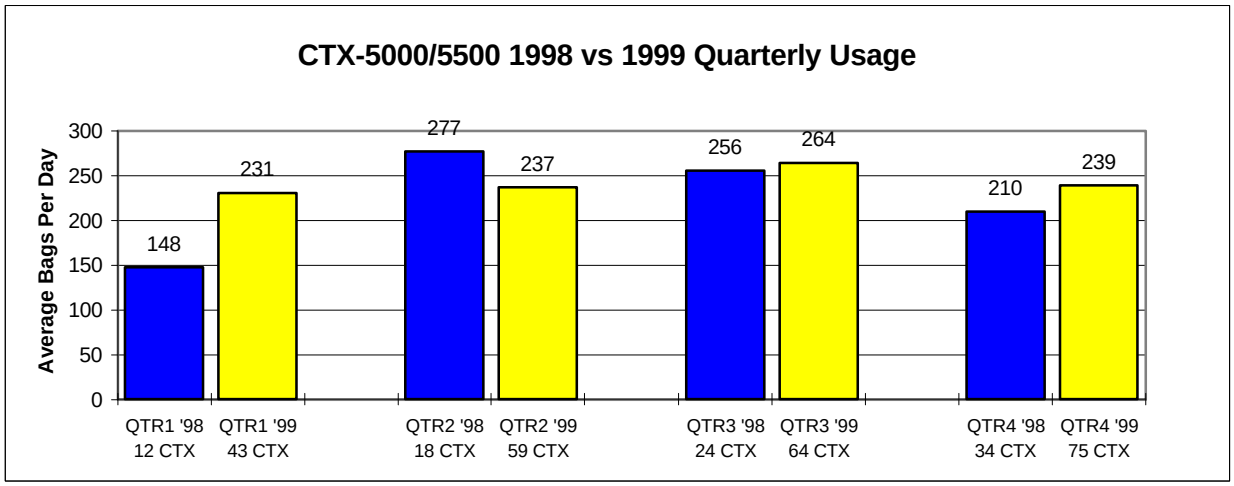
CBT has demonstrated that it can be a valuable and effective component in a system of systems intended to enhance aviation security. FAA needs to accelerate the deployment of this valuable training and evaluation technology.

---

[8] Category X airports represent the nation's largest and busiest airports as measured by the volume of passenger traffic and are potentially attractive targets for criminal and terrorist activity.

[9] Category I airports are somewhat smaller than Category X airports, and have an annual volume of at least 2 million passengers.

Explosives Detection Machines Used to Screen Checked Baggage Are Still Underused, and Screeners' Performance Needs Improvement. As the program to deploy bulk explosives detection equipment matures, and the record of operational experience with deployed machines lengthens, we expected to see an increase in utilization rates over what FAA was reporting a year ago. Certainly, there has been a steady increase in the total number of bags screened across the system, as more CTX machines are deployed. On the other hand, comparison of quarterly performance statistics compiled on a per machine basis in 1998 and 1999 shows no significant increase in CTX average usage rates, as shown below.



We compared the average number of bags screened daily by each CTX in 1998 and 1999, as reported quarterly by FAA, and found that there had been an average increase of only 20 bags per day per machine. We also found that the majority of deployed and operational machines still do not screen as many bags in a full day of operation as the machine is certified to screen in an hour. As shown in the table below, more than 50 percent of the deployed machines still screen less than 225 **bags per day**, on average, compared to a certified rate of 225 **bags per hour**.

	CY 1998				CY 1999			
	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr
Total machines in use	12	18	24	34	43	59	64	75
Machines averaging fewer than 225 bags per day	10	11	16	23	27	38	37	44
Percent of machines underused	83.3%	61.1%	66.7%	67.6%	62.8%	64.4%	57.8%	58.7%

FAA does not require the air carriers to screen more than the number of bags checked by "selectees." Selectees include (1) passengers selected by Computer-Assisted Passenger Prescreening Systems (CAPPS);[10] (2) passengers who cannot produce an approved form of identification; and (3) passengers unable to correctly answer the security questions required by the Air Carrier Standard Security Program.[11] Before full implementation of CAPPS, FAA expected a greater number of selectees then are currently being identified. These expensive machines have the demonstrated capability to screen more bags now than the air carriers are screening. Unless the number of CAPPS selectees is increased, or the air carriers agree to screen more than the minimum required number of bags, CTX machines will continue to be underused, which in turn could negatively affect the proficiency of screeners.

[10] CAPPS is an automated passenger profiling system that uses information in airline reservation systems to separate passengers into a very large majority who present no security risk, and a small minority (known as selectees) who merit additional attention, such as having their checked baggage screened using explosives detection equipment.

[11] The Air Carrier Standard Security Program, required by Title 14, Code of Federal Regulations, Part 108, describes the security procedures the air carrier agrees to follow.

According to a recent report by the National Research Council,[12] "Underutilization poses a potential problem for the maintenance of operator skills, particularly the skills required for resolving false alarms, because underpracticed skills often deteriorate. At some [CTX] locations, the throughput rate has been so low that operators could even lose their skills for operating the equipment."

This underutilization could result in screeners being less proficient when the equipment is being used. Our 1999 audit on security of checked baggage[13] demonstrated that CTX screening personnel were not competent at operating the equipment. We found that when CTX 5500's warned of a threat, the equipment operator did not look for or identify the threat object in a significant number of cases. During more recent testing by FAA, operators continued to fail a significant number of tests. The failures primarily occurred because operators cleared the test bag without a search, even though the machine had alarmed. FAA concluded that one of the major factors in the test failures appeared to be the performance of CTX operators, and not the performance of the machine itself.

In response to our October 1998 report on the deployment of explosives detection equipment, FAA agreed to conduct a study to determine the minimum CTX daily processing rates needed to ensure operator proficiency, and use the results to establish minimum daily utilization rates for machine operators. FAA expected to conduct this study and report the results by the end of FY 1999. To date, this study has not been conducted.

---

[12] Assessment of Technologies Deployed to Improve Aviation Security, First Report, National Research Council, issued in 1999.

[13] Security of Checked Baggage on Flights Within the United States, Federal Aviation Administration (Report No. AV-1999-113, July 16, 1999).

BACKGROUND INVESTIGATIONS

Effective security also requires that only trusted individuals are authorized access to secure areas. To accomplish this, FAA requires airport operators, air carriers and airport users to conduct employee background investigations before issuing airport ID that allows access secure airport areas.

FAA's background investigation procedures include: obtaining a 10-year employment history from those applying for access; verifying the most recent 5 years of that history; and performing an FBI criminal check when specific conditions are identified, such as a 12-month unexplained gap in employment. Individuals convicted within the past 10 years of any of 25 enumerated crimes are denied an airport ID.

However, our recent review at six U.S. airports found that FAA's background investigation requirements were ineffective. Specifically:

- FBI criminal checks are only required for employees applying for airport ID when one of four conditions triggers the checks. For example, one of the triggers, a 12-month unexplained gap in employment, was designed to identify individuals who were incarcerated for committing a serious crime. However, according to the U.S. Department of Justice, 61 percent of all state and Federal felony convictions resulted in probation or an average jail sentence of 6 months. Even for violent felonies, 43 percent of convictions resulted in probation or an average jail time of just 7 months.

- The list of 25 crimes that disqualified an employee from being issued airport ID was insufficient and did not include serious crimes, such as assault with a deadly weapon, unarmed robbery, burglary, larceny, and possession of drugs.

Our analysis of 53 employees issued airport ID and arrested in a recent Department of Justice investigation for smuggling contraband into and out of a major U.S. airport showed that individuals convicted of the 25 disqualifying crimes were not the only employees who presented a security risk. Of the 15 (28 percent) arrested employees with FBI criminal records, just one had a criminal record for a disqualifying crime (committed after being issued airport ID). Other arrested employees (14) had FBI criminal records for non-disqualifying felonies, such as larceny, battery, possession of a stolen vehicle, possession of drugs, and credit card fraud.

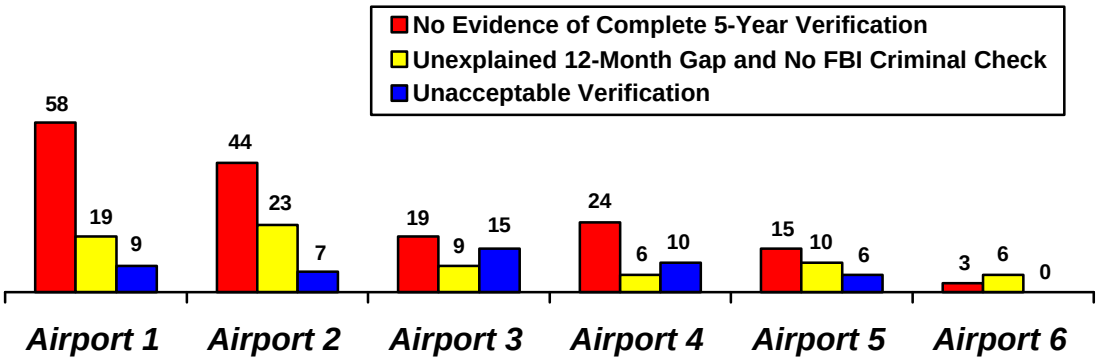
FAA should revise its background investigation requirements to include initial and recurring criminal checks for all employees issued airport ID to allow access to secure airport areas. In February 1992, FAA proposed requiring a criminal check for all individuals with unescorted access privileges. However, industry opposed the proposal based on its cost and the impracticality of escorting employees while waiting for results of a criminal check. In the past, performing a criminal check took up to 90 days, but with new technology, it can be completed in a few days.

Airport operators have supported requiring criminal checks for all employees with access to secure airport areas, and expanding the list of disqualifying crimes in the proposed FAA Reauthorization Act. As a result of the technology advancements and quicker processing time, FAA plans to initiate new rulemaking requiring criminal checks for all employees. We support these initiatives and recommend that new rules include initial and randomly recurring criminal checks for all employees with access to secure areas.

Although background investigation requirements need to be revised, it is important that airport operators, air carriers and airport users comply with current requirements. Our recent work at six airports found that these requirements were

not being met. For 35 percent of the employee files reviewed, there was no evidence that a complete background investigation was performed. Despite this failure to comply with security requirements, the employees were issued airport ID and granted access to secure airport areas.

Also, 15 percent of the employee files reviewed showed an unexplained gap of employment of 12 months or more, but the required FBI criminal check was not performed. Further, 9 percent of the background verifications we reviewed used an unacceptable method, such as verifying an employee's background with a personal reference or family member. The chart below summarizes the specific noncompliance with background investigation requirements for the six airports reviewed.



The most serious noncompliance was at Airports 1 and 2, which permitted airport users to self-certify that background investigations were performed but had not established controls to ensure the investigations were properly completed. For example, 58 percent of the employee files reviewed at Airport 1 did not have evidence that a complete verification was conducted of the 5-year history. In contrast, Airport 6, with the lowest rate of noncompliance, did not permit airport users to self-certify that background investigations were performed.

We also found FAA has not taken effective action to ensure compliance with current background investigation requirements. For example, FAA performs annual airport and air carrier assessments of compliance with security requirements and national assessments that focus on areas that require special emphasis. However, we found the assessments were limited in scope with regard to reviewing background investigation requirements. To illustrate, during an annual compliance review, FAA agents independently reviewed records for only airport operator employees and excluded airport user employees, where we found the majority of deficiencies. Also, FAA's national assessments of compliance mainly focused on airport users at 20 major U.S. airports.

Airport ID Controls. All six airport operators we reviewed did not properly account for airport ID or immediately deny access to secure areas when an employee's authorization changed. One of the primary requirements of an airport's access control system is the ability to immediately deny access to individuals whose authority changes, such as someone who has resigned. At the six airports reviewed, 9 percent (234 of 2,586 reviewed) of the IDs issued to employees for access to secure airport areas remained active even though the employees no longer needed the access.

Air carriers and airport users were not notifying the airport immediately when an employee no longer needed access. Although in some instances the employers had the active IDs in their possession, others were kept by employees who had resigned or had been terminated. For example, a regional air carrier could not account for 22 (18 percent) of 119 active airport IDs. Five of the IDs belonged to employees terminated prior to 1998.

We will be issuing a report to FAA on our work on airport ID controls. We will be recommending FAA revise its background investigation requirements, and

work with airport operators and air carriers to improve compliance with requirements for issuing and accounting for airport ID.

ACCESS CONTROL

Once hired, employees must be held accountable for compliance with airport access control requirements. Our December 1998 through April 1999 testing of airport access controls demonstrated significant access control vulnerabilities at all eight airports visited. We successfully penetrated secure areas on 117 (68 percent) of 173 attempts. Once we penetrated secure areas, we boarded aircraft operated by 35 different air carriers 117[14] times. Passengers were onboard 18 of the aircraft we boarded. In 12 instances, we were seated and ready for departure at the time we concluded our tests.

In these tests, the human element continued to be the primary access control weakness. The majority of our penetrations into secure areas that resulted in testers boarding aircraft would not have occurred if employees had (1) ensured the door closed behind them after entering the secure area; (2) challenged us for following them into secure areas; or (3) taken other steps required to restrict entry into secure areas, such as controlling pedestrian access through cargo facilities and vehicle gates.

After our testing, FAA conducted approximately 3,000 tests at 79 airports in the spring of 1999. FAA reported that its test results were "strikingly" different from our results and that compliance with access control requirements had dramatically improved. We have completed a review of FAA's test data and found the results

[14] It is a coincidence that the number of penetrations into secure areas and aircraft boardings both equal 117. Not all penetrations resulted in boarding aircraft, and some penetrations resulted in multiple aircraft boardings.

were very similar to those we reported with regard to penetrating secure areas. Specifically, FAA successfully penetrated secure areas 56 percent of the times tested versus our rate of 68 percent.

FAA reported improvement because 96 percent of its tests did not result in testers boarding aircraft for 3 minutes or more without being challenged. However, our testers were not required to remain onboard aircraft for a specified period of time, and some tests, such as driving through vehicle gates, could not result in boarding aircraft. Therefore, it is not accurate to compare FAA's test results to our results in terms of aircraft boardings.

In December 1999 and January 2000, FAA agents performed follow-up testing at 10 airports. They gained access to secure areas 40 percent of the times attempted without being challenged by employees, and they boarded 13 aircraft. In February 2000, FAA expanded its testing to 80 airports, resulting in FAA agents penetrating secure areas 32 percent of the times attempted with 57 aircraft boarded.[15] Although according to FAA the number of aircraft boardings compared to the number of tests performed has continued to decline, a different testing protocol for boarding aircraft was used during each assessment. Therefore, comparing test results with prior periods and determining improvement in compliance based on aircraft boardings may not be appropriate.

FAA's test results demonstrate that aggressive testing can result in improved compliance. Also, when FAA ensures that corrective actions are taken, access control violations are reduced. For example, for one airport we reviewed in 1999, FAA's recent testing showed that the employees continued to allow unauthorized access. FAA demanded that corrective action be taken immediately. As a result,

[15] Test results are as of February 23, 2000.

security guards were posted at doors entering secure areas and access was effectively controlled.

However, OIG and FAA testing alone will not be enough to motivate employees to accept and consistently meet their responsibilities for airport security. Employees must be held accountable for failing to meet their responsibilities for airport security. In June 2000, FAA plans to issue regulations making individuals directly accountable to FAA for noncompliance with access control requirements. This would permit FAA to take enforcement actions against employees. FAA also plans to issue regulations requiring airport operators to have a security compliance program, which describes the disciplinary actions and penalties to be assessed when employees do not comply with security requirements.

STRATEGIC PLAN

FAA has made significant progress in deploying existing advanced security technologies, including 92 FAA-certified CTX 5500 machines equipped with TIP at 35 airports, 553 explosives trace detection devices at 84 U.S. and foreign airports, 18 advanced technology bulk explosives detection x-ray machines at 8 airports, and 38 CBT platforms at 37 airports. FAA will continue the acquisition and deployment of CTX 5500s, explosives trace detection devices, and CBT platforms. In addition, FAA will begin to deploy several other recently-certified bulk explosives detection technologies, including one with a slower throughput intended for small airports and low-traffic stations within larger airports; TIP-ready x-ray machines for screening checkpoints; and Threat Containment Units.[16]

[16] Threat Containment Units are mobile containers that provide a safe and isolated environment to resolve threat items discovered at airports.

FAA has also conducted or sponsored aviation security research, engineering, and development on bulk explosives detection equipment, explosives trace detection equipment, integration of airport security technology, aviation security human factors, and aircraft hardening.

Impressive as the deployment of technologies is, FAA has continued to focus on the acquisition and deployment process, rather than on the necessary transition to integrating all the various assets into a comprehensive, seamless security program.

In 1998 we recommended that, to meet current and future threats to aviation security, FAA develop an integrated strategic plan to guide its efforts and prioritize funding needs. Concentration on deployment (what to buy, when to buy it, and where to put it) is not the complete solution. This plan should include a balanced approach covering basic research, equipment deployment and use, certification and operations testing processes, data collection and analysis on actual equipment and operator performance, and regulation and enforcement. FAA should work with the aviation industry (air carriers, shippers, and airport operators) in developing this integrated security plan.

The strategic plan that we recommended has not yet been developed. In our opinion, this must be done to guide the future $600 million Facilities and Equipment; and Research, Engineering, and Development funding expected in FYs 2001 through 2004.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you might have.