



**U.S. Department of
Transportation**

Office of the Secretary
of Transportation

Office of Inspector General

Memorandum

Subject: ACTION: Report on Audit of Airport Access
Control, Federal Aviation Administration
Report No. AV-2000-017

Date: November 18, 1999

From: Alexis M. Stefani
Assistant Inspector General for Auditing

Reply to
Attn of: JA-1:x61992

To: Federal Aviation Administrator

We are providing this report in response to your October 12, 1999 comments to our September 24, 1999 draft report. An executive summary of the report follows this memorandum.

In your comments to our draft report, you concurred with seven recommendations, promising to implement corrective actions, and partially concurred with two recommendations.

We consider your comments and actions taken or planned responsive to our recommendation that FAA work with airport operators and air carriers to implement and strengthen existing access controls to eliminate access control weaknesses. We also consider your comments and actions taken or planned responsive to our three recommendations addressing FAA's implementation of its oversight program. The recommendations are considered resolved subject to the follow-up provisions of Department of Transportation Order 8100.1C. Your comments and planned actions on our recommendation to improve employee compliance with access control requirements were acceptable, but you did not include an estimated completion date.

However, we consider your comments and actions planned non-responsive to our recommendation to require airport operators and air carriers to develop and implement comprehensive employee training programs. We also consider your comments and actions planned either partially responsive or non-responsive to our three recommendations to strengthen airport access control requirements in secure airport areas to ensure the security of passengers and aircraft.

We request that you reconsider your response and corrective actions for the recommendations to require airport operators and air carriers to develop and implement comprehensive employee training programs, and strengthen airport access control requirements. Please provide written comments in 15 working days to these recommendations and include specific actions taken or planned as well as estimated completion dates. Feel free to propose alternative courses of action to resolve the remaining recommendations in an effective manner. Additionally, please provide target dates for the actions planned to improve employee compliance with access control requirements.

This report is marked sensitive security information in its entirety and is therefore subject to the disclosure restrictions outlined in Title 14 Code of Federal Regulations Part 191.

We appreciate the cooperation and assistance provided by your staff during the audit. If I can answer any questions or be of further assistance, please contact me at x61992, or Robin K. Hunt, Director for Aviation Security and Infrastructure, at (415) 744-0420.

#

EXECUTIVE SUMMARY

Airport Access Control

Federal Aviation Administration

Objective and Scope

The objective of the audit was to assess the Federal Aviation Administration's (FAA) oversight of airport operators' and air carriers' implementation of airport access control requirements. We concentrated our work on FAA's efforts to implement corrective actions planned in response to our 1993 report on airport security.

In 1993, we reported that FAA oversight of airport security systems and programs was not adequate, and that FAA inspection and testing of airport security systems and programs were not aggressive. We concluded that, at the airports reviewed, FAA could not rely on existing security systems and programs for safeguarding aircraft, passengers, and property in secure areas and terminals.

FAA concurred with our finding and agreed to move beyond our recommendations in its corrective actions. FAA stated it was developing rules that would increase individual accountability and improve compliance with access control requirements.

We reviewed FAA's assessments and testing of airport operator and air carrier compliance with airport access control requirements for Fiscal Years (FY) 1997 and 1998. From December 1998 through April 1999, we tested airport operator and air carrier compliance

with access control requirements involving 35 U.S. and foreign air carriers at 8 major airports throughout the nation.

Background

U.S. airport operators, and U.S. and foreign air carriers, are required to implement FAA-approved security programs. The security programs must include procedures to control access to and movement of individuals within the Air Operations Area (AOA), and for prompt detection and action to control each penetration, or attempted penetration, of an

The **AOA** is the area of an airport designated for landing, take-off, or surface maneuvering of aircraft.

EXECUTIVE SUMMARY

AOA by an unauthorized person. In addition, security programs must include a system, method or procedure for controlling access to the secured area¹.

The system, method, or procedure must: (1) ensure only authorized persons gain access to secured areas; (2) immediately deny access to individuals whose authority changes, such as former airline employees; (3) differentiate between persons with unlimited access to the secured area and persons with only partial access; and (4) limit an individual's access by time and date. As of July 1999, over 450 airports and 290 air carriers were subject to the requirement and had FAA-approved security programs.

Results-in-Brief

Airport access control has been, and continues to be, an area of great concern due to increased threat to U.S. airport facilities, aircraft, and most importantly, the flying public. However, FAA has been slow to take actions necessary to strengthen access control requirements and adequately oversee the implementation of existing controls.

We tested access control from December 1998 through April 1999 at eight major U.S. airports and found airport operators and air carriers operating at those airports had not successfully implemented procedures for limiting access to and within secure² airport areas to only authorized persons. Throughout the report we will refer to this as controlling access.

We successfully penetrated secure areas on 117 (68 percent) of 173 attempts from the non-sterile and sterile areas of the airport. The **non-sterile area** is an area to which access is not controlled by the inspection of people and property in accordance with an approved security program, i.e. the area before passenger screening. For example, airport terminal areas that include ticketing and baggage claim are usually non-sterile areas. Once a person passes through passenger screening he/she enters the **sterile area**. Airport concourses that include the gates for aircraft departures and arrivals are sterile areas.

As seen in the following chart, we: piggybacked (followed) employees³ through doors located in non-sterile areas; penetrated other access points in sterile and

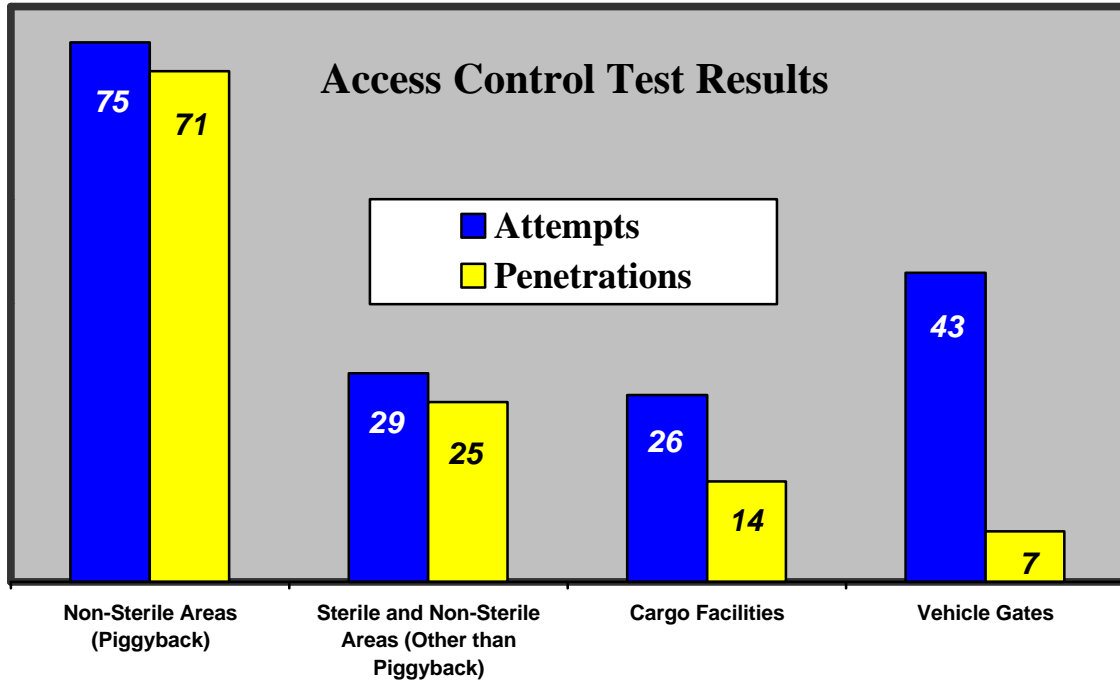
¹ The **secured area** is the portion of an AOA where passengers board and deboard aircraft, and the area surrounding the aircraft. In terms of access control, it must be the most secure area within the AOA.

² OIG uses the term **secure area** (versus secured 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 AOA or may be limited to the smaller, more restrictive, secured area.

³ Employees include all persons authorized for unescorted access to secure airport areas.

EXECUTIVE SUMMARY

non-sterile areas by riding unguarded elevators, and walking through concourse doors, gates and jetbridges⁴; walked through cargo facilities unchallenged; and drove through unmanned vehicle gates.



Once we penetrated secure areas, we boarded aircraft operated by 35 different air carriers 117⁵ times.

⁵ It is a coincidence that the number of penetrations and aircraft boardings both equal 117. Not all penetrations resulted in boarding aircraft, and some penetrations resulted in multiple aircraft boardings.

EXECUTIVE SUMMARY

The access control vulnerabilities we identified were due to:

- airport operators and air carriers not successfully implementing procedures for controlling access,
- employees not meeting their responsibilities for airport security,
- FAA not successfully implementing its oversight program for ensuring compliance with access control requirements, and
- FAA policies that contribute to weaknesses in access control.

On March 10, 1999, we presented the initial results of our audit at a hearing before the Subcommittee on Transportation and Related Agencies, Committee on Appropriations, U.S. House of Representatives⁶. We concluded if airport security systems are to be effective, FAA, airport operators, air carriers, and employees must work together to ensure access control systems function as planned.

Principal Findings

Airport Operators and Air Carriers Had Not Successfully Implemented Procedures for Controlling Access

Airport operators and air carriers are required to have and implement FAA-approved security programs that include procedures for controlling access to the AOA, as well as baggage rooms, aircraft, and other non-public areas. However, at the airports reviewed, airport operators and air carriers had not successfully implemented procedures for controlling access.

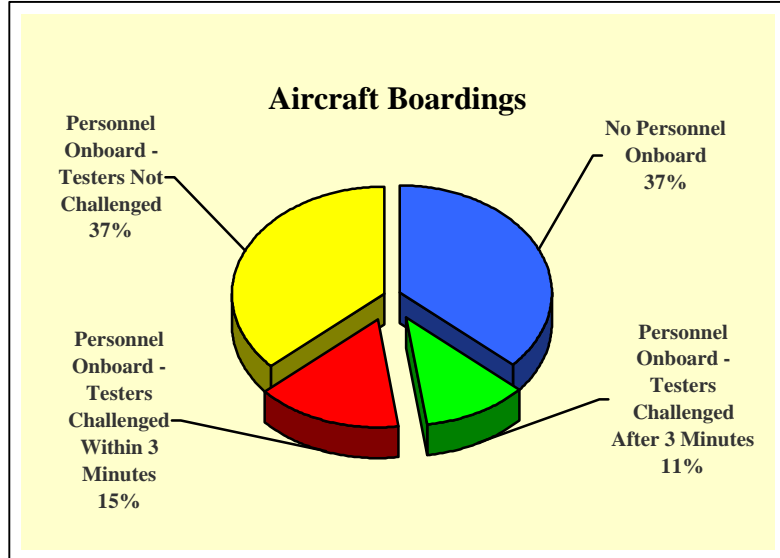
Results of our access control testing demonstrated the need for airport operators and air carriers to implement and strengthen existing controls to eliminate access

⁶ Aviation Security: Federal Aviation Administration (Report Number AV-1999-068, March 10, 1999).

EXECUTIVE SUMMARY

control weaknesses. The chart below shows that for the 117 aircraft boarded as a result of penetrating into secure areas:

- in 43 (37 percent) boardings, no air carrier personnel were onboard to ensure the security of the aircraft as required by security programs;
- in 43 (37 percent) boardings, employees (flight crews, maintenance staff, food service workers, and other vendor personnel) were onboard but did not challenge us as required;
- in 13 (11 percent) boardings, air carrier personnel were present and challenged us inside the aircraft more than 3 minutes⁷ after we boarded; and
- in only 18 (15 percent) boardings, air carrier personnel were present and properly challenged us inside the aircraft within 3 minutes.



In addition, 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.

It is important to note that we did not perform specific tests to board aircraft because we agree with FAA that “there are means to inflict harm to the flying public without gaining access to an aircraft . . .” Rather, to show the effect of penetrating secure areas, we attempted to board aircraft after walking through baggage and other non-public areas. Many times we observed aircraft that we determined to be secure and not boardable, or we were prevented from boarding aircraft because jetbridge or aircraft doors were locked.

Employees Often Did Not Meet Their Responsibilities for Airport Security

At each of the eight airports we reviewed, employees authorized for access in secure areas are responsible for, and a part of, airport access control. Employee responsibilities include requirements to: display identification, challenge others not displaying identification, and prohibit other employees and unauthorized individuals from piggybacking when entering secure areas. We frequently found

⁷ FAA uses 3 minutes as the threshold for determining whether an aircraft was successfully penetrated.

EXECUTIVE SUMMARY

that employees did not meet their responsibilities for airport security, and as a result, they are the primary reason for access control system weaknesses.

The majority of our penetrations (99 of 117) 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 (68 times); (2) challenged us for following them into secure areas (3 times); or (3) taken other steps required to restrict entry into secure areas (28 times), such as control pedestrian access through cargo facilities and vehicle gates.

In addition to our tests to penetrate secure areas, we performed two specific tests to identify weaknesses in employees' compliance with requirements to challenge and properly display identification in the secure area. The results of our tests found that:

- 283 (72 percent) of the 392 employees we encountered in secure areas failed to challenge testers for unauthorized access; and
- 116 (19 percent) of 625 employees we observed in secure areas did not display identification.

We reported the same weaknesses in 1993. In response to our 1993 recommendations, FAA disclosed that new rules to increase individual accountability for airport security were underway. The proposed rule was issued on August 1, 1997, but was not finalized. According to FAA, the final rule is scheduled to be issued March 1, 2000.

During our review, we discussed the need for new individual accountability rules with FAA, airport, air carrier, and industry officials. The majority of those interviewed stated that additional rulemaking is needed. In our opinion, new regulations to correct employee weaknesses are long overdue but cannot be considered the sole solution. FAA, airport operators, air carriers, and employees must carry out their existing responsibilities for access control.

Also, FAA must require airport operators and air carriers to develop and implement comprehensive training programs that teach employees their role in airport security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform. Training must be recurring.

Each of the eight airports reviewed required training for employees seeking authorization to secure airport areas. However, we found the training was not

EXECUTIVE SUMMARY

adequate to inform employees of their access control responsibilities, and it was generally one-time rather than recurring training. For example, only four airport training programs included instruction and testing.

Further, FAA should require airport operators and air carriers to develop and implement programs that foster and reward compliance with access control requirements, and discourage and penalize noncompliance. Just three of eight airports we reviewed had reward programs and seven of eight airports had penalty programs.

In our opinion, most of the programs were poorly implemented based on the few numbers of rewards and penalties given or assessed during 1997 and 1998. For example, 2 of the 3 airports with reward programs issued a combined 58 cash awards in 2 years (less than 15 awards per year per airport). Also, 4 of the 7 penalty programs combined for 164 penalties in 2 years (less than 21 penalties per year per airport). In contrast, we could have assessed substantially more penalties per airport in just 3 days of testing access control at each airport.

FAA Had Not Fully Implemented Its Oversight Program to Ensure Compliance with Airport Access Control Requirements

FAA has not adequately assessed and accurately reported on airport operator and air carrier compliance with access control requirements. We found FAA's airport assessments⁸ of compliance with access control requirements were limited in scope, included little testing, did not use a testing protocol, and failed to identify violations. Also, assessment data maintained in FAA's security database were inaccurate due to data reporting, entry, and administration errors. Further, FAA has not fully implemented its quality control program to ensure the adequacy and accuracy of compliance assessments. We reported similar conditions in 1993.

Airport Annual Assessments for Access Control Were Inadequate. FAA issued guidelines for field agents to follow for assessing whether an airport operator is complying with access control requirements. However, of the 16 annual airport assessments we analyzed for FYs 1997 and 1998 at the 8 airports reviewed, all were limited in scope due to agents not performing all required review steps. For example, there are 11 review areas and required steps to be completed for each assessment; however, in 1997 FAA agents at 1 airport omitted 5 areas and only partially addressed the other 6 areas. The same airport's 1998 assessment was improved; however, some areas were still not sufficiently reviewed to identify

⁸ FAA performs annual security assessments to review airport operators' and air carriers' compliance with all relevant Federal regulations and requirements.

EXECUTIVE SUMMARY

deficiencies. We found a significant deficiency in one of the areas, Lock and Key control, that should have been identified in both the 1997 and 1998 reviews. Additionally, we identified 52 violations in the assessments that were not accurately reported; therefore, FAA did not require any corrective action.

Also, FAA has not provided sufficient guidance to agents for determining how and when to test access controls. As a result, the assessments we reviewed included little, if any, testing. For example, at two airports we reviewed, agents attempted to penetrate the secured area by piggybacking a total of just eight times during the 1997 and 1998 annual assessments, even though the ability for intruders to piggyback is one of the primary access control weaknesses. At the other six airports we reviewed, no piggyback tests were performed during the annual assessments. At one airport we reviewed, the agent who performed the annual assessments for the past 8 years stated she never tried to piggyback because she was easily recognized.

Further, due to the failure to use a standard testing protocol, the access control test results cannot be used (and are not used) to identify systemic problems and allocate FAA resources to remedy the problems.

Security Database Deficiencies Need Correcting. We found that access control data collected in the field and maintained in the Airport/Air Carrier Information Reporting System (AAIRS) were inaccurate due to data reporting, data entry, and data administration errors. We attempted to verify the accuracy of a listing from AAIRS of air carriers that did not have the required annual assessment in FY 1997 and/or FY 1998. We found we could not rely on the AAIRS data. For example, air cargo carriers, and air carriers no longer in business, were incorrectly included in the database, and not all assessments had been recorded.

Better Execution of the Quality Control Program Is Needed. FAA has not fully implemented its quality control program to ensure annual assessments are performed adequately and assessment results are reported accurately in AAIRS. For example, FAA Headquarters staff are required to review at least 10 percent of each Region's annual assessments, and Regional staff must review at least 20 percent of the Region's annual assessments. We found these requirements were not implemented during FYs 1997 and 1998 at FAA Headquarters or at four of the five Regions we visited.

FAA Needs to Strengthen Airport Access Control Requirements

Although employees were the primary access control weakness, FAA policies also contributed to weaknesses in access control. FAA policies permitting airport

EXECUTIVE SUMMARY

operators and air carriers to use lesser controls in sterile areas and [REDACTED] were responsible for 77 of our 117 (66 percent) aircraft boardings.

We understand there is a fine line between security and maintaining a functioning business environment. Airport and air carrier personnel must be able to perform their jobs with limited inconvenience, and the public's safety must always be ensured during emergencies. However, FAA policies weaken security by allowing lesser controls, such as easily [REDACTED] can be used to access secure areas, and [REDACTED] have no required alarm response time from airport security and rely on challenge procedures to contain intruders. [REDACTED]

[REDACTED]. Although in theory this is correct, past and present test results show the serious vulnerability that exists in practice. For example, [REDACTED]

However, boarding aircraft is not our only concern with unlocked jetbridges. During our testing, we entered jetbridges seven times from sterile areas and exited onto the AOA. Also, after concluding many of our tests, we exited the AOA into non-sterile areas by simply pressing a door release button. This vulnerability [REDACTED]

[REDACTED] Therefore, additional precautions must be taken to ensure the security of aircraft and passengers.

EXECUTIVE SUMMARY

Recommendations

We made recommendations to FAA to improve airport access control, including:

- Work with airport operators and air carriers to implement and strengthen existing controls to eliminate access control weaknesses.
- Require airport operators and air carriers to develop and implement comprehensive training programs that teach employees their role in airport security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform. Training must be recurring.
- Require airport operators and air carriers to develop and implement programs that foster and reward compliance with access control requirements, and discourage and penalize noncompliance. FAA should issue national guidelines to implement the programs and standards to measure employee compliance with program requirements. Airport operators and air carriers must enforce individual compliance requirements and FAA must oversee the enforcement.
- Adequately assess and sufficiently test for compliance with access control requirements, accurately report findings, and assess penalties or take other appropriate enforcement actions when noncompliance is found.
- Improve and better administer its security database to ensure it is efficient and reliable, and can be used to identify systemic problems and allocate resources.
- Fully execute its quality control program to ensure annual assessments are performed adequately and assessment results are reported accurately.
- Require airport operators and air carriers to strengthen access control points in sterile areas to ensure the security of passengers and aircraft.

Management Position

FAA concurred with recommendations to: work with airport operators and air carriers to implement and strengthen existing access controls; require airport operators and air carriers to develop and implement comprehensive training programs; adequately assess and sufficiently test for compliance with access control requirements, accurately report findings, and assess penalties or take other appropriate enforcement actions when noncompliance is found; improve and

EXECUTIVE SUMMARY

better administer its security database; fully execute its quality control program; and strengthen existing access controls. FAA partially concurred with the recommendation to require airport operators and air carriers to develop and implement programs that foster and reward compliance with access control requirements.

FAA stated that it has reminded airports, air carriers, and airport security consortia of the criticality of maintaining sound access control practices. FAA indicated that a majority of the nation's major airports initiated new procedures to prevent unauthorized access to secured areas. FAA also indicated that recurrent security training for employees would be advantageous and will provide incentives to industry to conduct such training on a voluntary basis. FAA will also explore the feasibility of mandating recurrent training.

FAA stated it will continue to monitor access control as part of its regular, comprehensive, airport security assessments on a permanent basis. FAA also stated that both testing access controls, and requiring that security database entries be made accurately and promptly will be a part of its FY 2000 Work Plan. FAA regional managers and Headquarters divisions will conduct audits to ensure proper documentation of inspection data. FAA indicated that an extensive effort has been executed to ensure its entire security workforce understands the policies and requirements of FAA's compliance and enforcement program.

FAA also stated that several software adjustments were made to AAIRS in the past few months and several more enhancements are planned. By mid-2000, FAA expects to have an entirely new Web-based system to address the deficiencies we reported and improve the efficiency and use of inspection data.

FAA believes there are basic improvements that can be applied to improve access control, such as [REDACTED]. However, FAA maintains that, under current regulations, the use of lesser controls in combination with passenger screening checkpoints provides an equivalent level of security to that obtained by processing through automated access systems. Modification of this practice would require revisions to the regulation, something that FAA stated it would consider.

FAA concurred with the intent of the recommendation to require airport operators and air carriers to develop and implement programs that foster and reward compliance with access control requirements, and discourage and penalize noncompliance. However, FAA stated two separate rulemaking actions to hold individuals accountable for compliance with access control requirements are pending and the outcome cannot be predetermined. Meanwhile, FAA will continue to encourage airports and air carriers to voluntarily implement programs

EXECUTIVE SUMMARY

for educating employees and holding them individually accountable for not complying with access control requirements.

Office of Inspector General Comments

The actions FAA has taken or planned are responsive to recommendations to work with airport operators and air carriers to implement and strengthen existing access controls, and fully implement FAA's oversight program. The planned actions to improve employee compliance with access control requirements were acceptable; however, FAA needs to provide target dates for the final rulemaking.

FAA's planned actions to require airport operators and air carriers to develop and implement comprehensive employee training programs were non-responsive. Although FAA concurred with the recommendation to require airport operators and air carriers to develop and implement comprehensive training programs, its proposed corrective action does not meet the intent of the recommendation. We agree that FAA regulations require training for each person granted access to secure airport areas. However, as we discussed, the training was inadequate because it did not sufficiently teach employees what their role in airport security is, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform their responsibilities. FAA needs to provide a specific plan of action to improve employee training, including an estimated date of completion.

The actions FAA has taken or planned are either partially responsive or non-responsive to our recommendations to strengthen airport access control requirements. FAA concurred with the recommendation to require airport operators and air carriers to strengthen access control points in sterile areas to ensure the security of passengers and aircraft. However, FAA's response does not meet the intent of the recommendation because (1) the current use of lesser controls in combination with passenger screening is not sufficient to meet access control system regulations, and (2) strengthening these controls does not require rulemaking. Therefore, FAA should reconsider its position to ensure lesser controls are strengthened.

In 2001, we plan to perform a follow-up review to determine whether the corrective actions taken in response to the recommendations resulted in improved airport access control.

TABLE OF CONTENTS

TRANSMITTAL MEMORANDUM

EXECUTIVE SUMMARY

I. INTRODUCTION

Background1
Objective, Scope and Methodology3

II. PROGRAM STATUS4

III. FINDINGS AND RECOMMENDATIONS

Finding A: Airport Operators and Air Carriers Had Not
Successfully Implemented Procedures for
Controlling Access7
Finding B: Employees Often Did Not Meet Their
Responsibilities for Airport Security 12
Finding C: FAA Had Not Fully Implemented Its Oversight
Program to Ensure Compliance with Airport Access
Control Requirements..... 17
Finding D: FAA Needs to Strengthen Airport Access Control
Requirements25

IV. EXHIBITS



Exhibit B: Major Contributors to This Audit

V. APPENDIX

Appendix: FAA Response to Draft Report

I. INTRODUCTION

Background

U.S. airport operators, and U.S. and foreign air carriers, are required to implement FAA-approved security programs. The security programs must include procedures to control access to and movement of individuals within the Air Operations Area (AOA), and for prompt detection and action to control each penetration, or attempted penetration, of an AOA by an unauthorized person. In addition, security programs must include a system, method, or procedure for controlling access to the secured area.

The system, method, or procedure must: (1) ensure only authorized persons gain access to secured areas, (2) immediately deny access to individuals whose authority changes, (3) differentiate between persons with unlimited

The **AOA** is the area of an airport designated for landing, take-off, or surface maneuvering of aircraft.

The **secured area** is the portion of an AOA where passengers board and deboard aircraft, and the area surrounding the aircraft. In terms of access control, it must be the most secure area within the AOA.

access to the secured area and persons with only partial access, and (4) limit an individual's access by time and date.

As of July 1999, over 450 airports and 290 air carriers were subject to the requirements and had FAA-approved security programs. According to FAA, these requirements are intended to prevent individuals, such as former airline employees, from using forged, stolen, or noncurrent identification (ID) or their familiarity with airport procedures to gain unauthorized access to secured areas.

ID is any form of recognition issued or approved by an airport operator who provides a person unescorted access to secured/restricted areas of an airport as designated in an FAA-approved security program.

For Fiscal Years (FY) 1998 and 1999, Congress appropriated \$8.7 million and \$9.0 million, respectively, for airport security research and development, including human factors studies and access control technologies. The planned appropriation for FY 2000 is \$9.2 million.

Objective, Scope and Methodology

We assessed FAA's oversight of airport operators' and air carriers' implementation of airport access control requirements. To assess FAA's oversight of the implementation of airport access control requirements, we concentrated our work on FAA's controls for ensuring compliance with established requirements, and airport operators' and air carriers' compliance with access control requirements. We also reviewed new technologies used by airport operators and air carriers to eliminate unauthorized access to secure airport areas.

To assess FAA's controls for ensuring compliance with established requirements, we analyzed FAA's compliance reviews for eight major U.S. airports to determine the adequacy of the reviews and quality of the data reported in the Airport/Air Carrier Information Reporting System (AAIRS).

To assess airport operators' and air carriers' compliance with requirements for controlling access, we independently tested the day-to-day access control operations of airports and air carriers at the eight airports. We developed a testing protocol and performed tests to determine the following: (1) ability of unauthorized individuals to penetrate secure areas, (2) number of individuals

The Office of Inspector General uses the term **secure area** (versus secured area) to define the area of an airport where each person is required to continuously display airport-approved identification. Each airport defines this area, which may be the entire AOA or may be limited to the smaller, more restrictive, secured area.

not displaying ID, (3) number of individuals who did not challenge others for not displaying ID, (4) airport law enforcement response to emergency door alarms, and (5) ability of unauthorized individuals to

bypass passenger screening checkpoints. We also met with industry associations to discuss issues that affect airport access control.

We performed the audit in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. The audit included such tests of procedures and records as were considered necessary in the circumstances.

The audit was performed during the period October 1998 through May 1999, and covered the period October 1997 through May 1999. The audit was performed at the FAA offices and airports listed in Exhibit A.

II. PROGRAM STATUS

In the 1990's, the OIG has reported on various aspects of aviation security, including airport access control. Also, in the 1990's, Presidential Commissions have been appointed to review and report on critical aviation issues, including security. In response to the OIG and Commission recommendations to improve aviation security, FAA has proposed rules to address security weaknesses. Also, as part of its Strategic Plan, FAA has as one of its goals "to eliminate security incidents in the aviation system."

FAA Oversight of Airport Security Systems and Programs Was Not Adequate

In 1993, we reported¹ that FAA oversight of airport security systems and programs was not adequate. We entered secure areas by following airport personnel through access control points, [REDACTED] [REDACTED]. For each penetration, employees² failed to comply with established airport policies and procedures, and permitted us to go unchallenged into secure areas.

We also found that FAA inspection and testing of airport security systems and programs were not aggressive. As a result, we concluded that, at the airports reviewed, FAA could not rely on existing security systems and programs for safeguarding aircraft, passengers, and property in secure areas and terminals.

FAA concurred with our finding and agreed to move beyond our recommendations in its corrective actions. FAA stated rules were being developed that would increase individual accountability and improve compliance with access control requirements.

Deficiencies Continued in 1995

To follow up on the 1993 audit and determine if corrective actions were taken, the OIG's FY 1995 Audit Plan included an audit of the effectiveness of FAA's Airport Security Program. However, on June 7, 1995, the Inspector General and the FAA Administrator agreed that a follow-up audit would only demonstrate that airports continue to exhibit serious deficiencies in access control procedures. Instead of performing the audit, we agreed to

¹ Audit of Airport Security (Report Number R9-FA-3-105, September 20, 1993).

² Employees include all persons authorized for unescorted access to secure airport areas.

participate in FAA's testing of airport and air carrier security requirements at a number of critical airports.

White House Commission on Aviation Safety and Security

The July 1996 crash of TWA Flight 800 was the catalyst for important advances in aviation security. Although the Federal Bureau of Investigation 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 (Commission). In its February 12, 1997 final report, the Commission concluded that:

Access to airport controlled areas must be secured and the physical security of aircraft must be ensured. Air carriers and airport authorities, working with FAA, must develop comprehensive and effective means by which to secure aircraft and other controlled areas from unauthorized access and intrusion.

FAA's Notice of Proposed Rulemaking

In response to the Commission's recommendation, FAA issued a Notice of Proposed Rulemaking on August 1, 1997, to provide a comprehensive update to Title 14, Code of Federal Regulations, Parts 107 and 108. The proposed revision would strengthen access controls by: (1) establishing individual accountability for complying with security procedures, (2) more clearly defining secure airport areas, (3) modifying escort procedures for individuals without access authority, (4) expanding the requirement for an identification system to include a challenge system, and (5) strengthening FAA authority to conduct inspections and investigations of compliance with federally-mandated security requirements. FAA had not finalized the revisions as of November 1999.

Government Performance and Results Act

In accordance with the Government Performance and Results Act of 1993, FAA has established safety and security goals, objectives, and outcome-based performance measures. In its FY 1999 Annual Performance Plan, FAA's goal was to increase the percentage of airports in compliance with access control requirements by 10 percent by FY 2000 from a 1998 baseline of 85 percent. FAA determined the rate of compliance by calculating the number of individuals who displayed airport ID and challenged others failing to display airport ID. However, as a result of our

testing that showed the percentage of airports in compliance may be substantially lower than 85 percent, FAA is developing a new baseline and revising its goal.

III. FINDINGS AND RECOMMENDATIONS

Airport access control has been, and continues to be, an area of great concern due to increased threat to U.S. airport facilities, aircraft, and most importantly, the flying public. However, FAA has been slow to take actions necessary to strengthen access control requirements and adequately oversee the implementation of existing controls. We found that airport operators and air carriers have not successfully implemented procedures for controlling access, and employees have not met their responsibilities for airport security. We also found that FAA has not successfully implemented its oversight program to ensure compliance with established airport access control requirements, and FAA policies contributed to weaknesses in access control. As a result, at the eight airports reviewed, the access control security systems and programs to safeguard passengers, aircraft, and airport property did not function as planned.

Finding A: Airport Operators and Air Carriers Had Not Successfully Implemented Procedures for Controlling Access

Airport operators and air carriers are required to have and implement FAA-approved security programs that include procedures for controlling access to the AOA, including baggage rooms, aircraft, and other non-public areas. However, at the airports reviewed, airport operators and air carriers had not successfully implemented procedures for controlling access.

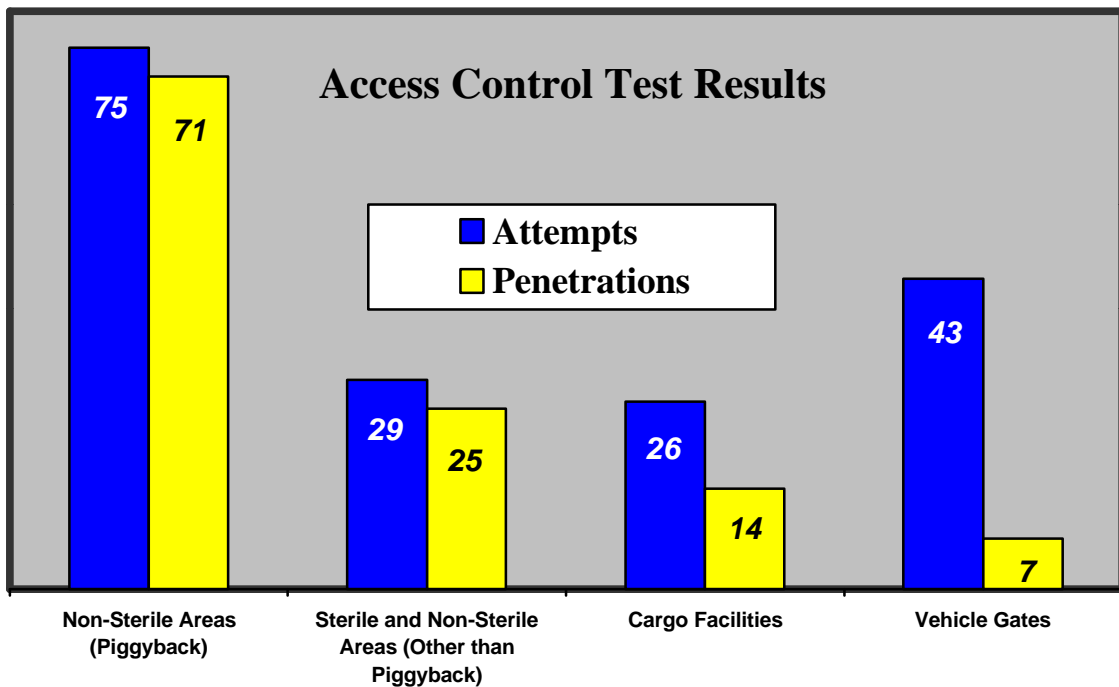
Secure Airport Areas Are Highly Vulnerable to Unauthorized Access

To review airport access control, we developed a testing protocol and performed tests to determine the following: (1) ability of unauthorized individuals to penetrate secure areas, (2) number of individuals who did not challenge others for not displaying ID, (3) number of individuals who did not display ID, (4) airport law enforcement response to emergency door alarms, and (5) ability of unauthorized individuals to bypass passenger screening checkpoints.

We tested access control from December 1998 through April 1999 at 8 major U.S. airports and successfully penetrated secure areas on 117 (68 percent) of 173 attempts from the non-sterile and sterile areas of the airport. The **non-sterile area** is an area to which access is not controlled by the inspection of people and property in accordance with an approved security program, i.e. the area before passenger screening. For example, airport terminal areas that

include ticketing and baggage claim are usually non-sterile areas. Once a person passes through passenger screening, he/she enters the **sterile area**. Airport concourses that include the gates for aircraft departures and arrivals are sterile areas.

As seen in the following chart: we piggybacked (followed) employees through doors located in non-sterile areas; penetrated other access points in sterile and non-sterile areas by [REDACTED], and walking through concourse doors, gates and jetbridges³; walked through cargo facilities unchallenged; and drove through unmanned vehicle gates.



Once we penetrated secure areas, we boarded aircraft operated by 35 different air carriers 117⁴ times.

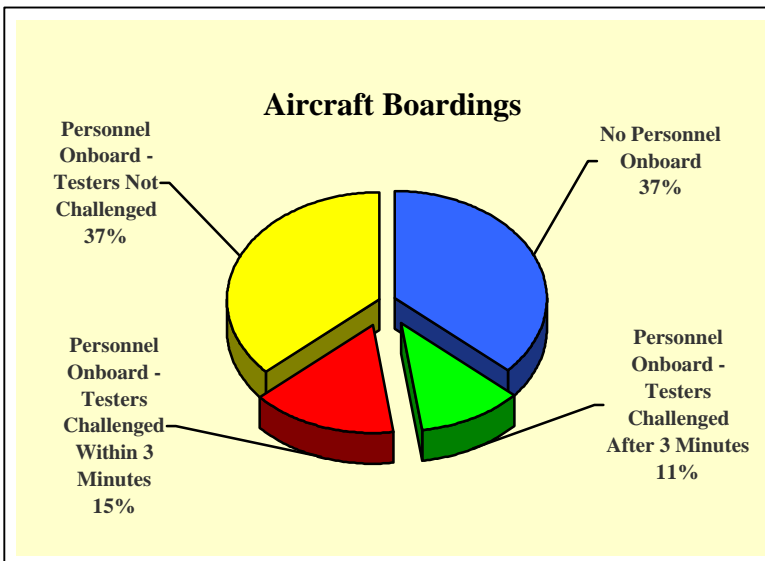
³ A jetbridge provides access from the concourse gate and AOA to the aircraft. In most cases, there is at least one door in the jetbridge that leads directly to the secured area.

⁴ It is a coincidence that the number of penetrations and aircraft boardings both equal 117. Not all penetrations resulted in boarding aircraft, and some penetrations resulted in multiple aircraft boardings.

The chart below shows that for the 117 aircraft boarded as a result of penetrating into secure areas:

- in 43 (37 percent) boardings, no air carrier personnel were onboard to ensure the security of the aircraft as required by security programs;

- in 43 (37 percent) boardings, employees (flight crews, maintenance staff, food service workers, and other vendor personnel) were onboard but did not challenge us as required;



- in 13 (11 percent) boardings, air carrier personnel were present and challenged us inside the aircraft more than 3 minutes⁵ after we boarded; and

- in only 18 (15 percent) boardings, air carrier personnel were present and properly challenged us inside the aircraft within 3 minutes.

In addition, 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.

It is important to note that we did not perform specific tests to board aircraft because we agree with FAA that “there are means to inflict harm to the flying public without gaining access to an aircraft” Rather, to show the effect of penetrating secure areas, we attempted to board aircraft after walking through baggage and other non-public areas. Many times we observed aircraft that we determined to be secure and not boardable, or we were prevented from boarding aircraft because jetbridge or aircraft doors were locked.

We also found poor control of keys used to access secure areas at five of the eight airports reviewed. For example, 1 airport issued 750 keys to doors accessing the secured area. FAA requires 100 percent accountability for such keys. However, airport officials could not account for 100 (13 percent) of the 750 keys. One of the missing keys was a [REDACTED] [REDACTED] During FY 1997, the FAA Civil Aviation Security Field Office

⁵ FAA uses 3 minutes as the threshold for determining whether an aircraft was successfully penetrated.

omitted reviewing key control during the airport's annual assessment. In FY 998, key control was reviewed but no problems were reported.

Based on our results, we concluded that airport operators and air carriers have not successfully implemented procedures for controlling access. FAA needs to work with airport operators and air carriers to implement and strengthen existing controls to eliminate weaknesses in access control.

Recommendation

We recommend that FAA work with airport operators and air carriers to implement and strengthen existing controls to eliminate access control weaknesses. One suggestion would be to review access control points to determine if they can be closed to all traffic or if improvements can be made at specific access locations, such as increased lighting to identify intruders, shortened door closing time, and increased distance between public areas and access control points.

Management Position

FAA, in its response of October 12, 1999, concurred with the recommendation and stated that airports, air carriers, and airport security consortia were reminded by FAA of the criticality of maintaining sound access control practices. FAA also stated that a majority of the nation's major airports initiated new procedures to prevent uncontrolled access to secured areas, such as positioning security guards at access control points as an additional means of ensuring only authorized access to secured areas. Further, FAA stated it will continue to monitor access control as part of its regular, comprehensive assessments of airport security, and will conduct compliance testing.

In its additional comments to this finding, FAA stated that it conducted over 3,000 access control tests at 79 airports just a few weeks after our testing and

Office of Inspector General Comments

The actions FAA has taken and planned are responsive to this recommendation and, if properly executed, should improve airport and air carrier compliance with access control requirements. However, with respect to FAA's additional comments to this finding, FAA's comparison of its test results of 96 percent compliance rate with our 32 percent compliance rate is misleading for two reasons:

- There is no common basis for comparison. FAA’s criterion for testing was the ability to *gain access to an aircraft and remain onboard for* [REDACTED]. In 96 percent of FAA’s tests, agents were not able to meet that criterion. Our criterion for testing was the ability to *penetrate a secure area through any access point*. In 32 percent of our tests, we were not able to penetrate a secure area. Because FAA did not account for the total number of times its agents penetrated secured areas, no comparison between tests can be made.

FAA has stated, and we agree, that “there are means to inflict harm to the flying public without gaining access to an aircraft” This is especially true if unauthorized access is gained to an air carrier checked baggage make-up area, where an explosive device could be inserted into passengers’ checked baggage.

- FAA does not account for the percentage of time its agents were onboard an aircraft for [REDACTED]. In our opinion, [REDACTED] has no validity because there are means to inflict harm to the flying public while onboard an aircraft for less [REDACTED]. This was evident during our testing. On many occasions, we boarded an aircraft, walked the length of the aircraft and back, exited and boarded another aircraft all [REDACTED], we could have easily sabotaged the aircraft boarded.

In 2001, we plan to perform a follow-up review to determine whether the corrective actions taken resulted in improved airport access control.

Finding B: Employees Often Did Not Meet Their Responsibilities for Airport Security

At each of the eight airports we reviewed, employees authorized for access in secure areas are responsible for, and a part of, airport access control.

[REDACTED]

[REDACTED] tests, 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 control pedestrian access through cargo facilities and vehicle gates. As a result, employees are the primary reason for access control system weaknesses. Therefore, access control systems that include a combination of technology and a human element can only be effective with adequate employee training and enforcement, and can only be cost effective if employees assume their responsibility for airport security.

Employees Must Assume Their Responsibility for Airport Security

FAA's Guidance for FAR 107.14 Access Control System, dated May 19, 1995, states the following:

A critical element of an access control system is the procedure to make employees aware of their security responsibilities. Every employee should understand that they must use their issued access media [ID], as required, each time they enter or exit airport secured areas. They must understand their challenge and reporting responsibilities if they observe an individual attempting to circumvent the system

We agree that employees are a vital part of airport security and access control. The majority of our penetrations (99 of 117) into secure areas that resulted in testers boarding aircraft would not have occurred if employees had [REDACTED]

[REDACTED] or (3) taken other steps required to restrict entry into secure areas (28 times), such as control pedestrian access through cargo facilities and vehicle gates.

We performed two specific tests to identify weaknesses in employees' compliance with requirements to challenge and properly display ID in the secure area. The results are as follows:

- 283 (72 percent) of the 392 employees we encountered in secure areas failed to challenge testers for unauthorized access; and
- 116 (19 percent) of 625 employees we observed in secure areas did not display ID.

We reported the same weaknesses in 1993. In response to our recommendations, FAA disclosed that new rules to increase individual accountability for airport security were underway. The proposed rules were issued on August 1, 1997, but were not finalized. According to FAA, the final rule is scheduled to be issued March 1, 2000.

During our review, we discussed the need for new individual accountability rules with FAA, airport, air carrier, and industry officials. The majority of those interviewed stated that additional rulemaking is needed. In our opinion, new regulations to correct employee weaknesses are long overdue but cannot be considered the sole solution. FAA, airport operators, air carriers, and employees must carry out their existing responsibilities for access control.

Training Was Inadequate. Each of the eight airports reviewed required training for employees seeking authorization to secure airport areas. However, we found the training was not adequate to inform employees of their access control responsibilities, and it was generally one-time rather than recurring training.

Only four airport training programs included instruction and testing. The other four airports had programs consisting of playing a video tape(s) and answering questions, but no testing was required. Specifically, one airport offered training by playing videotapes in English only; however, many of those who received the training spoke little or no English. Another airport had a training program that was totally inadequate. It consisted of viewing an outdated, generic airport security tape. No introduction to the tape was given, questions answered, or test given. Finally, just one airport required recurring training for all employees. In our opinion, training must be ongoing to attain and maintain compliance.

FAA must require airport operators and air carriers to develop and implement comprehensive training programs that teach employees their role in airport

security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform. Training must be recurring.

Reward and Penalty Programs Were Deficient. Just three of eight airports we reviewed had reward programs, and seven of eight airports had penalty programs. In our opinion, most of the programs were poorly implemented based on the low numbers of rewards and penalties given/assessed during 1997 and 1998.

For example, 2 of the 3 airports with reward programs issued a combined 58 cash awards in 2 years (less than 15 awards per year per airport). Also, 4 of the 7 penalty programs combined for 164 penalties in 2 years (less than 21 penalties per year per airport). In contrast, we could have assessed substantially more penalties per airport in just 3 days of testing access control at each airport. Two of the eight airports had both a reward and penalty program, but neither airport fully implemented the programs in FY 1997, and only one airport fully implemented both programs in FY 1998.

Airport operators and air carriers must develop and consistently implement programs that foster and reward compliance, and discourage and penalize noncompliance.

Access Control Technologies Were Not Cost Effective. We found that new technologies that relied in part on the human element were not cost effective. For example, after we tested two of the eight airports,

[REDACTED]

At one airport, the air carriers were being charged \$15,000 per week for the services. In effect, the costly access control technology installed was now not necessary.

In our opinion, airport operators and air carriers must make individual accountability for airport security a part of each person's job description. All employees must realize that if they fail to assume their responsibility for security they will not be permitted to work in a secure area. Federal regulations already provide for these responsibilities. However, these regulations are not being enforced.

FAA should issue national guidelines to implement the programs and standards to measure employee compliance with program requirements. Further, airport operators and air carriers must be responsible for enforcing

individual compliance requirements and FAA must be charged with overseeing the enforcement.

Recommendations

We recommend FAA:

1. Require airport operators and air carriers to develop and implement comprehensive training programs that teach employees what their role in airport security is, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform. Training must be recurring.
2. Require airport operators and air carriers to develop and implement programs that foster and reward compliance with access control requirements, and discourage and penalize noncompliance. FAA should issue national guidelines to implement the programs and standards to measure employee compliance with program requirements. Further, airport operators and air carriers must enforce individual compliance requirements, and FAA must oversee the enforcement.

Management Position

FAA, in its response of October 12, 1999, concurred with Recommendation B1 and partially concurred with Recommendation B2. Regarding Recommendation B1, FAA stated that training is already required for persons granted access to secured areas, but agreed that recurrent security training for employees would be advantageous. FAA also agreed to provide incentives to industry to conduct such training on a voluntary basis. FAA would also explore the feasibility of mandating recurrent training.

In response to Recommendation B2, FAA stated that two separate rulemaking actions to hold individuals accountable for compliance with access control requirements are pending and the outcome cannot be predetermined. Meanwhile, FAA will continue to encourage airports and air carriers to voluntarily implement programs for educating employees and holding them individually accountable for not complying with access control requirements.

Office of Inspector General Comments

FAA's response to Recommendation B1 does not address our finding or meet the intent of the recommendation. We agree that FAA regulations require

training for each person granted access to secure airport areas. However, as we discussed, the training was inadequate because it did not sufficiently teach employees what their role in airport security is, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform their responsibilities. FAA needs to provide a specific plan of action to improve employee training, including an estimated date of completion. We request that FAA reconsider its position to require airport operators and air carriers to develop and implement comprehensive training programs.

The actions FAA has taken and planned for Recommendation B2 are responsive to this recommendation and, if properly executed, should improve employee compliance with access control requirements. However, FAA needs to provide target dates for the final rulemakings.

Finding C: FAA Had Not Fully Implemented Its Oversight Program to Ensure Compliance with Airport Access Control Requirements

FAA had not adequately assessed and accurately reported on airport operator and air carrier compliance with access control requirements. We found FAA's airport assessments of compliance with access control requirements were limited in scope, included little testing, did not use a testing protocol, and failed to identify violations. We also found that access control data collected and maintained in FAA's security database (AAIRS) were inaccurate due to data reporting, entry, and administration errors. We further found that FAA had not fully implemented its quality control program to ensure the adequacy and accuracy of compliance assessments. As a result of these deficiencies, AAIRS data do not provide an accurate picture of access control weaknesses. We reported similar conditions in 1993.

FAA Inspections and Tests Were Insufficient to Assess Airport and Air Carrier Compliance with Access Control Requirements

FAA field offices are required to perform annual assessments⁶ for all Category X and I airports⁷. According to FAA:

A Comprehensive (annual) Assessment is a complete review of a regulated party's compliance with all relevant Federal regulations [and] approved security program requirements. . . .

Assessments include 11 areas that FAA agents must review by conducting surveillance, interviewing airport personnel, reviewing documents, and performing tests. When agents discover circumstances that indicate a security concern or issue, they report a finding. Findings are classified as either violations or observations. A violation is when the regulated party failed to perform a requirement of a Federal Aviation Regulation or approved security program.

⁶ FAA performs annual security assessments to review airport operators' and air carriers' compliance with all relevant Federal regulations and requirements.

⁷ 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. [REDACTED]

An observation is a weakness in a system or procedure established to carry out the provisions of a security program, which could lead to a violation of an FAA requirement. Violations require the regulated party to take corrective action. Observations do not require the regulated party to take corrective action.

FAA also performs scheduled Supplemental Assessments throughout the year that are nationally focused reviews of compliance with one or more rules or standards. Additionally, FAA performs unscheduled Supplemental Assessments that are not nationally focused and are conducted only as necessary.

Annual Assessments Were Not Sufficient. We analyzed FYs 1997 and 1998 annual assessments for the eight airports reviewed and found that:

- All 16 assessments were limited in scope, i.e. not all areas were reviewed during the assessments or the areas were not sufficiently reviewed.

For example, in 1997 FAA agents at 1 airport omitted 5 of the 11 required review areas and only partially addressed the other 6 areas. The same airport's 1998 assessment was improved; however, some areas were still not sufficiently reviewed to identify deficiencies. We found a significant deficiency in one of the areas, Lock and Key control, that should have been identified in both the 1997 and 1998 reviews.

- None of the 16 assessments included sufficient testing to validate the airport access control system, and there were no standard testing protocols.

Although FAA's National Assessment Program Guidance specifies testing as a method of conducting assessments, it does not contain standard protocols to specify when or how to test. Further, FAA's agent training manual and the training conducted at FAA's academy in Oklahoma City, Oklahoma, do not include testing.

We found that little, if any, testing was performed during annual assessments. For example, at two airports we reviewed, agents attempted to penetrate the secured area by piggybacking a total of just eight times during the 1997 and 1998 annual assessments, [REDACTED].

At the other six airports we reviewed, no piggyback tests were performed during the annual assessments. At one airport we reviewed, the agent

who performed the annual assessments for the past 8 years stated she never tried to piggyback because she was easily recognized.

Also, when tests were conducted, no standard protocol was used. Therefore, results cannot be used (and are not used) to identify systemic problems and allocate FAA resources to remedy the problems.

- Observations should have been classified as violations. In the 16 annual assessments we reviewed, 31 (39 percent) of the 80 findings reported were classified as observations but should have been classified as violations. As a result of the misclassification, FAA did not require corrective actions. We also identified 21 violations that were included in the report narrative but not listed as findings; therefore, corrective actions were not required.

We interviewed field agents who conducted assessments and found the majority either did not know the correct definitions of a violation and an observation, or incorrectly thought that a violation could not be entered into AAIRS without opening an investigation. Therefore, the agents incorrectly classified violations as observations. As a result, corrective actions were not required and may not have been taken.

We analyzed AAIRS data for FYs 1997 and 1998, and found this problem nationwide. Of the 467 findings for failure to display airport ID or failure to challenge for not displaying ID at Category X and I airports, 244 (52 percent) were incorrectly classified as observations and no corrective action was required.

Supplemental Assessments Not Performed or Not Adequate. No nationally focused assessments of access control were conducted during FYs 1997 and 1998. On April 12, 1999, FAA initiated a national assessment of access control at all Category X and I airports to attempt to emulate our findings. The testing protocol required 40 tests at each airport.

We reviewed FYs 1997 and 1998 unscheduled Supplemental Assessments for the eight airports and found little, if any, testing of access controls. For example, at two airports agents attempted to [REDACTED] No piggyback tests were performed at the other six airports.

Security Database Deficiencies Need Correcting. AAIRS was developed beginning in 1994 to remedy deficiencies in the prior checklist-based data collection system, which FAA determined did not provide decision makers

with enough information about compliance and "...was not an effective tool for either the entry or retrieval of the inspection results." As a result, FAA instituted a "Narrative" inspection format (i.e., document inspection results in narrative fashion). AAIRS was developed to capture the data and was delivered for operational use in June 1995. AAIRS has cost more than \$1.2 million to develop and administer from 1994 through FY 1999.

In our review of AAIRS, we found that access control data collected in the field and maintained in the system were inaccurate due to data reporting, data entry, and data administration errors. For example:

- Data reporting -- as previously discussed, FAA field agents failed to report violations or incorrectly reported violations as observations.
- Data errors -- we requested a listing from AAIRS of air carriers that did not have the required annual assessment in FY 1997 and/or FY 1998. We attempted to verify the accuracy of the listing and found that AAIRS data were not reliable. For example, air cargo carriers, and air carriers no longer in business, were incorrectly included in the database, and not all assessments had been recorded.
- Data administration -- we requested an AAIRS listing of Category X and I airports that did not have an annual assessment in FY 1997 and/or FY 1998. No airports were listed for FY 1997 and seven airports were listed for FY 1998. Of the seven, two were incorrectly listed even though FAA had provided us the assessment reports. According to FAA's Civil Aviation Security, Standards and Evaluations division, the specific problem that resulted in the incorrect listings had previously been reported to the systems administrator, but remained uncorrected.

As a result of AAIRS problems, FAA initiated an evaluation of the system. The resulting report, dated January 8, 1999, identified numerous software deficiencies, data errors, and administrative support problems, as well as poor communications between the system administrator and FAA field offices.

FAA has now concluded that the "Narrative" inspection approach is not working and plans to develop a new Web-based system⁸ by the end of 1999, costing approximately \$325,000. According to FAA's Manager for

⁸ According to an FAA Civil Aviation Security computer specialist, a Web-based system allows for better access to a database that is constantly changing. By integrating with other Web applications, on-line availability of all information within a local environment aids personnel in accessing other critical documents quickly and efficiently. Plus, with the proper setup, a Web-based system becomes more secure.

Information Resource Management, transferring AAIRS data into the new system may not be possible and could result in the loss of archived records.

As stated in the FAA's National Assessment Program Guidance:

AAIRS supports our assessment process by providing a platform for . . . b. a user friendly entry of assessment information and, c. an extremely friendly, dynamic and flexible data retrieval capability, which significantly enhances the ability to analyze compliance in a variety of ways.

According to FAA Headquarters, Regional and field staff, and based on our experience with making simple data requests, AAIRS has failed on both counts.

Better Execution of the Quality Control Program Is Needed. FAA had not fully implemented its quality control program to ensure annual assessments are performed adequately and assessment results are reported accurately in AAIRS. For example, FAA Headquarters staff are required to review at least 10 percent of each Region's annual assessments, and Regional staff must review at least 20 percent of the Region's annual assessments. We found these requirements were not implemented during FYs 1997 and 1998 at FAA Headquarters or at four of the five Regions we visited.

At the field office level, a supervisor is required to approve each assessment before entering the data into AAIRS. However, AAIRS does not allow for remote approval. Therefore, reports prepared by agents with supervisors at different office locations did not have a supervisor listed in AAIRS as the approving official. The supervisor is still required to review the assessment before entering the data into AAIRS. However, we found that review sometimes did not occur and reports were instead approved by a member of the assessment team. We also noted that, even in offices where supervisors were available, some reports were inappropriately approved by an assessment team member.

To determine the extent of the problem, we requested a listing from AAIRS of all FY 1997 and 1998 annual airport and air carrier assessments approved by a member of the assessment team. We found 951 assessments were approved by an assessment team member. We understand that a supervisor at a remote location may have appropriately reviewed some of the assessments before the team member entered the report in AAIRS. However, the FAA Director, Office of Civil Aviation Security Operations, also

addressed this issue in a memorandum to the Regions dated February 5, 1999 (approximately one month after our data request) and wrote the following:

I would like to take this opportunity to ask that you again stress the importance of a thorough supervisory review and approval of all assessments. Even though supervisory review and approval of assessments has been a requirement since . . . 1996, our recent review of assessment approvals for FYs 1997 and 1998 revealed a staggering 4,941 airport, air carrier, screening location and screener evaluation assessments which had a participating agent also approving the assessment. Even after eliminating assessments approved by formerly assigned managers, supervisors, and team leaders, as well as the posts of duty and Civil Aviation Security Units without an assigned supervisor, significant questions were still raised about overall assessment quality control.

We agree with the Director's statement that questions were still raised about overall assessment quality control. Based on the deficiencies we identified in the performance of assessments, data accuracy and quality control, we concluded that AAIRS data do not provide an accurate picture of access control weaknesses. Also, due to the failure to use a standard testing protocol, the data cannot be used (and are not used) to identify systemic problems and allocate FAA resources.

FAA must adequately assess and sufficiently test for compliance with access control requirements, accurately report findings, and assess penalties, or take other appropriate enforcement actions, when noncompliance is found. Also, FAA needs to improve and better administer its security database to ensure it is efficient, is reliable, and can be used to identify systemic problems. Further, FAA must allocate resources and fully execute its quality control program to ensure annual assessments are performed adequately and assessment results are reported accurately. We made similar recommendations in 1993.

Recommendations

We recommend FAA:

1. Adequately assess and sufficiently test for compliance with access control requirements, accurately report findings, and assess penalties, or take other appropriate enforcement actions, when noncompliance is found.

2. Improve and better administer its security database to ensure it is efficient and reliable, and can be used to identify systemic problems and allocate resources.
3. Fully execute its quality control program to ensure annual assessments are performed adequately and assessment results are reported accurately.

Management Position

FAA concurred with Recommendations C1, C2, and C3. Regarding Recommendation C1, FAA stated that testing of access control will be a part of its FY 2000 Work Plan, which also requires security database entries be made accurately and promptly. Also, FAA regional managers and Headquarters divisions will conduct audits to ensure proper documentation of inspection data. Further, FAA trained 748 security personnel to ensure they understand the requirements of its Compliance and Enforcement Program.

In response to Recommendation C2, FAA stated that several software adjustments were made to AAIRS in the past few months and several more enhancements are planned. Also, by mid-2000, FAA expects to have an entirely new Web-based system to address the deficiencies we reported and improve the efficiency and use of inspection data.

For Recommendation C3, FAA stated its FY 2000 Work Plan requires regional managers and Headquarters program divisions to conduct quality control audits to ensure that AAIRS data is accurate, timely, updated and transmitted as required.

Office of Inspector General Comments

The actions FAA has taken and planned are responsive to Recommendations C1, C2, and C3 and, if properly executed, should improve FAA's oversight of airport operators' and air carriers' compliance with access control requirements.

Finding D: FAA Needs to Strengthen Airport Access Control Requirements

Although employees were the primary access control weakness, FAA policies also contributed to security weaknesses. FAA policies permitting airport operators and air carriers to use lesser controls in sterile areas and to [REDACTED] were responsible for 77 of our 117 (66 percent) aircraft boardings.

We understand there is a fine line between security and maintaining a functioning business environment. Airport and air carrier personnel must be able to perform their jobs with limited inconvenience and the public's safety must always be ensured during emergencies. However, FAA policies weaken security by allowing lesser controls, such as easily observed cipher locks on doors in sterile areas that can be used to access secure areas, and unlocked emergency exits that have no required alarm response time from airport security and rely on challenge procedures to contain intruders. We tested airport security's response to emergency exit alarms in sterile areas. For 10 (40 percent) of 25 tests, airport security failed to respond to the alarms.

FAA permits the use of lesser controls in sterile areas because individuals without airport ID have passed through passenger screening and are deemed to pose less risk. We acknowledge that progress has been made in civil aviation security with the continued deployment of new technologies that detect explosives at passenger screening checkpoints. However, based on our access control testing, we conclude that the additional layer of security that passenger screening provides, in combination with lesser controls, is not sufficient to meet access control system requirements. Therefore, the lesser controls must be strengthened (this need not impede airport and air carrier business).

For example, FAA can require controls be strengthened by:

- installing covers over cipher locks so that code numbers cannot be observed when being used,

[REDACTED]

- installing cameras outside emergency exits to record and identify intruders, and

[REDACTED]

However, boarding aircraft is not our only concern with unlocked jetbridges.

[REDACTED]

In our opinion, changes are needed in FAA policy to strengthen access control in sterile areas. Also, FAA must require airport operators and air carriers, to the extent possible, to plan and design new airport construction and reconstruction so that access control points in sterile areas allow employees to perform their jobs and meet access control system requirements, without relying on additional layers of security. Further,

[REDACTED]

Recommendations

We recommend FAA:

1. Change its policy to strengthen access control points in sterile areas, including requiring a swift response to emergency exit door alarms to contain unauthorized access.
2. Issue policy to require airport operators and air carriers, to the extent possible, to plan and design new airport construction and reconstruction so that access control points in sterile areas permit employees to perform their jobs and meet access control system requirements, without relying on additional layers of security.
3. Issue policy to require that unattended jetbridge doors leading to and from the AOA be locked.

Management Position

FAA concurred with Recommendations D1, D2, and D3. Regarding Recommendation D1, FAA stated that airports [REDACTED]

[REDACTED] FAA also believes there are basic improvements that can be applied to improve access control, such as shrouded combination locks; and that this type of improvement may be implemented with minor dislocation of systems and equipment. However, FAA maintains that, under current regulations, the use of lesser controls in combination with passenger screening checkpoints provides an equivalent level of security to that obtained by processing through automated access systems. Modification of this practice would require revisions to the regulation, something that FAA stated it would consider.

In response to Recommendation D2, FAA stated that implementing the recommendation will require accommodation between airport security and the need to provide relatively free access to aviation employees. FAA further stated it would require the cooperation of industry and Government, and significant redesign of airports.

For Recommendation D3, FAA stated that, effective June 1999, the Air Carrier Standard Security Program (ACSSP) requires [REDACTED]

Office of Inspector General Comments

FAA was non-responsive to Recommendation D1. FAA provided no plan of action to address the serious deficiencies we identified in the use of alternative access control systems. Although FAA requires [REDACTED]

[REDACTED] Also, FAA stated it would consider issuing a new ruling to modify the use of lesser controls in combination with passenger screening. However, the regulation, 14 CFR 107.14, Access Control System, only specifies that an alternative access control system that provides an overall level of security equal to that of an access control system can be approved by the Director of Aviation. It is FAA Policy ACP-100-95-001 that explains an alternative access control system can include the screening checkpoint in conjunction with lesser controls such as [REDACTED]. Consequently, rulemaking would not be required to strengthen access control points in sterile areas.

Based on our audit results, the use of lesser controls in combination with passenger screening does not meet 14 CFR 107.14 requirements. Therefore, the lesser controls must be strengthened. Otherwise, requiring stronger and more expensive controls in non-sterile areas cannot be justified. FAA needs to specify a responsive planned action for Recommendation D1 and include estimated completion dates.

FAA was non-responsive to Recommendation D2. In our opinion, this recommendation was forward-looking by requiring airport operators and air carriers to plan and design new airport construction and reconstruction so that access control points in sterile areas meet access control system requirements. FAA should reconsider its position on this recommendation.

FAA was partially responsive to Recommendation D3. In June 1999, FAA amended the ACSSP to require [REDACTED]

[REDACTED] The amendment does not require [REDACTED]. Therefore, it does not address the ability of unauthorized personnel to board aircraft with employees onboard (attended) through [REDACTED] (63 percent of our total boardings). The amendment also does not address the ability of unauthorized personnel to penetrate from sterile areas into secure areas through [REDACTED]

LOCATIONS VISITED

FAA Offices of Civil Aviation Security
Operations, and Policy and Planning

Washington, D.C.

FAA Aviation Security Research and
Development Division

Atlantic City, New Jersey

FAA Office of Civil Aviation Security Regional Offices

Eastern

Jamaica, New York

Great Lakes

Des Plaines, Illinois

Northwest Mountain

Renton, Washington

Southern

College Park, Georgia

Western-Pacific

Hawthorne, California

FAA Civil Aviation Security Field Offices and Units

Burlingame, California

Chicago, Illinois

Miami, Florida

Jamaica, New York

Atlanta, Georgia

Salt Lake City, Utah

Honolulu, Hawaii

Washington, D.C.

[REDACTED]

[REDACTED]

[REDACTED]

MAJOR CONTRIBUTORS TO THIS AUDIT

The following staff members were major contributors to this audit:

| | |
|----------------------|-------------------|
| Robin K. Hunt | Director |
| A. Robert Lund | Auditor-in-Charge |
| Gary Kirk | Auditor |
| Judy W. Nadel | Auditor |
| Gerald L. Blumenthal | Auditor |
| Paul Nagulko | Auditor |
| Scott C. Seaborn | Evaluator |
| James K. Wahleithner | Evaluator |



U.S. Department
of Transportation
**Federal Aviation
Administration**

Memorandum

Subject: **INFORMATION:** Draft Report on the Audit of
Airport Access Control

Date: 001 12 1999

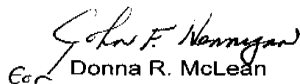
From: Assistant Administrator for Financial Services

Reply to
Attn. of:

To: Assistant Inspector General for Auditing

As requested in your September 24 memorandum, we have reviewed the subject report and offer the attached response.

Should you have any questions, please contact Mr. Anthony R. Williams, Management Programs Division, APF-200. Mr. Williams can be reached on 267-9000.


Donna R. McLean

Attachment

Federal Aviation Administration's (FAA) Response to the
Office Of Inspector General's (OIG) Draft Report on

Audit of Airport Access Control

OIG Recommendation A: FAA is to work with airport operators and air carriers to implement and strengthen existing controls to eliminate access control weaknesses.

FAA Response: Concur. Beginning in early 1999, FAA reminded airports, air carriers, and airport security consortia of the criticality of maintaining sound access control practices. Consortia meetings were convened and airport operators, in a majority of the Nation's major airports, initiated new procedures to prevent uncontrolled access to secured areas. Many airports installed additional access [REDACTED] established practices.

A major Special Emphasis Assessment (SEA) was conducted nationwide during the period March through May 1999, as described above to follow up on the OIG audit results and determine the effectiveness of the new measures and increased industry vigilance.

FAA will continue monitoring access control on an airport by airport basis as a part of regular, comprehensive, airport security assessments on a permanent basis. Beyond that, FAA will ensure through its operational work plan that nationwide access control assessments will be incorporated into its field program. The next SEA will take place during fiscal year (FY) 2000 and similar efforts will be made periodically in future years. Through this ongoing process, FAA will ensure that the level of compliance remains high.

OIG Recommendation B1: FAA require airport operators and air carriers to develop and implement comprehensive training programs to teach employees their role in airport security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform. Training must be recurring.

FAA Response: Concur. FAA already requires training to be delivered to each person who is granted unescorted access to the Security Identification Display Area (SIDA). We agree that recurrent training for employees would be advantageous and will provide incentives to industry to conduct such training on a voluntary basis and simultaneously explore the feasibility of mandating recurring training.

OIG Recommendation B2: FAA require airport operators and air carriers to develop and implement programs that foster and reward compliance with access control requirements and discourage and penalize non-compliance. FAA should issue national guidelines to implement the programs and standards to measure employee compliance with program requirements. Airport operators and air carriers must enforce individual compliance requirements and FAA must oversee the enforcement.

FAA Response: Partially Concur. While FAA generally supports this recommendation, the matter is subject to rulemaking described below; the outcome of which cannot be predetermined at this time. However, in the interim, FAA will seek opportunities to encourage industry to voluntarily adopt individual accountability and reward programs on a local basis.

Two separate, pending, rulemaking actions involve strengthening programs to hold individuals directly accountable for compliance with access control requirements. We are finalizing regulations to make individuals accountable to the FAA for violating access controls. FAA is pursuing further regulatory action to establish airport and air carrier individual accountability compliance programs. The FAA has already gathered public comment on the proposal. In addition, the FAA continues to encourage airports and air carriers to voluntarily implement programs for educating employees and holding them individually accountable through progressive discipline for violations.

OIG Recommendation C1: FAA adequately assess and sufficiently test for compliance with access control requirements, accurately report findings, and assess penalties or take other appropriate enforcement actions, when non-compliance is found.

FAA Response: Concur. The Office of Civil Aviation Security Operations Fiscal Year 2000 Work Plan was issued on September 1. This plan specifically requires that all comprehensive assessments at Category X-II airports, and when practical at Category III airports, include the use of testing protocols and assessment methods that have been adopted in the previous SEA. This includes the protocol developed for access control. Additionally, each CAT X-III airport will also have a supplemental assessment conducted on any problem area(s) identified during the FY 2000 comprehensive assessment. Also, as indicated above, an unannounced access control SEA will also be conducted on a systemwide basis during FY 2000 to determine if industry is maintaining effective access control.

The Work Plan also specifically requires that the security data base entries be made accurately and promptly. Additionally, both regional Civil Aviation Security (ACS) division managers and the Washington headquarters program

divisions will conduct audits to ensure proper documentation of all specifics related to the completed assessments.

A very extensive effort has been undertaken to ensure that the entire workforce understands the requirements of FAA Order 2150.3A, Compliance and Enforcement (C&E) Program and other security enforcement policies. Seven hundred and forty-eight FAA security personnel have been given enhanced and uniformly consistent training in C&E.

OIG Recommendation C2: FAA improve and better administer its security database to ensure that it is efficient and reliable, and can be used to identify systemic problems and allocate resources.

FAA Response: Concur. Several software adjustments have been made to the Airport/Air Carrier Information Reporting System (AAIRS) security data system these past few months to improve efficiency and reliability. This includes numerous application changes and enhanced report writing capabilities. We are also adding features that will identify potential data problems before entry throughout the system. In the near future, we will be including several more enhancements to further lessen the potential for data discrepancies.

OIG Recommendation C3: FAA fully execute its quality control program to ensure annual assessments are performed adequately and assessment results are reported accurately.

FAA Response: Concur. As reported above, the FY 2000 Work Plan specifically requires that entries into AAIRS data base are accurate, timely, updated, and transmitted as required. ACS regional managers and Washington headquarters program divisions will conduct quality control audits.

OIG Recommendation D1: [REDACTED]

FAA Response: [REDACTED]

[REDACTED]

The FAA believes that there are basic improvements that can be applied to the access control systems such as shrouded combination locks, and random or scrambled keypad access devices. These may be implemented with a relatively minor dislocation of systems and equipment.

Improvement in the detection of weapons and explosives at checkpoints has occurred over the last several years and will continue to get better with the implementation of threat image projection training and testing and certification of screening checkpoint security firms.

FAA maintains that the measures applied to employees entering through checkpoints provide an equivalent level of security to that obtained by processing through automated access systems. The current access control rule provides for checkpoint screening as an alternative to automated systems. Modification of this practice would entail revision of the rule. FAA will consider this option.

OIG Recommendation D2: FAA issue a policy to require airport operators and air carriers, to the extent possible, to plan and design new airport construction and reconstruction so that access control points in sterile areas permit employees to perform their jobs and meet access control system requirements, without relying on additional layers of security.

FAA Response: Concur. Implementing the recommendation will require accommodation between the strict security that FAA would apply to persons who enter secured areas, and the need to provide relatively free access to aviation employees. It will require the cooperation of industry and government and significant redesign of airport facilities.

OIG Recommendation D3: FAA issue a policy to require unattended jetbridge doors leading to and from the AOA be locked.

FAA Response: Concur. As a means of requiring this measure, FAA in 1997 issued a proposed change to the Air Carrier Standard Security Program (ACSSP). This proposal included a requirement that

[REDACTED]

[REDACTED]

[REDACTED]

Accordingly, even though such individuals would have been previously screened [REDACTED] further tightening of control over these doors.

ADDITIONAL COMMENTS TO OIG FINDINGS


Finding A: Airport operators and air carriers had not successfully implemented procedures for controlling access.

FAA Comments on Finding: We acknowledge the deficiency at the eight locations visited by OIG. Auditors attempted to penetrate secured areas 173 times and were successful 117 times. The rate of compliance was characterized by OIG [REDACTED]. We believe it is important, however, to keep in mind that the access control system relies on a combination of overlapping and redundant measures to protect aircraft. The failure of a single component is a serious matter, but not a total system failure.

The OIG findings are strikingly different from those found a few weeks later by FAA at the same and other locations. The initial OIG results were a matter of significant attention by the FAA and the industry during the intervening period. When FAA conducted over 3,000 tests at the original eight airports and at 71 additional airports, the rate of compliance [REDACTED]. These tests were conducted using a carefully designed testing protocol and by agents who, like the OIG auditors, were generally not locally known. Including weaknesses that did not involve a failure, per se, FAA opened 393 enforcement cases.

We believe this demonstrates that the industry is capable of achieving, at least for a limited period of time, much higher levels of access control performance than that indicated by the OIG audit at the initial eight airports. The important long term challenge for the FAA and the industry will be to sustain access control measures throughout the system at a high level of effectiveness and not again lapse to the extent that they did between 1995 and 1998.

Finding B: Employees often did not meet their responsibilities for Airport Security. These responsibilities include requirements [REDACTED]



FAA Comments on Finding: FAA agrees with the finding with respect to the eight airports. It is clear that access control measures are ineffective if not properly carried out by the employees who use the system.

Finding C: FAA had not fully implemented its Oversight Program to ensure Compliance with Airport Access Control requirements.

FAA Comments on Finding: We agree. FAA began upgrades and improvements to the security data system prior to the commencement of the OIG audit; but continued to experience significant difficulties with the retrieval of data during much of the audit period. Major adjustments to the system have been recently put into effect and are expected to restore credibility in this system for the near term. By mid 2000 we expect to have an entirely new web-based system which should permanently address both the deficiencies noted by the OIG and to provide significant enhancements to the efficiency of data input and retrieval and use of the system for trend analysis.

With respect to field actions to test, inspect and report results, FAA has for some time been developing standardized national protocols for testing and the expansion of the use of aggressive testing methods to additional elements of the aviation security system through individual SEA. This includes the new access control testing protocol.

An SEA concerning access control had been planned for late FY 1999 in connection with our FY 1999 workplan, issued in September 1998. This SEA was accelerated and begun before the end of the second quarter of FY 1999 in response to the early OIG findings.