

GAO

Report to the Chairwoman, Government
Activities and Transportation
Subcommittee, Committee on Government
Operations, House of Representatives

August 1988

AVIATION SECURITY

Corrective Actions Underway, but Better Inspection Guidance Still Needed



RESTRICTED—Not to be released outside the General
Accounting Office except on the basis of the specific approval
by the Office of Congressional Relations.



United States
General Accounting Office
Washington, D.C. 20548

**Resources, Community, and
Economic Development Division**

B-226652

August 23, 1988

The Honorable Cardiss Collins
Chairwoman, Government Activities
and Transportation Subcommittee
Committee on Government Operations
House of Representatives

Dear Madam Chairwoman:

As you requested, we have evaluated the Federal Aviation Administration's (FAA) domestic civil aviation security program. This report presents our findings, conclusions, and recommendations regarding the effectiveness of FAA's inspections in identifying and rectifying security deficiencies.

Unless you publicly announce its contents earlier, we plan no further distribution of this report until 15 days from the date of this letter. At that time, we will send copies to interested congressional committees; the Secretary of Transportation; and the Administrator, Federal Aviation Administration. We will also make copies available to others upon request.

This report was prepared under the direction of Kenneth M. Mead, Associate Director. Other major contributors are listed in appendix II.

Sincerely yours,

A handwritten signature in cursive script that reads 'J. Dexter Peach'.

J. Dexter Peach
Assistant Comptroller General

Executive Summary

Purpose

The nation's airports, air carriers, and the traveling public rely on a network of security features designed to protect them from criminal acts against aviation. The Federal Aviation Administration (FAA) is responsible for ensuring that both airport operators and air carriers take adequate security measures to safeguard the traveling public.

At the request of the Chairwoman, Government Activities and Transportation Subcommittee, House Committee on Government Operations, GAO evaluated FAA's domestic civil aviation security program, including the effectiveness of FAA's inspections in identifying and rectifying security deficiencies.

Background

Since the need for special aviation security measures was first recognized in 1969, FAA has developed and administered programs to prevent criminal acts against aviation. Through these programs, airport operators and air carriers are responsible for installing and operating security features, such as airport perimeter fencing and passenger-screening systems.

Following a series of international terrorist incidents against the flying public during 1985, public and congressional interest in aviation security increased. A Department of Transportation Safety Review Task Force began reviewing FAA's aviation security program in February 1986. Subsequently, in June 1986, the Subcommittee on Government Activities and Transportation held hearings on the adequacy of security and FAA program management pertaining to one of the nation's highest risk airports.

As a result of the security shortcomings surfaced in these hearings, the Subcommittee asked GAO to evaluate FAA's inspection program at six of the nation's largest airports to determine whether this program was fully disclosing security weaknesses.

Results in Brief

During the initial stages of GAO's review, GAO found security weaknesses at six of the nation's highest risk airports. These weaknesses could have resulted in the access of unauthorized persons to air operations areas. FAA's inspection process, one of its most important management tools, was unsuccessful in disclosing some of these weaknesses. FAA has acted or planned actions to address many of the security deficiencies identified by GAO and the Department of Transportation Safety Review Task Force. GAO believes, however, that FAA's inspection process needs to be

further improved to ensure that security weaknesses are sufficiently disclosed and that corrective actions are taken by responsible airport and air carrier officials.

Principal Findings

Security Deficiencies

Security deficiencies were identified by GAO and the Department of Transportation's Safety Review Task Force at the nation's highest risk airports. Chief among the deficiencies were inadequate controls over personnel identification systems and air operations access points. GAO found, for example, that inadequately secured doors provided access to restricted air operations areas and aircraft. GAO and the Safety Review Task Force made recommendations aimed at correcting security deficiencies. Among GAO's recommendations in a January 1988 report, for example, were that FAA require air carrier and airport officials to inventory identification badges.

FAA has acted to address many of the deficiencies identified in this report. These actions include a proposal through its rulemaking process for the installation of computer-controlled identification systems and steps to strengthen the passenger screening process. At the time of GAO's review, FAA was also in the process of addressing recommendations made by the Department's Task Force.

Security Inspections

Nevertheless, FAA still needs to improve its inspection program to ensure that security inspections disclose deficiencies and bring about necessary corrective actions. At the six airports GAO reviewed, it found instances when procedures governing the use of testing and verification were not included as part of the inspection process. As a consequence, GAO found, for example, that FAA inspectors did not test or verify personnel and vehicle identification systems. Instead of verifying that personnel badges and vehicle permits were strictly controlled, inspectors primarily assessed the adequacy of these features by relying on an airport or air carrier official's description of the system and judgment regarding its adequacy.

The lack of testing and verification and the reliance by FAA inspectors on unsubstantiated descriptions of security controls resulted in inaccurate

security assessments. This in turn has prevented inspectors from adequately advising air carriers and airport operators on the breakdown or potential breakdown in security procedures and has prevented FAA management from receiving a complete, accurate security assessment for airports inspected.

Recommendations

GAO believes that improvements in FAA's inspection process are needed to ensure that existing security problems are properly resolved and that potential problems are detected and corrected quickly. Among GAO's recommendations are that the Secretary of Transportation direct the Administrator of FAA to develop appropriate testing and verification procedures to determine the adequacy of key security features, such as lock and key controls and personnel identification systems, and issue clear instructions to inspectors on the use of these procedures.

Agency Comments

The Department of Transportation agreed with GAO's recommendations, and cited a number of actions being taken or planned to address them. These include (1) designing specific inspection procedures to ensure consistent, in-depth evaluations of critical security systems at airports nationwide and (2) incorporating the procedures into formal training presentations for FAA security inspectors. The full text of the Department's comments is included as appendix I.

Contents

Executive Summary		2
Chapter 1		8
Introduction	Role of FAA's Office of Civil Aviation Security	8
	Governing Regulations	9
	Objectives, Scope, and Methodology	10
Chapter 2		12
Security Deficiencies Found at Category X Airports	GAO and DOT Identify Security Deficiencies	12
	Aviation Security Measures Are Interrelated	13
	Access to AOA	13
	Challenge Procedures	15
	Personnel Identification	17
	Passenger Screening	17
Chapter 3		19
A Strengthened Inspection Process Would Enhance FAA Actions to Improve Aviation Security	FAA Has Acted to Improve Security	19
	FAA Needs to Improve Security Inspection Process	21
	Conclusions	23
	Recommendations to the Secretary of Transportation	24
	Agency Comments	24
Appendixes		26
	Appendix I: Comments From the Department of Transportation	26
	Appendix II: Major Contributors to This Report	29

Contents

Abbreviations

AOA	air operations area
DOT	Department of Transportation
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
GAO	General Accounting Office
ICAO	International Civil Aviation Organization

Introduction

Terrorist and criminal attacks against civil aviation have led to a concerted effort to strengthen aviation security around the world. In response to a series of crimes against aviation, the Congress mandated, through amendments to the Federal Aviation Act of 1958, that the Federal Aviation Administration (FAA), as part of the Department of Transportation (DOT), assume primary responsibility for civil aviation security. In accordance with this act, the FAA, in cooperation with airports and air carriers, is responsible for ensuring that security measures are instituted that will safeguard passengers, crew, aircraft, and airports.

Security-screening procedures, which include inspection of all passengers and their carry-on items, have been in effect since 1973. Since the initiation of passenger screening, over 8.5 billion persons have been screened and over 9.5 billion carry-on items have been inspected, according to FAA. This screening and inspection activity has resulted in the detection of approximately 38,600 firearms and approximately 17,000 associated arrests. From January 1973 through June 30, 1987, there were 108 hijacking incidents involving U.S. air carriers operating from both foreign and domestic airports.

In 1986, the Government Activities and Transportation Subcommittee, House Committee on Government Operations, held hearings on the adequacy of security at one of the nation's largest airports. As a result of the security shortcomings surfaced in these hearings, congressional interest in the effectiveness of security at both domestic and foreign airports has increased. This report examines FAA's domestic civil aviation security program, including the effectiveness of FAA's inspections in identifying and rectifying security deficiencies. Later this year, we will issue a separate report on FAA's program to assess security at foreign airports.

Role of FAA's Office of Civil Aviation Security

FAA's security program for domestic airports is designed to prevent unauthorized persons, weapons, or other dangerous devices from getting on board or near airplanes. Through FAA-approved air carrier standard security programs and airport security programs, air carriers and/or airport operators are responsible for implementing appropriate security measures. These security measures include, for example, a comprehensive system of both physical barriers, such as airport perimeter fencing, and personnel-dependent security features, such as those which encourage aviation employees to be alert to potential security breaches and to question the presence of unidentified persons.

In FAA's organization, the Office of Civil Aviation Security is responsible for ensuring aviation security. The Office's headquarters staff develop the security regulations that airports and air carriers must follow and prepares guidance on how FAA inspectors should perform security inspections. This Office also analyzes and responds to threat information received from intelligence sources and coordinates the law enforcement response to hijackings.

The Office has established six airport categories primarily on the basis of the level of air carrier activity. These categories include a set of 16 "category X" airports that are perceived to carry the highest security risk. More stringent security measures are applied to the busiest airports since high activity level is associated with a greater threat potential. Security risk categories I through V have been assigned to the nation's remaining 424 airports, with category V being the lowest of the risk categories.

In addition to the above, this Office oversees various research and development initiatives related to improving explosive detection capabilities. Present methods used to detect explosives carried on passengers, and in baggage and cargo, primarily consist of employing hand searches, X-ray examination, and/or specially trained dogs. Reliable technology currently does not exist, however, to detect emerging, highly sophisticated explosives and detonating devices that may be carried on passengers, or in baggage or cargo. To facilitate accelerated research and development efforts, funding for the FAA research and development program was increased from \$1 million to \$2 million before fiscal year 1985 to between \$11 million and \$12 million per year during the past 2 fiscal years.

The Office oversees the work of its Civil Aviation Security divisions located in FAA's nine regional offices. These divisions interpret headquarters guidance, perform administrative functions, and supervise the operations of field units. Security inspections are conducted by approximately 345 inspectors in about 30 field office units. Security inspectors periodically inspect both airports and air carriers to ensure that adequate security procedures are continually in effect. These inspectors are also responsible for initiating enforcement actions when security regulations are not adhered to.

Governing Regulations

Federal Aviation Regulations (FAR) Parts 107 and 108 govern domestic airport and air carrier security, respectively. These regulations mandate

the adoption and effective implementation of minimum security programs by airports and air carriers. These programs must include specific measures for passenger screening, protection of aircraft, and airport access controls. In general, FAR Part 107 requires that the airport operator (1) create a security program for the airport, (2) provide controls to prevent or deter unauthorized persons from accessing the air operations area (AOA),¹ and (3) provide law enforcement support. For air carriers, FAR Part 108 generally requires that the carrier (1) adopt and carry out a security program, (2) screen passengers and property, (3) provide and use ground and in-flight security coordinators, and (4) prohibit unauthorized access to the airplane.

In addition to the above requirements, the United States recognizes the security standards developed by the International Civil Aviation Organization (ICAO) and is a signatory to ICAO. FAA expects the nation's category X airports to adhere to the ICAO standards. In October 1987, FAA regions were directed by headquarters to use these standards as inspection criteria in assessing the adequacy of security at these airports.

Besides developing security standards, ICAO has also published a series of security manuals establishing required and recommended practices for safeguarding international civil aviation. The 1987 third edition of the manual contains numerous recommended measures and procedures and is intended to be a collection of material to help implement the ICAO standards. ICAO recognizes that implementation of the recommended practices and procedures will be based on priorities of the individual nation-states as signatories to ICAO. According to ICAO, specific, detailed security regulations would have to be prepared by each nation-state. ICAO's recommended practices and procedures are advisory in nature.

Objectives, Scope, and Methodology

On July 29, 1986, the Chairwoman, Government Activities and Transportation Subcommittee, House Committee on Government Operations, requested that we evaluate FAA's domestic civil aviation security program. The Subcommittee specifically asked that we determine the effectiveness of FAA's inspections in identifying and rectifying security deficiencies.

Chapter 2 discusses the major components of airport and air carrier security programs and the security deficiencies identified by GAO, FAA,

¹The air operations area is the part of the airport where aircraft operate, load, and disembark cargo and passengers.

and the Department of Transportation. Chapter 3 summarizes FAA's actions to address the identified deficiencies. Within this framework, chapter 3 discusses the effectiveness of FAA security inspections and also presents our conclusions and recommendations.

This report is based on work conducted at FAA headquarters and at six category X airports in four of FAA's nine regions. For security reasons, we do not identify the airports or regions. To assist in our review, we employed the services of a consulting firm with experience in aviation security work and knowledge of FAA's security program.²

At each airport, we evaluated the adequacy of FAA's airport and air carrier security inspections by accompanying inspectors and by comparing the inspection process to FAR and ICAO standards. We also independently tested certain security features in those areas for which we believed the security inspections were insufficient. At these airports, we interviewed regional officials and field office inspectors, supervisors, and managers. We also interviewed airport and air carrier representatives in each location. We reviewed inspection reports and other documentation related to inspections that FAA performed.

At the headquarters level, we reviewed available inspection results and the written airport security programs for all category X airports. We reviewed agency documents and interviewed FAA officials, including the Director of the Office of Civil Aviation Security. We also reviewed FAA and DOT initiatives relating to the security program, including DOT's Safety Review Task Force reports on various aspects of the security program.

We conducted our field work and headquarters review from January 1987 through April 1988. This work was done in accordance with generally accepted government auditing standards.

²Systems, Requirements & Services Associates, Inc., McLean, Va. 22101.

Security Deficiencies Found at Category X Airports

Numerous security deficiencies existed at the time of our review at the nation's highest risk airports, those 16 labeled "category X." If left uncorrected, these deficiencies could allow unauthorized persons to gain access to the air operations areas. Among the deficiencies we found were inadequate controls over air operations access points and over personnel identification systems, and ineffective passenger screening. These deficiencies and others were also identified by DOT's Safety Review Task Force and, to some extent, by FAA through its inspection process. As discussed in chapter 3, FAA has acted to address personnel identification system and passenger-screening deficiencies. FAA has also instituted a National Airport Inspection Program, which will focus on category X airports during fiscal year 1988.

GAO and DOT Identify Security Deficiencies

GAO's and DOT's work in the aviation security area has demonstrated the existence of the security deficiencies discussed in this chapter.¹ To some extent, FAA inspectors also identified security deficiencies for these airports. We found, however, that FAA's inspection process has not been adequate to fully disclose deficiencies at the six category X airports subject to our review. Specifically, through independent testing of various security features at the six airports we visited, we found serious deficiencies that FAA inspectors had not noted. In general, FAA inspectors advised air carriers and airport officials that corrective actions were needed, either as a result of our or the inspectors' own work.

The DOT Safety Review Task Force also reviewed, beginning in February 1986, FAA's aviation security program and published a series of reports on five security areas, including AOA security and passenger screening. The findings of this task force also demonstrate that the security weaknesses identified in this chapter exist at the nation's highest risk airports. For each of the major security areas outlined in this chapter, the task force found many of the same weaknesses identified by GAO and FAA despite the variances in airports selected for review.

During our review, FAA was in the process of responding to approximately 65 recommendations contained in the task force's series of reports. FAA officials agreed with the large majority of DOT findings and had developed action plans to address each of the recommendations.

¹Aviation Security: Improved Controls Needed to Prevent Unauthorized Access at Key Airports (GAO/RCED-88-86, Jan. 29, 1988).

Aviation Security Measures Are Interrelated

In the context of aviation security, an airport is divided into two parts: (1) the AOA, which is the part of the airport where aircraft operate, and (2) the rest of the airport, predominantly the terminal, cargo areas, other structures such as those containing electrical systems and fuel tanks, and vehicle parking lots. A hallmark of the approach to aviation security is redundancy. The numerous security measures in place at our nation's airports are interrelated; generally, in the event that one measure fails, another measure is in place to support the first measure. For example, fencing and personnel identification systems are not enough; security lighting, law enforcement personnel, and the awareness of aviation employees are integral parts of a complete security program designed to protect the AOA from unauthorized access.

Access to AOA

Among the important and more visible aviation security features are those that define the perimeter of the AOA, such as perimeter fencing, vehicle and pedestrian gates, and perimeter buildings, including air cargo facilities. Other important features include fire doors, jetways, and employee waiting rooms. All of these features have at least one thing in common: they provide almost immediate access to the AOA. When not properly controlled in accordance with FAR and ICAO standards, these features can provide a direct avenue for criminal attacks against aviation.

During the early stages of our review, we found serious security deficiencies related to all of these features. Using the results of FAA inspections, the DOT task force, and our own security tests, we found that access to the AOA could easily be gained because these features were not adequately controlled. In some cases, the weaknesses of these particular features were compensated for when airport/air carrier employees "challenged" or questioned the unauthorized presence of the FAA inspector or our evaluators. In most cases, however, challenge procedures were nonexistent and therefore did not compensate for the security weaknesses identified here.

Perimeter Fencing, Gates, and Buildings

FAA and ICAO recommend that all openings in the perimeter be controlled to prevent unauthorized access. According to ICAO recommended procedures, security fences should be kept clear of trees, stowed equipment and material, and vehicles for a distance of 10 feet inside the fence line and 20 feet outside, wherever possible. Where feasible, buildings and other suitable permanent obstacles are to be used as part of the physical barrier, provided that access through the buildings is controlled. FAA

Advisory Circular 107-1 further states that gates, doors, and other openings in the perimeter of the AOA should be secured or controlled to minimize the possibility of unauthorized entry.

At one airport, we found that perimeter fences were not cleared of items that could help an intruder cross the perimeter fencing. The DOT task force found instances where fence bottoms were high enough above ground level to permit a person to slip beneath and also found gates that were chained loosely enough to permit a person to slip through. According to the task force report, fencing was often in disrepair and poorly lighted or covered with overgrowth.

The DOT task force found that vehicle gates remained open longer than needed to permit one vehicle to pass through, raising the potential for unauthorized persons or vehicles to pass through the opening. Pedestrian gates were also identified as a security problem when, through common courtesy, authorized persons held gates open for others without determining proper authorization.

DOT's March 1987 report on perimeter security and AOA access recommends that FAA require that all doors in terminal buildings between the public areas and the AOA be locked. Exceptions would be permitted for doors or gates that are attended when they are unlocked (such as doors used for passenger access to aircraft) and emergency exits with alarm locks. In addition, the report notes that the number of doors leading from the terminal area to the AOA that are not barred or otherwise permanently locked should be limited to the minimum number required by safety, security, or operations.

By accompanying FAA inspectors and by independently testing the security features mentioned above, we found that access to the AOA could be gained and, as discussed later in this chapter, that in general, employee "challenge" procedures were not used. For example, at three major airports we were able to walk unchallenged through various perimeter buildings, including post office and air cargo buildings, and exit directly onto the AOA. In these instances, we made no attempt to disguise ourselves as airport or air carrier employees.

Fire Doors, Jetways, and Employee Waiting Rooms

Air carrier guidance states that fire doors may be considered adequately controlled if restricted area signs and challenge procedures are used during operational hours. During nonoperational hours, or when challenge procedures are not in effect owing to the absence of aviation

employees, these doors must be secured or controlled by other means acceptable to FAA. ICAO recommends that airports use audible and visual alarms as controls.

At one airport, we found unalarmed fire doors through which we were able to walk onto the AOA. Jetways also proved to be inadequately secured at two airports. For example, we were able to exit the terminal through the jetway and on to the AOA at one airport. The air carrier representative responsible for controlling the jetway was inside the parked aircraft talking to the crew members. When asked why the door to the jetway was left open, he said that it was too hot in the terminal to close the door and that he was still “controlling” access even though he was in the aircraft and not positioned at the jetway door. After pointing out that we had already gained access to the AOA without his seeing us, he acknowledged that he could not properly control access from his particular vantage point inside the parked aircraft.

We also gained access to another airport’s AOA by entering air carrier-maintained rooms where employees waited for buses which shuttled them between the sterile concourse and employee parking lots. Such “bushold” rooms, as they are called, should be controlled to restrict unauthorized persons from gaining access to the AOA from these rooms. In one case, the lock was defective and we gained access to the room, which was empty at the time. We then exited from the concourse onto the AOA. In another instance, we dressed in the air carrier’s colors and, without showing any identification, walked past the room guard and onto the AOA.

Challenge Procedures

In accordance with part 108 of FAR, the air carrier standard security program requires airport and air carrier employees to challenge unauthorized persons in the AOA as well as in baggage rooms, cargo areas, and other nonpublic areas. Each airport or air carrier employee who has been issued an identification card or badge is responsible for challenging or questioning persons whose authorization is not apparent, that is, a person who is not displaying the proper identification. Each airport we visited included challenges as a requirement of its approved security program in an effort to restrict unauthorized access to air operations and nonpublic areas.

At most of the airports we visited, challenge procedures were not working effectively. With the full knowledge and cooperation of FAA inspectors, we gained access to the AOA without being challenged by the airport

and air carrier employees who saw us. Without wearing identification or attempting to disguise ourselves, we entered open or unlocked cargo doors and walked through the buildings or gates and out onto the AOA. In all cases, employees were present who could have challenged us. At such times, we had access to cargo shipments or aircraft in which we could have planted an item or inflicted damage.

At one major airport, we were able to enter a plane being serviced by several baggage handlers. After staying in the plane for several minutes, we left the plane and stood next to it. Despite our extended presence, none of the crew challenged us. The FAA inspector with us finally approached the crew members to ask them why they did not challenge us. According to the inspector, these crew members stated that since we were professionally dressed, they assumed we were official airport visitors.

At all of the airports we visited, employees we questioned seemed to be aware of the importance of challenging. In some cases, however, employees said that for personal safety reasons, they were afraid to challenge people without visible identification, particularly if they were working in an isolated area of the airport. According to the DOT report on perimeter security and AOA access, airport managers told the task force that in some cases aviation employees were afraid to challenge the unknown, for fear of personal danger. These employees were described as being afraid to put themselves at risk because they often have no easy means of summoning assistance. For example, a mechanic working on an aircraft alone at an obscure area of the airport and without a way to call for help is reluctant to "ask for trouble."

Nevertheless, we found that aviation employees usually have relatively easy access to phones located in surrounding offices. While they may not want to immediately challenge the unknown, they would in the majority of cases at least be able to ask airport law enforcement officers for assistance.

Complicating this problem is the fact that at one of the airports we visited, airport and air carrier employees were not displaying their identification badges. DOT and FAA officials also noted this problem at another category X airport. FAA officials acknowledged that the incentive to challenge is seriously diminished when most of an employee's coworkers are not displaying identification. Given the right clothing, an unauthorized person could go unnoticed in such a work group. Challenge procedures have been referred to as a "last line of defense." That is, if the

other security features of an airport have been breached and an unauthorized person has gained access to the AOA, the last security feature to be encountered would be the airport or air carrier employee who questions or challenges the presence of an unauthorized person.

Personnel Identification

FAA and ICAO require strict accountability and control over personnel identification systems. Airport operators are expected via FAA Advisory Circular Part 107-1 to institute strict accountability procedures for all identification cards and badges. Similarly, ICAO requires strict control and accounting procedures to ensure that at least annually all issued identification cards can be accounted for.

During our review we found that, in general, airport officials could not account for personnel identification badges. Our verification of airport personnel identification records for four tenants at a category X airport showed that three of the four companies had terminated employees and reportedly returned the badges to the airport. Airport officials, however, had no records of the badges being returned. For example, 4 of 17 badges (24 percent) for one security company's terminated employees could not be accounted for. At another category X airport, three tenants were not tracking the retrieval of badges from terminated employees. These tenants said that they could only guess at the number of lost badges.

Inspection results for all category X airports reviewed at headquarters showed that at 6 of the 16 X airports, airport officials acknowledged that they could not properly account for personnel identification badges. DOT noted that some airports lack an effective means of recovering permits from separated employees and that at many airports, identification badges are issued without an expiration date. The task force also noted that at some airports, identification badges are issued that categorically authorize access to all areas of the airport, even to persons whose jobs do not require such broad access.

Passenger Screening

As shown in our prior work on FAA's testing of the passenger-screening process,² shortfalls exist in the screening process. FAA test results as of March 1988 show that improvements are needed to ensure that the process effectively prevents firearms, explosives, and other dangerous

²Aviation Security: FAA Needs Preboard Passenger Screening Performance Standards (GAO/RCED-87-182, July 24, 1987).

weapons from being carried on board an airplane and presenting a danger to the traveling public. DOT's report on passenger screening concluded that the process must be strengthened through a variety of measures. The report concluded that historical evidence points to the overall success of the process, but it also noted that the consequences of a single incident are such that the FAA must continually monitor the screening program to ensure its effectiveness.

At the six category X airports we visited, we found that overall, the screening process was not effective in detecting test weapons. During 30 tests of the screening process conducted in the presence of FAA inspectors, we were able to pass 11 test weapons through the screening system without being detected. At one of these airports, the screener did not identify an FAA-test weapon even though the screener picked it up and visually inspected it. Training records showed that the screener had seen this particular test weapon during the required screener training course.

A Strengthened Inspection Process Would Enhance FAA Actions to Improve Aviation Security

FAA has acted or is planning actions to address many of the airport security deficiencies identified in chapter 2. The agency's inspection program is its key management tool to ensure that such corrective actions are effective and to prevent other problems from continuing unnoticed. We found, however, that FAA's airport security inspection process needs improvement because it lacks sufficient testing and verification procedures to adequately disclose security deficiencies, as discussed in the previous chapter.

FAA Has Acted to Improve Security

Chief among FAA's actions to improve airport security are new requirements over personnel identification system controls and the passenger-screening process. FAA has also taken steps to strengthen challenge procedures. To evaluate the application of security initiatives such as these and to determine whether additional measures are needed, FAA has also initiated a National Airport Inspection Program that will focus on the nation's category X airports.

Personnel Identification Systems

In response to both DOT and GAO recommendations,¹ FAA has proposed through its rulemaking process that airport operators install and use a computer-controlled card system for access to restricted airport areas. According to FAA, the proposed system would be capable of (1) monitoring each location where access to the restricted area is permitted by means of a "card reader" linked to the central computer and (2) denying access for persons who do not possess an appropriate card. A unique code for each card would allow the computer to be reprogrammed in a matter of minutes to deny access to any specific card. As proposed, this type of system would be installed at 269 of the nation's 440 airports. All category X airports would be subject to the new requirements.

Passenger Screening

Both GAO and the DOT Safety Review Task Force recommended that FAA establish a passenger-screening performance standard and fine air carriers when screening system performance does not meet the standard. In July 1987, the Task Force recommended that FAA take more aggressive enforcement action, fining carriers for any failure to detect test items at a checkpoint. In October 1987, FAA established a 100-percent standard and began levying, under certain conditions, civil penalties ranging up to the then maximum of \$1,000. Generally, civil penalties were levied only

¹Aviation Security: Improved Controls Needed to Prevent Unauthorized Access at Key Airports (GAO/RCED-88-86, Jan. 29, 1988).

if a screening checkpoint missed three or more test items during the last five tests. Warning letters were issued in other instances.

In March 1988, FAA announced that, overall, passenger-screening performance had not significantly improved since October 1987 and that more stringent measures would be taken. FAA increased the amount of its maximum civil penalty from \$1,000 to \$10,000² and, implementing the July 1987 recommendation of the Task Force, directed that a civil penalty would be levied for any failure by a screening system to detect an FAA test object. Under the new procedures FAA now fines air carriers \$10,000 for each failure where screening checkpoint performance falls below a 95-percent detection rate. For those failures at screening checkpoints where the detection rate is 95 percent or better, the recommended sanction would be \$1,000, unless aggravating circumstances, such as lack of screener training, exist.

The policy further states that the detection rate will be established by an evaluation of the 20 most recent tests of that checkpoint. The first failure at a checkpoint would carry a \$1,000 civil penalty. The second failure and all subsequent failures would carry a \$10,000 civil penalty unless the results of the 20 previous tests of that checkpoint warranted a reduction in civil penalty by virtue of demonstrating a 95-percent or better detection rate.

Before FAA established a standard, air carriers responsible for passenger-screening checkpoints had not been given a clearly defined performance expectation. Moreover, no enforcement actions were taken against air carriers when their screening checkpoints failed to detect test weapons passed through the system during FAA tests.

In addition, on December 21, 1987, FAA made a procedural change and began requiring all airport and air carrier employees at all U.S. airports to undergo full security screening when entering restricted areas controlled by screening checkpoints. The intent of this requirement, coupled with the proposed computer-controlled identification system discussed previously, is to better control access to air operations and other restricted areas by requiring everyone who passes a screening checkpoint to undergo screening.

²Public Law 100-223, enacted on December 30, 1987, raised the maximum allowable civil penalty.

Challenge Procedures

FAA has taken several steps to reemphasize the importance of challenging and of wearing identification badges—areas that DOT and we pointed out as needing to be strengthened. In March 1987, the DOT Task Force recommended that FAA should require airport operators to implement programs emphasizing the challenge requirement. According to FAA officials, FAA has emphasized to its field staff the need for aggressive enforcement action when employees do not challenge unauthorized persons or wear their identification badges. In addition, FAA has contracted to buy five videotapes specifically designed for presentation to groups of airport and air carrier employees. The tapes will stress a team approach to security at airports and emphasize the need to challenge and/or report individuals who are not wearing appropriate identification badges or otherwise seem out of place.

National Airport Inspection Program

In January 1988, FAA initiated the Civil Aviation Security National Airport Inspection Program. FAA developed this program to conduct comprehensive, in-depth inspections of major airports nationwide to evaluate the application of security initiatives and the effectiveness of the overall Civil Aviation Security Program. During fiscal year 1988, these inspections will be conducted at all category X airports.

As of May 1988, FAA had completed eight of these inspections. FAA headquarters officials stated that once these inspections are completed, the results would be a useful management tool for identifying systemic problems that may require further changes in security procedures.

FAA Needs to Improve Security Inspection Process

FAA relies on its inspection process—a key management tool—to identify airport and air carrier security deficiencies and, thus, bring about corrective actions. The importance of the inspection process is further evidenced by the significant increase in FAA security inspectors over the past 2 years. FAA's security inspector work force nearly doubled from 184 on-board inspectors in June 1985 to 345 in May 1988. In addition, FAA increased its inspection activity at major airports. Monthly security inspections are now called for at category X airports and for air carriers serving them.

Although FAA inspectors are responsible for ensuring that adequate security procedures are continually in effect, we found that FAA's inspection process as conducted at the six airports we reviewed was not sufficient to adequately disclose security deficiencies such as those discussed in chapter 2 and further discussed below. As a result, inspection

reports for these airports understated the existing deficiencies. We also found that the weaknesses we noted in the inspection process and associated methodology itself, while specific to the six airports we reviewed, were systemic in that the process is the same nationwide and requires no testing and verification procedures to determine the adequacy of certain security features. Standardized checklists identifying security features to be inspected are used during inspections, but the extent of coverage for individual security components is left to the judgment of each inspector.

These inspection weaknesses existed because, for all category X airports, FAA headquarters has not developed for inspectors clear inspection procedures and associated guidance on the extent of verification and testing needed to determine the adequacy of a security feature. As a result, certain security features, such as accountability and controls over keys and personnel identification badges, were not adequately tested or verified as part of the inspection process.

Inspection Process Does Not Include Testing/ Verification Procedures

FAA's inspection process does not include procedures or guidance concerning the extent of testing and/or verification needed to ensure the adequacy of certain security features such as locks and keys, and personnel and vehicle identification systems. At the six airports we reviewed, we found that none of the inspectors tested or verified the accountability and control over these features. Instead, we found that inspectors assessed the adequacy of these security features on the basis of airport and air carrier officials' description and personal assessment of the individual features.

Controls Over Locks and Keys

Although FAA and ICAO state that keys should be controlled to protect personnel and property from unauthorized access, FAA inspectors we accompanied did not determine if airport officials could account for keys. Rather, the inspectors discussed key control procedures with airport officials and/or verified that some gates and doors were actually controlled or locked. The inspectors noted no deficiencies on the six category X airport inspection reports for this aspect of security.

Airport officials responsible for controlling locks and keys acknowledged poor controls over keys. One major airport's key official told us he controlled keys for gates only. He said his predecessor had issued the keys to maintenance, fire, and police personnel, but to his knowledge the airport had no record of who actually had received the keys. Similarly,

an official at another large airport told us he approves key requests but has no control over air carriers' and service companies' keys once he provides them. He assumed that companies were losing keys since they requested more keys almost weekly. Another official at a third airport told us he does not maintain control over approximately 400 maintenance employees' keys or keys to gates located on leasehold property.

The inspectors cited several reasons for not verifying key control procedures. One inspector commented that determining if the airport could account for keys and inquiring into tenant companies' key control procedures were activities outside the scope of security inspections. Another inspector stated that too many people were involved in key control and it would take too much time for him to check out the various companies' key control procedures. A third inspector's supervisor stated that because of other work requirements, key control was not adequately assessed during the inspections even though FAA was aware that it was a problem at this airport.

Controls Over Identification Systems

FAA inspectors at the six category X airports we reviewed did not test or verify personnel and vehicle identification systems. Instead of verifying that actual procedures adhered to the requirement that personnel badges and vehicle permits be strictly controlled, inspectors primarily assessed the adequacy of these features by relying on an airport or air carrier official's description of the system and judgment regarding its adequacy.

At all of the six category X airports we reviewed, inspectors rated personnel and vehicle identification systems as adequate. In each case, inspectors conducted no tests to determine the adequacy of controls over these systems. In some cases, inspectors documented procedures for issuing badges and permits and rated these procedures as satisfactory on the basis of airport and air carrier officials' judgments. FAA inspectors did not visit airport tenants, however, to verify that their controls over personnel badges and vehicle permits were adequate to prevent an unauthorized individual from obtaining access to vehicles that would be allowed entry to these areas.

Conclusions

The numerous security deficiencies found at the nation's category X airports, as discussed in chapter 2, have demonstrated the need for increased FAA management attention. While the features described in

this report do not encompass all aspects of security in place at individual airports, these features are, nevertheless, some of the more significant components of airport security. As such, FAA, acting with air carriers and airport operators, must ensure that only authorized persons are gaining access to air operations areas and aircraft.

FAA has acted or planned actions to address some of these deficiencies and should be able to address others through its National Airport Inspection Program. FAA's key management tool—its inspection process—can be improved, however, to ensure that security deficiencies are sufficiently disclosed at the category X airports. The lack of testing and verification procedures undermines the validity of the inspection process and prevents inspectors from adequately advising air carriers and airport operators on the breakdown or potential breakdown in their security procedures.

Because inspections did not include comprehensive testing and verification procedures, FAA management did not receive a complete security assessment for these airports. Inspection reports provided to regional and headquarters management did not provide complete information on the adequacy of controls over personnel and vehicle identifications systems and locks and keys. On the basis of our identifying deficiencies not noted by inspectors during the inspection process, we believe that FAA inspection reports often understated the deficiencies that existed at these airports.

Recommendations to the Secretary of Transportation

FAA should improve its domestic aviation security inspection process at category X airports. We recommend that the Secretary of Transportation direct that the Administrator, FAA,

- develop appropriate testing and verification procedures to determine the adequacy of key security features, such as lock and key controls and personnel and vehicle identification systems;
- issue clear instructions to inspectors on the use of these procedures during the inspection process; and
- incorporate these procedures and associated instructions into inspectors' formal training curriculum to ensure that they are adequately trained in the inspection process to be followed.

Agency Comments

DOT agreed with our recommendations and commended the report for its "insightful conclusions." Actions being taken or planned to address our

Chapter 3
A Strengthened Inspection Process Would
Enhance FAA Actions to Improve
Aviation Security

recommendations include (1) designing specific inspection procedures to ensure consistent, in-depth evaluations of critical security systems at airports nationwide and (2) incorporating the procedures into formal training presentations for FAA security inspectors. The full text of DOT's comments is included as appendix I.

Comments From the Department of Transportation



U.S. Department of
Transportation

Assistant Secretary
for Administration

400 Seventh St., S.W.
Washington, D.C. 20590

JUL 18 1988

Mr. Kenneth M. Mead
Associate Director
Resources, Community, and Economic
Development Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Mead:

Enclosed are two copies of the Department of Transportation's comments concerning the U.S. General Accounting Office draft report entitled, "Aviation Security: Corrective Actions Underway But Better Inspection Guidance Still Needed."

Thank you for the opportunity to review this report. If you have any questions concerning our reply, please call Bill Wood on 366-5145.

Sincerely,

Maurice J. Allen *bc*
Jon H. Seymour

Enclosures

Enclosure

Department of Transportation Reply to
General Accounting Office Draft Report
Entitled: "Aviation Security: Corrective Actions Underway
But Better Inspection Guidance Still Needed"

SUMMARY OF GAO FINDINGS AND RECOMMENDATIONS

The General Accounting Office (GAO) draft report states that security deficiencies were identified both by GAO and the Department of Transportation's (DOT) Safety Review Task Force at the Nation's highest risk airports. Chief among the deficiencies were inadequate controls over personnel identification systems and air operations access points. GAO found, for example, that inadequately secured doors provided access to restricted air operations areas and aircraft. GAO and the Safety Review Task Force have made recommendations aimed at correcting security deficiencies. Among GAO's past recommendations were that the Federal Aviation Administration (FAA) require air carrier and airport officials to inventory identification badges.

GAO further states that FAA has acted to address many of the deficiencies identified in this report. These actions include plans for the installation of computer-controlled identification systems and steps to strengthen the passenger screening process. At the time of GAO's review, FAA was also in the process of addressing recommendations made by the Department's Safety Review Task Force.

GAO recommends that the Secretary of Transportation direct the Administrator, FAA, to: (1) develop appropriate testing and verification procedures to determine the adequacy of key security features, such as lock and key controls and personnel and vehicle identification systems; (2) issue clear instructions to inspectors on the use of these procedures during the inspection process; and (3) incorporate these procedures and associated instructions into inspectors' formal training curriculum to ensure that they are adequately trained in the inspection process to be followed.

SUMMARY OF DEPARTMENT OF TRANSPORTATION POSITION

The Department concurs with GAO's recommendations and would like to commend GAO for its insightful conclusions. In response to the first recommendation, the Civil Aviation Security National Airport Inspection Program (CASNAIP) was developed by FAA to conduct

Appendix I
Comments From the Department
of Transportation

- 2 -

special, in-depth inspections of selected airports and inspections/reviews of the air carriers that operate from those airports. CASNAIP inspection guidelines were provided to field personnel by memorandum dated February 4. Included in the guidelines is the requirement that in-depth examination and verification should be made of identification media control and accountability procedures.

Subsequent CASNAIP team leader instructions were provided to the field by memorandum dated April 14. The instructions directed that air carrier and airport identification procedures should be closely evaluated by monitoring the procedures of the issuing office(s) and determining the actual application of those procedures through sampling of identification media. The instructions further directed that similar techniques should be applied to inspections of vehicle identification procedures and lock and key control procedures. Associated reporting formats accompanied these instructions.

In response to the second recommendation, we recognize that more detailed guidelines to field personnel are needed. Accordingly, a staff study has been initiated to design specific inspection procedures which will ensure consistent, in-depth evaluations of critical security systems at airports nationwide.

In response to the third recommendation, after development of the procedures indicated above, they will be provided to field personnel for immediate application and will be incorporated into formal training presentations for FAA security inspectors.

Major Contributors to This Report

Resources,
Community, and
Economic
Development Division,
Washington, D.C.

Kenneth M. Mead, Associate Director, (202) 275-1000
Victor S. Rezendes, Associate Director
Thomas J. Barchi, Group Director
Robert W. Shideler, Project Manager
Connie Brindle, Evaluator-in-Charge
John M. Nicholson, Senior Evaluator

Atlanta Regional
Office

Elliott Appleman, Regional Assignment Manager
Anita L. Lenoir, Senior Evaluator
Margaret Jolley, Evaluator

Chicago Regional
Office

Clem Preiwisch, Regional Assignment Manager
Roger Bothun, Evaluator
Michael Hartnett, Evaluator



Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are \$2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

United States
General Accounting Office
Washington, D.C. 20548

Official Business
Penalty for Private Use \$300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100
