United States General Accounting Office
Report to Congressional Committees

GAO

January 1994

AVIATION SECURITY

Additional Actions Needed to Meet Domestic and International Challenges

GAO/RCED-94-38

GAO

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

Resources, Community, and
Economic Development Division

B-226652

January 27, 1994

The Honorable Frank R. Lautenberg
Chairman
The Honorable Alfonse M. D'Amato
Ranking Minority Member
Subcommittee on Transportation and
Related Agencies
Committee on Appropriations
United States Senate

The Honorable Bob Carr
Chairman
The Honorable Frank R. Wolf
Ranking Minority Member
Subcommittee on Transportation
and Related Agencies
Committee on Appropriations
House of Representatives

This report, prepared at your request, examines the Federal Aviation Administration's (FAA) response to the Aviation Security Improvement Act of 1990. We are making recommendations aimed at ensuring that (1) the nation's category X airports (airports that have a high volume of traffic and complex security programs) are properly assessed to fully examine threats and vulnerabilities, (2) U.S. citizens traveling on foreign airlines receive an adequate level of security, (3) efforts to safeguard mail and cargo carried by passenger aircraft are effectively carried out, and (4) FAA's efforts are sufficient to meet current and future challenges to aviation security.

As arranged with your offices, we will send copies of this report today to the Secretary of Transportation; the Administrator, FAA; the Director, Office of Management and Budget; and other interested parties. We will also send copies to others upon request.

This work was performed under the direction of Kenneth M. Mead, Director, Transportation Issues, who can be reached at (202) 512-2834. Major contributors to this report are listed in appendix III.

Keith O. Fultz
Assistant Comptroller General

Executive Summary

Purpose

In December 1988, a terrorist bomb destroyed Pan Am Flight 103, killing all 259 passengers and crew. In response, the Congress passed the Aviation Security Improvement Act of 1990, which directed the Federal Aviation Administration (FAA) to improve aviation security. Citing the need for FAA to maintain an effective and forward-looking security program, the Chairman and Ranking Minority Member, Subcommittee on Transportation and Related Agencies, Senate Committee on Appropriations, and the Chairman and Ranking Minority Member, Subcommittee on Transportation and Related Agencies, House Committee on Appropriations, asked GAO to assess FAA's response to the act. Specifically, GAO was asked to (1) examine FAA's efforts to assess, in conjunction with the Federal Bureau of Investigation (FBI), the security of domestic airports; (2) review FAA's efforts to determine if a similar level of protection exists for U.S. citizens traveling on foreign airlines; and (3) assess FAA's efforts to improve the security of mail and cargo. In addition, GAO was asked to identify additional steps that FAA could take to improve its security program.

Background

In the aftermath of Pan Am 103, the President's Commission on Aviation Security and Terrorism was established to examine the nation's aviation security system. In May 1990, the Commission reported that the system was seriously flawed and that it failed to provide adequate protection for the traveling public. The Aviation Security Improvement Act of 1990 incorporated many of the Commission's recommendations and mandated both organizational and programmatic changes in FAA's security program. Among its mandates, the act directed FAA to (1) assess, in conjunction with the FBI, security at domestic airports; (2) accept a foreign carrier's security program only if FAA determines that the program provides a level of protection similar to that provided by domestic carriers serving the same airport; and (3) report to the Congress on the need for additional measures to safeguard the transport of mail and cargo by passenger aircraft.

Results in Brief

FAA has taken important steps to respond to the act, such as placing additional staff at category X domestic airports (airports that have a high volume of traffic and complex security programs). Although the joint FAA-FBI assessments of 18 of the 19 category X airports examined a wide range of problems affecting aviation security and confirmed the need for many of FAA's initiatives, the assessments did not match the capabilities, methods, or intent of known terrorist groups in the United States with vulnerabilities at individual airports. FAA's matching of known terrorists'

capabilities, methods, and intent with airports' vulnerabilities is important to help determine the appropriate level of security at domestic airports and develop effective contingency plans.

Important differences in security requirements exist between U.S. and foreign carriers for flights departing from some foreign airports. U.S. carriers are required to take more stringent security measures than their foreign counterparts. Nevertheless, on the basis of a review of foreign carriers' security programs, FAA officials believe that a similar level of protection exists for U.S. passengers flying via most foreign carriers. GAO believes this conclusion is premature because, among other things, FAA has not completed its analyses of countermeasures that individual foreign carriers will be asked to adopt at specific airports and has not developed guidance defining such similarity or how it will be enforced.

FAA recently issued requirements to improve cargo security. FAA is taking actions to identify freight forwarders—entities that consolidate cargo and buy space on aircraft—and heighten security awareness in the cargo industry. However, FAA has not developed an inspection strategy to ensure that freight forwarders comply with the new requirements. In addition, FAA and the U.S. Postal Service (USPS) have negotiated an agreement in which USPS is taking certain measures to improve the security of mail flown via passenger carriers. However, a prior agreement between FAA and USPS for securing mail was not successfully implemented.

The safety of the traveling public rests on how well FAA can adapt to changing conditions. GAO has identified several actions that FAA could take to improve its security program and help shape the future of aviation security. These actions include (1) pilot-testing new procedures before implementing them, (2) paying greater attention to such human factors issues as security screeners' performance and passenger profiling (interviewing), (3) making better use of the security information that FAA collects on air carrier and airport inspections, and (4) providing airport security coordinators at category X airports with security clearances.

Principal Findings

FAA Has Taken Important Steps, but Concerns Remain

FAA has completed many of the organizational and administrative requirements of the act. For example, FAA has established Federal Security Managers at the 19 category X airports. However, important questions

about domestic and international aviation security remain unanswered and will continue to challenge FAA. For example, the joint FAA-FBI assessments of the category X airports pointed out that problems persist with airport screeners' proficiency and mail and cargo security. Also, the assessments did not examine the capabilities or intent of known terrorist groups and the relationship to vulnerabilities at each category X airport. Until FAA does so, neither it nor the industry will have adequate information to guide future efforts.

Important questions remain about the security of U.S. passengers using foreign airlines to travel to and from the United States because most foreign airlines rely on less stringent international standards. FAA officials recognize that differences exist between domestic and foreign security requirements but believe that a similar level of protection generally exists. However, GAO believes it is too early to make judgments on foreign carriers' security and similarity to U.S. carriers because some foreign governments have not been willing to share important information with FAA. In addition, FAA officials acknowledge that their analyses of foreign carriers' security programs and countermeasures needed at various locations are not complete. This complex issue may have competitive implications for domestic airlines in terms of costs and passenger-processing times and will remain controversial until FAA develops guidelines on the specific actions foreign carriers must take to safeguard U.S. passengers.

In July 1993, FAA published new cargo security requirements for (1) airlines to identify freight forwarders with whom they do business and (2) forwarders to submit security plans by January 31, 1994, for FAA's approval. In the past, FAA's oversight of freight forwarders was frustrated because the agency did not know how many existed. Although FAA will now be able to identify freight forwarders, the success of the efforts by the agency rests on its developing an effective inspection strategy—on the basis of security plans submitted by freight forwarders—to ensure the industry's compliance.

After nearly 2 years of negotiation with FAA, USPS recently began implementing a program designed to enhance the security of airmail flown on passenger aircraft. FAA and USPS plan to conduct joint audits to monitor the effectiveness of the new measures. However, FAA officials are concerned that problems identified by the joint audits will not be adequately addressed. Because of differing institutional perspectives and the failure of a similar agreement in 1979, FAA officials believe that if the

two agencies cannot resolve problems identified in the joint audits, then the information should be reported to a third party, such as the Office of Management and Budget, that has oversight authority and the ability to resolve disputes.

FAA Can Take Steps to Improve Its Security Program

The threat to aviation in today's uncertain world requires that FAA be forward-looking in its approach to security. FAA can take several steps to improve its efforts and ensure that its security program can meet the evolving threat to aviation. For example, pilot-testing new security procedures and technology at airports could identify operational problems and save the industry millions of dollars. In 1989, FAA directed airports to install computer access systems to prevent unauthorized access to important areas. Because of concerns about time and cost, FAA did not pilot-test these systems. Consequently, industry's costs for these systems skyrocketed over FAA's initial estimates, and serious questions remain about their effectiveness. In addition, the human factors issues associated with security will require attention well into the foreseeable future. For example, FAA's continued efforts to, among others things, improve screeners' performance and enhance airport employees' awareness of security concerns have the potential to enhance security.

In addition, FAA can make better use of the wide range of security information it collects. For example, FAA collects security data in its Civil Aviation Security Information System. FAA needs to improve this system to help focus resources and identify trends before they become serious security concerns. Lastly, airport security coordinators—officials responsible for security—at category X airports do not have access to important information because they do not have security clearances. Therefore, FAA cannot tell these officials about security threats or share airport assessments with them. Providing security clearances for security coordinators at the 19 category X airports could enhance communication and engender closer cooperation between FAA and airports.

Recommendations

GAO recommends that the Secretary of Transportation direct the Administrator, FAA, to (1) develop, in conjunction with the FBI, information on threats and the individuals with the capability to carry them out for 19 category X airports and a plan to reassess the airports' security in light of this information; (2) develop guidance specifying the types of actions needed to ensure that a similar level of protection exists for U.S. citizens traveling on foreign airlines; (3) use the security plans submitted by freight

forwarders to develop a strategy to ensure compliance with the plans; (4) pilot-test new security equipment and procedures before requiring their implementation, unless threat levels or other factors warrant more rapid implementation; and (5) obtain security clearances for security coordinators at the 19 category X airports. GAO is making additional recommendations. (See chs. 2 and 3.)

Agency Comments

GAO discussed this report with senior Department of Transportation (DOT) and FAA officials, including FAA's Acting Associate Administrator for Civil Aviation Security and DOT's Director for Intelligence and Security, who generally agreed with the findings and recommendations. GAO incorporated their views where appropriate. However, FAA and DOT disagreed that airport security coordinators need security clearances and noted that airport officials receive adequate information on a routine basis. GAO finds it difficult to understand FAA's nonconcurrence with this recommendation. First, FAA recognizes this as a problem and has proposed a pilot study at two or three airports to evaluate the merits of providing clearances to airport security coordinators. Second, the Federal Security Managers and airport security coordinators with whom GAO spoke are concerned that airports are not receiving important information and strongly believe that providing security clearances for airport officials would lead to greater awareness, cooperation, and action.

Contents

Abbreviations

ATA	Air Transport Association
CASIS	Civil Aviation Security Information System
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FSM	Federal Security Manager
GAO	General Accounting Office
ICAO	International Civil Aviation Organization
RE&D	Research, Engineering, and Development
SLO	Security Liaison Officer
USPS	United States Postal Service

Introduction

On December 21, 1988, a terrorist bomb destroyed Pan Am Flight 103, killing all 259 passengers and crew aboard along with 11 residents of Lockerbie, Scotland. Since that time, remarkable geopolitical changes have occurred. The dissolution of the Soviet Union and success of the coalition forces led by the United States against Iraq in the Persian Gulf War have resulted in a lessening of global tensions. According to a recent Department of State report, international terrorism in 1992 fell to the lowest level since 1975.[1] Despite this positive trend, experts at the State Department, Central Intelligence Agency, and Federal Bureau of Investigation (FBI) stress that the terrorist threat remains quite real. It is against this backdrop that the current threat from international terrorism needs to be assessed.

Aviation Security Improvement Act Mandates Significant Changes

In the aftermath of Pan Am 103, the President's Commission on Aviation Security and Terrorism was established to examine the nation's aviation security system. The Commission issued its final report in May 1990 and concluded that the U.S. civil aviation security system was seriously flawed and failed to provide the proper level of protection for the traveling public. The Commission also concluded that the Federal Aviation Administration (FAA) had been too reactive in its approach to aviation security and ill-equipped to anticipate future threats. The Commission made 65 recommendations to improve U.S. aviation security, many of which were subsequently included in the Aviation Security Improvement Act of 1990.

The act mandated sweeping changes in FAA's and the Department of Transportation's (DOT) approach to aviation security. For example, the act mandated the following changes:

- DOT was required to establish an Office of Intelligence and Security to enhance communication, cooperation, and information sharing between DOT, FAA, and the intelligence community.
- FAA was required to establish several new positions, including the Assistant Administrator for Civil Aviation Security, to elevate security within FAA. The act also required FAA to establish Federal Security Managers (FSM) to serve as the focal points for security at the 19 category

[1]Patterns of Global Terrorism, 1992, Department of State, Apr. 1993.

X airports and Security Liaison Officers (SLO) to cover high-risk airports abroad.[2]

- FAA and the FBI were required to jointly assess the threats to and vulnerabilities of the nation's airports.
- FAA was required to review the security programs of foreign air carriers and approve those that provide a level of protection similar to that provided by U.S. carriers serving the same airport.
- FAA was required to study the need for additional measures to safeguard the transportation of cargo and mail by passenger aircraft.
- FAA was directed to support the acceleration of research to develop explosive detection equipment.[3]

(App. I provides information on FAA's response to other provisions of the act.)

The Threat to Domestic Airports Is Low, but Concerns Exist

Since the early 1970s, FAA has based its domestic security program on the assumption that hijacking by other than terrorists is the major domestic threat. Indeed, terrorist acts inside the United States are rare. In 1992, the last year that the FBI published data on the subject, the United States experienced four incidents; three involved the use of explosive or incendiary devices. None resulted in the loss of life. Table 1.1 provides information on terrorist acts inside the United States from 1987 to 1992.

Table 1.1: Terrorist Activity in the United States, 1987-92

Year	Terrorist incident	Suspected incident	Terrorist acts prevented
1987	9	8	5
1988	9	5	3
1989	4	16	7
1990	7	1	5
1991	5	1	4
1992	4	0	0
Total	**38**	**31**	**24**

Source: FBI.

[2]FAA categorizes airports on the basis of passenger volume, the complexity of airport security operations, and the level of international traffic. Category X airports are those that have a high traffic volume, have complex security operations, and generally serve as international gateways. In August 1993, FAA increased the number of category X airports from 18 to 19. All other airports are categorized as level I through level IV airports, which indicates traffic volume and complexity on a descending scale. For example, a level I airport is busier than a level II airport.

[3]We plan to report later on FAA's efforts to develop new explosive detection equipment.

According to FBI officials, networks exist for some terrorist groups inside the United States that could support terrorist activities. These networks are important because they supply the necessary equipment, logistics, training, and financial aid to potential terrorist groups. Because information on these individuals, groups, and their networks is classified, we are precluded from discussing these issues in greater detail in this report. Although FAA, airports, and airlines have taken measures to strengthen domestic security, FAA and FBI officials believe that airports and aircraft will remain an attractive target for terrorists well into the foreseeable future.

However, the terrorist threat is continually evolving and presenting unique challenges to FAA and law enforcement agencies. For example, after FAA responded to the rash of hijackings in the 1970s by deploying metal detectors at domestic airports, terrorists began to board aircraft and leave explosive devices in the aircraft via carry-on baggage at various overseas locations. Similarly, after FAA began examining carry-on baggage, terrorists were successful in placing explosive devices on board aircraft via checked baggage without actually boarding the aircraft at foreign airports. At each level, terrorists have made it more difficult for FAA and law enforcement authorities to identify the perpetrators. Because of the uncertain nature of terrorist acts, FAA and the FBI have great difficulty in assembling a long-term view of the threat to aviation security, which underscores the need to continually reassess threats to aviation.

Terrorist Threat Is Greater Overseas

FBI, State Department, FAA, DOT, and airline officials maintain that the terrorist threat is still far greater overseas. Terrorists are more comfortable operating closer to home and closer to their infrastructure. According to experts, some terrorist groups seek a high body count. To this end, civil aviation is a tempting target—but one more likely to be located in Europe rather than the United States.

State Department officials point to the terrorist threat emanating from Latin America because of both the growing animosity of so-called "drug lords" to U.S. interdiction policies and their financial wherewithal to sponsor "narco-terrorism." According to the 1992 State Department report on terrorism, the continued threat of international terrorism to Americans and U.S. interests abroad is illustrated by the fact that, while the number of terrorist incidents has declined in recent years, attacks against American targets, both in real terms and as a percentage of the total, have increased. In addition, despite official beliefs that terrorists will continue

to operate closer to home (most notably in Europe), the World Trade Center bombing in New York in February 1993 sends a signal that it is possible for terrorists to operate in the United States.

Objectives, Scope, and Methodology

At the request of the Chairman and Ranking Minority Member, Subcommittee on Transportation and Related Agencies, Senate Committee on Appropriations, and the Chairman and Ranking Minority Member, Subcommittee on Transportation and Related Agencies, House Committee on Appropriations, we examined FAA's implementation of the Aviation Security Improvement Act of 1990. Specifically, we focused our efforts on (1) the FAA-FBI joint vulnerability assessments of the nation's category X airports, (2) FAA's efforts to determine if a similar level of protection exists for U.S. passengers traveling to or from the United States on foreign airlines, and (3) FAA's efforts to safeguard mail and cargo. In addition, we were asked to identify additional steps that FAA could take to improve its security program.

We reviewed the Aviation Security Improvement Act and Foreign Airport Security Act of 1985 as well as numerous FAA security regulations pertaining to air carriers and airports. In addition, we reviewed a number of FAA's security strategy papers and reports, including FAA-FBI airport vulnerability assessments, the draft Strategy for Civil Aviation Security, as well as the Report to Congress on the Security of Mail and Cargo in Transportation by Passenger Carrying Aircraft. Moreover, we followed up on some issues discussed in our prior aviation security reports.[4] We coordinated our work with DOT's Inspector General.

To gain a general understanding of the terrorist threat that challenges FAA's security program, we interviewed counterterrorism experts at the State Department, the FBI, and the Central Intelligence Agency, and a private security consultant. We also discussed this issue with FAA officials responsible for analyzing information from the U.S. intelligence community. In addition, we reviewed various reports and studies prepared by these agencies. We did not validate the threat estimates or the effectiveness of information sharing between FAA and the U.S. intelligence

[4]Aviation Security: Training Standards Needed for Extra Security Measures at Foreign Airports (GAO/RCED-90-66, Dec. 15, 1989); Aviation Security: FAA's Assessments of Foreign Airports (GAO/RCED-89-45, Dec. 7, 1988); Aviation Security: Corrective Actions Underway, but Better Inspection Guidance Still Needed (GAO/RCED-88-160, Aug. 23, 1988); Aviation Security: Improved Controls Needed to Prevent Unauthorized Access at Key Airports (GAO/RCED-88-86, Jan. 29, 1988); and Aviation Security: FAA Needs Preboard Passenger Screening Performance Standards (GAO/RCED-87-182, July 24, 1987).

community. Because some of this information is classified, we are precluded from discussing it in this report.

We also met with officials from Northwest and American airlines and officials from Detroit, Dallas/Fort Worth, Dulles, and National airports concerning various aspects of the act. We toured several category X domestic airports, observed airport security screeners and airline procedures, and interviewed FSMs and airport security officials at those airports.

In addition, to determine the usefulness of the joint FAA-FBI vulnerability assessments, we examined the assessment reports for 18 of the 19 category X domestic airports. FAA designated one airport as a category X airport in August 1993. As a result, we did not include that airport in our review. We interviewed DOT's former Director of Intelligence and Security, FAA's former Assistant Administrator for Civil Aviation Security, FAA's Director of the Office of Intelligence, and the FBI's Chief for Counterterrorism to obtain their views on the assessments. We also discussed the assessments and potential airport vulnerabilities with FSMs at several category X airports.

In assessing FAA's effort to determine if a similar level of protection is provided by foreign carriers, we analyzed selected inspections of such carriers at various overseas locations and weekly reports from SLOs. We also discussed this issue with knowledgeable officials from FAA's (1) Office of Civil Aviation Security Policy and Planning, (2) Office of Intelligence, and (3) International Liaison Staff. We obtained information on FAA's approach and methodology for determining if a similar level of protection exists but did not validate the approach. Some of the information used in this analysis is classified; therefore, we are precluded from discussing it in this report. To obtain industry's views, we spoke with several airline officials that are responsible for security as well as officials from the Air Transport Association (ATA).

We also analyzed FAA's and the United States Postal Service's (USPS) plans and procedures to determine FAA's efforts to safeguard mail and cargo. In addition, we interviewed DOT, FAA, USPS, and airline officials and observed mail and cargo operations at one category X domestic airport. Furthermore, we discussed FAA's new requirements with the American Association of Airport Executives, Airforwarders Association, and Air Cargo Management Group.

In addition, we discussed current and future challenges facing FAA with DOT, FAA, and airline officials and obtained information on FAA's research efforts to develop new security technology and future work to meet long-term security needs. We also assessed FAA's ability to focus its resources and identify emerging issues by obtaining and independently analyzing data from the Civil Aviation Security Information System (CASIS). CASIS contains a wide range of aviation security information ranging from bomb threats to domestic airport assessments.

We discussed our findings and recommendations with FAA's Acting Associate Administrator for Civil Aviation Security, the Director of Aviation Planning and Policy for Civil Aviation Security, the Director of the Office of Intelligence for Civil Aviation Security, and the Director and Deputy Director of DOT's Office of Intelligence and Security. We also discussed our results with the FBI's Chief for Counterterrorism, officials in the State Department's Office of the Coordinator for Counterterrorism, and officials in USPS' Office of Criminal Investigations, Prevention and Countermeasures Branch. These officials generally agreed with our findings; their comments have been incorporated as appropriate. As requested, we did not obtain written agency comments on a draft of this report. Our work was conducted between July 1992 and September 1993 in accordance with generally accepted government auditing standards.

FAA Has Made Progress in Implementing the Act, but Important Actions Need to Be Taken

FAA has taken important steps to address some of the act's domestic and international requirements. FAA has established FSMs at category X domestic airports and SLOs at high-threat foreign airports. However, serious concerns exist about several important FAA efforts to comply with the act. For example, the joint FAA-FBI assessments of 18 of the 19 domestic category X airports did not explore the critical relationship between airports' vulnerabilities and known terrorist groups, their methods, or intent.[1] In addition, U.S. carriers are concerned about the safety and competitive implications of differences between U.S. and foreign security requirements. Furthermore, the success of FAA's efforts to bolster cargo security will depend on the development of an inspection strategy to ensure that freight forwarders—entities that consolidate cargo and buy space on commercial aircraft—comply with new regulations. Finally, FAA is concerned that USPS will not follow through on a security cooperative agreement unless monitored by a third party.

FAA Has Taken Steps to Respond to the Act

FAA has taken important steps to respond to the act. Two noteworthy accomplishments were the establishment of FSMs and SLOs at domestic and overseas airports. FAA, DOT, and industry officials with whom we spoke believe that FSMs and SLOs have enhanced security both at home and abroad. FAA has made some progress with other aspects of the act. For example, FAA has published standards for the employment and training of airport screeners, issued cargo security rules, published airport design and construction guidelines, and accelerated research efforts to develop explosive detection equipment. (App. I provides information on FAA's response to the act's key provisions.)

FSMs are in place at the 19 category X airports. FSMs serve as the primary FAA representatives dealing with airport managers, airport tenants, law enforcement agencies, and other federal agencies for aviation security. FSMs are responsible for, among other things, (1) receiving intelligence information, (2) assisting in the development of comprehensive airport security plans, and (3) serving as the on-site coordinator for terrorist threats and incidents. FSMs view themselves as problem solvers rather than traditional FAA security inspectors.

FAA has 17 SLOs in place throughout the world to ensure greater cooperation between U.S. carriers, foreign air carriers, and foreign governments. These individuals are particularly important because they

[1]In August 1993, at the end of our review, FAA designated an additional airport as category X. As a result, we did not include that airport in our review.

frequently assist U.S. carriers by negotiating with foreign aviation authorities to satisfy the security requirements of FAA and the host country. Although the act required FAA to establish SLOs, the agency had begun placing some SLOs overseas prior to the act's passage. SLOs receive threat information and share it with the United States and host countries as well as promote consistency between FAA's and host countries' security requirements. Because of FAA's heavy workloads and difficulty of finding staff with the necessary expertise, we testified that FAA may experience difficulties in finding qualified candidates to staff some SLO positions in the future.[2]

FAA-FBI Joint Assessments Are a Good First Step, but Concerns Remain

Vulnerability assessments of domestic category X airports are important to ensure that current policies, procedures, and technologies can provide effective security for the traveling public. Although the joint FAA-FBI assessments provide valuable information on the security of the nation's airports and reinforce the need for many of FAA's actions, our review of the assessments and discussions with DOT and FAA officials as well as several FSMs highlighted several concerns.

The Aviation Security Improvement Act of 1990 required FAA to assess the domestic air transportation system with the FBI. Specifically, the act states that

"such assessment shall include the consideration of the extent to which there are individuals with the capability and intent to carry out terrorist and related unlawful acts against the domestic aviation system and the methods by which such individuals might carry-out such acts."

Also, the President's Commission on Aviation Security and Terrorism noted that potential vulnerabilities exist at the nation's airports and viewed joint FAA-FBI assessments as a vehicle to design security systems. In 1988, we reported that weaknesses at category X airports could result in unauthorized access to important airport areas.[3] According to FAA, unauthorized access—including access by a vehicle—continues to be a concern at category X domestic airports.

Since early 1990, FAA and the FBI have assessed 18 of the 19 category X airports and 10 other domestic airports that have high traffic levels and

[2]FAA Work Forces: Important Decisions Affecting Staff Use and Management (GAO/T-RCED-93-59, June 30, 1993).

[3]Aviation Security: Corrective Actions Underway, but Better Inspection Guidance Still Needed (GAO/RCED-88-160, Aug. 23, 1988).

complex security operations. The assessments examined, among other things, (1) the security of checked baggage, mail, and cargo; (2) space requirements for security personnel and equipment; (3) separation of screened and unscreened passengers; and (4) coordination between FAA, law enforcement, and industry security personnel. FAA and the FBI completed 18 category X airport assessments early in 1992. The assessments reinforced the need for continuing many of FAA's current policies. For example, the assessments reinforced the need for new explosive detection devices, passenger bag-matching procedures (to ensure that luggage is not loaded onto an aircraft unless the passenger boards the aircraft) for international flights, and better security screening and more realistic testing of screeners. (Ch. 3 discusses screeners' performance.)

The assessments also noted several problems identified by the President's Commission that continue to affect airport security. The Commission raised concerns about screeners' efficiency, mail and cargo, and the coordination of security between law enforcement and airport personnel. At the category X airports, the FAA-FBI assessments found that the turnover rate among screeners remains high and training is inadequate. For example, at 16 category X airports, screeners' turnover rate was in excess of 50 percent, and screeners themselves noted that they needed better and more frequent training. In addition, the assessments found that some airline employees do not consistently apply FAA's cargo security standards, especially for accepting and inspecting packages. Furthermore, the assessment teams noted that coordination between airport security and law enforcement officials could be improved.

According to FAA and FBI officials, most, if not all, of the concerns identified by the assessments are being addressed by FAA or the respective airports. For example, FAA is developing new explosive detection equipment, has initiated a rulemaking to increase on-the-job training for screeners, and is developing more realistic test objects for screeners.

Concerns About Joint Assessments in Assessing Domestic Airport Security

The joint assessments are a positive step in examining domestic airports and represent the first structured effort between FAA and the FBI to examine airport security. Assessments that match known airport vulnerabilities with threat groups and their capabilities in an innovative way can be useful in shaping aviation security. As the World Trade Center bombing reminds us, the United States is not immune to terrorist acts inside its borders. Our review of the reports for 18 category X airports and

discussions with top-level DOT, FAA, and FBI officials as well as several FSMs identified several concerns.

- First, the assessments did not address the wide range of current and potential threats to civil aviation. For example, FAA and the FBI examined the vulnerability of checked baggage, mail, and cargo but did not explore the possibility that sophisticated weapons—such as surface-to-air missiles—could be used at a domestic airport.[4] DOT and FAA officials believe that the use of such sophisticated weapons needs to be explored and factored into airport contingency plans. Moreover, the assessments did not examine the wide range of methods by which a terrorist could attack an airport. FAA and the FBI examined the physical layout of an airport and the perimeter's security but did not generally view an airport and its vulnerabilities from a terrorist's perspective. For example, one airport has a river close to an active runway. The assessment noted the vulnerability but did not explore how this weakness could be exploited by a potential threat group or how this vulnerability posed a risk to departing and arriving aircraft. At another category X airport, an FSM showed us several locations that were not mentioned in the assessment report where aircraft are vulnerable to well-armed potential threat groups.
- Second, the assessments did not match vulnerabilities with the capabilities and intent of known high-threat groups in the United States or located near airports. According to DOT and FAA intelligence officials, a sound assessment not only determines the vulnerabilities that exist but also the capabilities and intent of potential actors. They also noted that such information is critically important to ensure that both FAA and airport contingency plans address potential threats.[5] Furthermore, without matching vulnerabilities with known threat groups, their methods, and intent, FAA and the FBI cannot assess the threat nationwide. The former Director of DOT's Office of Intelligence and Security and the former FAA Assistant Administrator for Aviation Security acknowledged this weakness in the assessments and noted that several potentially hostile groups are located near category X airports. FAA officials caution, however, that terrorists often do not attack locations close to their own base.
- Third, not all 18 category X airports received the same level of attention from FAA and the FBI. Six of the category X airports were assessed by both FAA and FBI specialists, including explosive detection experts; 12 were assessed by FBI and FAA regional staff using a standardized assessment

[4]A January 1992 report by the Office of Technology Assessment discussed sophisticated methods that could be used by terrorists (Technology Against Terrorism: Structuring Security).

[5]Contingency plans outline additional steps that FAA and the industry can take to meet increased threats. For example, during the Gulf War, FAA prohibited the use of curbside baggage check-in.

protocol or checklist. At one airport we visited, the assessment was largely conducted by the FSM with little input from the FBI. According to the FSM, he could not draw on the FBI's expertise and experience when assessing the airport because the FBI agent was not available. Also, FAA has a small staff that helps airport personnel identify explosives and provides advice to them on actions to take if a device is found and how to safeguard vulnerable areas. This staff did not participate in the assessments.

FAA and the FBI recognize these weaknesses and attribute them to several factors. First, FAA and the FBI were not experienced in conducting such assessments. Although the FBI is knowledgeable about criminal acts and terrorist groups operating in the United States, FAA and FBI officials told us that FBI field agents were not intimately familiar with airport and air carrier operations. Similarly, FAA participants had not previously viewed airport security from a threat assessment perspective, which goes beyond industry's compliance.

Although the act states that FAA and the FBI shall periodically assess and analyze threats to the domestic air transport system, whether the two agencies will continue to assess individual airports is uncertain. FAA and FBI officials told us they had not determined when and if the category X airports will be reassessed. FBI officials are not optimistic about doing so and expressed concern about the resources required to do the assessments. Currently, FAA and the FBI are assessing level I airports. These airports have a high level of traffic, but unlike category X airports, they are not all international gateways. FAA has identified over 50 level I airports. Neither FAA nor FBI officials have determined whether the agencies will assess all of these airports or a select few.

FAA Has Made Limited Progress in Determining If a Similar Level of Protection Exists for Passengers Traveling Overseas

The safety and security of U.S. citizens traveling overseas has long been a concern of the Congress, FAA, and the aviation community. A particular concern over the past several years has been whether foreign carriers provide U.S. citizens with a level of protection similar to that provided by U.S. carriers. Most foreign carriers comply with international security standards that are less stringent than FAA's requirements for domestic carriers. According to FAA, even when no significant threat exists to foreign carriers, U.S. carriers serving the same foreign destination must comply with more stringent requirements. As a result, ATA officials believe that domestic carriers are at a competitive disadvantage at many foreign airports.

Each year, thousands of U.S. citizens travel overseas, and almost 50 percent travel via foreign carriers. Because of differing security requirements for foreign and domestic carriers, U.S. citizens traveling via foreign carriers—about 13.8 million in 1991—may not be receiving the same level of protection that would be afforded by a U.S. carrier serving the same airport. This is important because, according to the Department of State, although terrorist incidents have decreased over the past few years, the attacks against U.S. targets and businesses overseas have increased. Furthermore, according to FAA, the majority of criminal acts against aviation over the past several years have taken place outside of the United States.

Part 129 of the Federal Aviation Regulations governs the operation of foreign carriers that hold an operating permit issued by DOT. In 1989, FAA revised its regulations to require foreign carriers that fly to or from the United States to submit their security programs to FAA for review and acceptance. In essence, the regulations required foreign carriers to adopt certain security procedures for each point of operation in the United States and for the last point of departure into the United States. To facilitate the adoption of the new procedures, FAA offered foreign carriers a model security program based on the International Civil Aviation Organization's (ICAO) standards.[6] ICAO's standards provide carriers with a general minimum framework for security and do not, for example, require passenger profiling (interviewing) or the X-raying of all baggage at specific airports where additional security is warranted. In contrast, FAA's requirements for U.S. carriers are more stringent and require passenger profiling and the X-raying of all baggage. According to FAA officials, most of the 161 foreign carriers that FAA has identified adopted the model program.

The Aviation Security Improvement Act confirmed the need for this program and introduced the concept of a similar level of protection. The act permits FAA to accept a foreign carrier's security program only if FAA determines that the program provides a level of protection similar to that provided by U.S. carriers serving the same airports. At extraordinary

[6]ICAO has developed and adopted 18 technical annexes involving such varied fields as security, airworthiness, and aeronautical communications. ICAO's annexes contain standards that member countries must meet and that are intended to produce a degree of technical uniformity that enables international civil aviation to function in a safe, orderly, and efficient manner. ICAO's standards represent the minimum that each country and carrier must meet. ICAO has no enforcement mechanism.

airports, the act allows FAA to require that foreign carriers use procedures equivalent to FAA's.[7]

Important Questions Remain About FAA's Efforts to Determine Similarity

Since the passage of the act, FAA has struggled with implementing a means for ensuring that foreign carriers provide a similar level of protection. According to FAA officials, they are examining threats and vulnerabilities to determine if a foreign carrier faces a particular risk at a specific airport. FAA focuses its attention on a foreign carrier's last point of departure before entering the United States. Because the terrorist threat varies significantly from region to region and airport to airport, a foreign carrier's security program may suffice at one, but not another, location. Therefore, FAA must not only accept a foreign carrier's program but also recommend specific modifications for each location that is served by that carrier on the basis of historical patterns of terrorist activity and the foreign carriers' security programs—including both procedures and equipment—for specific airports. FAA's analysis could show that, since a foreign carrier faced no significant threat at a particular airport, less stringent international standards would suffice, while a U.S. carrier, serving the same airport, must maintain a higher level of security.

FAA officials acknowledge that deciding whether a foreign carrier provides a similar level of protection is difficult. Moreover, FAA officials told us that comparing different threats, procedures, and countermeasures with standards for U.S. carriers requires a careful marriage of operational and intelligence information. FAA has struggled to develop an approach and has decided to focus on threats to a carrier at specific locations instead of a strict comparison of U.S. and foreign carriers' security programs. Although FAA has developed a general approach to examine threats to and vulnerabilities of foreign carriers at specific airports, it has not issued FAA orders or advisory circulars for the industry or FAA staff to interpret how a similar level of protection will be determined, enforced, or achieved.

To assist in determining if a similar level of protection exists, FAA has developed an analytical model to examine foreign carriers on the basis of threat and vulnerability. We discussed this model and the data it uses with FAA, but we did not validate or test its usefulness. The approach relies heavily on threat information from the U.S. intelligence community; the results are classified and, hence, cannot be incorporated into this report. On the basis of their analysis, FAA officials told us that they can determine

[7]Extraordinary airports are high-risk foreign airports. At these airports, U.S. carriers are required to take additional actions, such as profiling, to ensure the safety and security of passengers. FAA has designated over 50 foreign airports as extraordinary.

if minimum standards—based on ICAO's standards—will suffice at various locations. If minimum standards cannot suffice, FAA plans to work with the carrier or foreign government to bring about security improvements.

FAA has completed developing its model and threat assessments for individual carriers. However, as of November 1993, FAA had not started to work with foreign carriers to bring about needed improvements or determined the additional countermeasures that individual carriers will be asked to adopt. These actions will require additional FAA analysis and close cooperation with foreign carriers and their governments. FAA officials believe that some foreign carriers will resist efforts to change their policies and procedures. More importantly, FAA officials told us that several issues—including diplomatic sensitivities and the manner in which disagreements regarding the need for additional countermeasures will be resolved—need to be addressed. According to FAA officials, bilateral discussions with foreign governments will be conducted in coordination with the Department of State and some issues and sensitivities will be unique to individual countries or airports.

Nevertheless, FAA officials believe that most foreign carriers are generally providing a similar level of protection. FAA officials estimate that a small percentage of all foreign carriers will need to implement additional measures to provide a similar level of protection. FAA officials base this view largely on insights obtained from foreign carriers' operations through the foreign airport assessment program, SLOs, and a review of foreign carriers' security programs.[8]

Airline security experts from several U.S. carriers do not believe that a similar level of protection exists for U.S. citizens traveling on foreign airlines. They are concerned about the security provided by several carriers in Europe as well as some carriers from developing nations at select airports around the world. They believe that FAA should require foreign carriers to provide an identical—not similar—level of protection at particular airports. They believe that FAA should adopt airport-specific requirements that combine host nations' measures with FAA's requirements to ensure that security functions are identical for both U.S and foreign carriers.

[8]FAA's foreign airport assessment program examines security at certain airports to ensure that they meet minimum security requirements.

FAA Will Continue to Face Significant Challenges in Determining Similarity

FAA faces significant challenges in determining whether a similar level of protection is provided by foreign carriers because the global security framework is marked by different approaches, priorities, and changing conditions. Moreover, some foreign governments, most notably the Western European and Pacific Rim nations, have not been willing to share some security information with FAA and, according to agency officials, resent FAA for attempting to exert control over their carriers.

Although the carriers themselves have been willing to cooperate with FAA while operating in the United States, foreign governments have not always been forthcoming in granting FAA access to carriers' operations at their airports. Furthermore, many functions that are generally carried out by U.S. airlines, such as passenger screening, are the responsibility of the host government. If additional information on security procedures or equipment is needed, a foreign carrier refers FAA to the host government. According to FAA officials, their determining if a similar level of protection exists requires constant analysis and updating because of the changing nature of the terrorist threat and because foreign carriers may implement procedures for a limited time to meet a perceived threat and then relax security when the threat subsides.

Since the act's passage, FAA has begun inspecting foreign carriers at the point of last departure before entering the United States. The inspections examine, among other things, passenger and baggage screening procedures as well as procedures for guarding aircraft. FAA officials explained that these inspections alone cannot determine if a similar level of protection exists but do provide valuable information on a carrier's operations. FAA officials caution that their inspections are only a snapshot and, therefore, only capture a carrier's security at a specific time. FAA has inspected a little over half of the 161 foreign carriers it has identified worldwide. (App. II provides information on inspections of foreign carriers.) According to FAA, the inspections indicate that most foreign carriers are meeting minimum ICAO security standards. More importantly, FAA officials told us that most carriers have instituted positive bag-matching procedures.

Despite FAA's positive findings, our examination of selected inspections of foreign carriers and discussions with FAA and DOT officials identified several concerns. First, FAA has had little success in inspecting carriers in one of the highest threat regions—Western Europe. Since Western European governments are in many cases responsible for performing security functions (functions that would be performed by carriers in the

United States), sovereignty issues have impeded FAA's ability to inspect carriers from those countries. In contrast, FAA officials told us that they have had success in inspecting foreign carriers from developing nations. According to FAA officials, many developing nations view the inspection as a means of joining the growing international aviation community.

Second, FAA classifies its inspection findings as satisfactory or unsatisfactory but does not examine a foreign carrier's security program in detail. Although FAA determines whether a foreign carrier performs a procedure, such as positive bag matching, it does not determine the procedure's effectiveness or how well it is implemented or note potential weaknesses. Similarly, the inspections do not differentiate among or assess the effectiveness of security programs as a whole. For example, two carriers with markedly different security procedures and philosophies and facing different threats received satisfactory marks from FAA inspectors. FAA officials told us that, in January 1993, the agency implemented new procedures requiring inspectors to prepare detailed narratives on foreign carriers' procedures and their effectiveness.

Third, the inspections are based primarily on ICAO's standards. As the President's Commission pointed out, ICAO has some inherent limitations. For example, ICAO's security standards are based on the least common denominator and do not adequately address threats at some airports. In high-threat countries, carriers rely on additional measures that the inspections do not examine, such as controls over the transfer of baggage from one airline to another and enhanced passenger profiling. Cost is an issue because many countries cannot afford higher levels of security. Another weakness, according to the Commission, is that ICAO has no enforcement mechanism; it cannot impose sanctions on a member that violates the standards.

Last, FAA has not placed a high priority on inspecting foreign carriers. In November 1992, DOT's Office of Intelligence and Security evaluated FAA's efforts at one foreign location and found, among other things, that FAA was not inspecting foreign carriers in Western Europe. The evaluation noted

"Probably the biggest surprise of all was the fact that the [FAA inspection] team did not inspect the foreign air carriers that were operating at the airport, and the airport was the last point of departure for a few foreign air carriers [to the United States]. The team leader advised that the region does not have a program to do that."

This raises questions about FAA's efforts to determine if a similar level of protection exists. FAA officials acknowledge these issues but point out that they have a program to inspect foreign carriers. However, because of sovereignty issues, FAA has not inspected foreign carriers at certain locations; FAA officials believe the foreign airport assessment program provides sufficient information on those foreign carriers' security programs.[9] Moreover, FAA believes more detailed inspection of foreign carriers may jeopardize relationships with the carriers and their governments. FAA believes that working closely with foreign governments and conducting joint inspections is the prudent course of action.

Similar Level of Protection May Have Competitive Implications

U.S. carriers assert that differences between security requirements for U.S. and foreign carriers have competitive implications. Airline officials with whom we met said that this was a major issue that FAA needs to address. Because FAA requires more stringent regulations—including passenger profiling—for U.S. carriers operating from foreign airports, industry officials believe they are at a competitive disadvantage.[10] Airline officials told us that more stringent FAA requirements result in increased costs and longer passenger-processing times. Moreover, because of the differences in U.S. and foreign approaches to security, airline officials believe that the concept of "similar level of protection" is much too broad for FAA to assess and make a determination about the security of U.S. passengers traveling on foreign airlines.

Domestic airlines argue that they are taking important steps that their European counterparts are not. Domestic carriers argue that they are losing full-fare business travelers—lucrative passengers for U.S. airlines—who are not willing to wait in check-in lines or to arrive at airports 2 hours ahead of schedule to pass screening. This effect is difficult to measure, and airline officials with whom we spoke could not provide us with data indicating that they are at a competitive disadvantage. In 1990, DOT examined this issue and found that it could not conclude whether U.S. carriers were at a competitive disadvantage. According to agency officials, FAA allowed U.S. carriers in 1985 to assess a security surcharge against passengers to help offset the costs of security. However, according to ATA officials, U.S. carriers have not been assessing a security surcharge against passengers for competitive reasons.

[9]We did not examine the foreign airport assessment program.

[10]Most foreign carriers do not profile passengers.

In a January 1992 report, the Office of Technology Assessment raised concern about differing requirements for U.S and foreign carriers—most notably passenger profiling—and its competitive implications. The report pointed out that most foreign carriers are state-supported and find it easier to pay for security measures. Also, the report noted that

"U.S. carriers do not have this luxury, and, for small competitive margins, the added cost of security may be a serious handicap to the ability of U.S. carriers to compete successfully."

FAA officials recognize that differences exist in requirements for U.S. and foreign carriers but do not believe that U.S. carriers are at a competitive disadvantage. However, FAA has not studied the issue and could not provide documentation to support this position.

FAA's Response to Mail and Cargo Needs an Effective Strategy to Ensure Success

FAA has taken several steps to enhance security for cargo and airmail. As required, FAA studied the need for additional security measures, including enhanced screening procedures for mail and cargo.[11] Because of significant disagreements between it and USPS, FAA issued its study over 1 year after the statutory deadline. In its report, FAA identified the need for better oversight of freight forwarders—entities that consolidate between 60 and 90 percent of all air cargo flown on passenger aircraft. In addition, FAA and USPS are developing an agreement in which USPS is taking certain measures to improve the security of mail flown on passenger aircraft.[12] FAA and USPS acknowledge, however, that a similar program in 1979 was not implemented and essentially forgotten and that no effort was made to ensure its success. FAA and USPS plan to conduct joint audits to monitor the implementation of the new agreement, but FAA has concerns about how problems identified by the audits will be resolved.

President's Commission Identified Mail and Cargo as Presenting Huge Security Gap

The President's Commission on Aviation Security and Terrorism identified mail and cargo operations as presenting "a huge gap in the security umbrella for domestic and international flights." The Commission concluded that FAA's oversight of freight forwarders was inadequate because FAA could not even identify most of the forwarders. The Commission recommended that FAA's regulatory program governing

[11]Report to Congress on the Security of Mail and Cargo in Transportation by Passenger Carrying Aircraft, FAA, Aug. 1992.

[12]FAA also has efforts underway with the U.S. Customs Service and the Department of Defense for international and military mail, respectively. For purposes of this report, we limited our analysis to FAA's and USPS' domestic activities.

freight forwarders be replaced and that FAA concentrate its cargo security efforts on air carriers' cargo operations at airports.

The Commission also made recommendations to improve airmail security. It called on USPS to redefine the category of mail that is "sealed against inspection," thus removing legal obstacles to screening (X-raying) such mail. The Commission recommended that mail be screened at certain category X airports and at other airports when a credible threat has been identified. In addition, it recommended that airlines, not USPS, be responsible for screening mail because they already have the operational technology to screen mail along with checked baggage. The Commission urged that mail screening be implemented in stages: first, screening would be implemented at airports with extraordinary security measures in place and at other airports when warranted by an identified threat, then screening would be phased in for all U.S. international flights, and eventually screening would be implemented for all nonletter mail on those flights for which checked baggage is screened.

The Aviation Security Improvement Act required FAA to determine if additional security requirements are needed for the transportation of mail and cargo by passenger aircraft. In conducting its study, FAA was required to consult with USPS and other interested parties in considering several factors including the (1) extent to which it is practicable to require that mail and cargo be screened in the manner required for checked baggage, (2) constitutional limitations on the authority of the U.S. government to screen mail, (3) use of inspection procedures specific to mail and cargo, and (4) desirability of not unduly delaying the delivery of mail and cargo. The act required FAA to issue a report to the Congress by May 15, 1991; FAA did so in August 1992.

The screening of mail has been and will likely continue to be controversial. As originally introduced, the act would have required the Postmaster General to issue regulations modifying the definition of mail "sealed against inspection" to exclude those parcels capable of containing explosives that can cause catastrophic damage to commercial aircraft. This bill would also have permitted air carriers to screen such mail when directed by FAA to do so. This version of the bill was not enacted, however, because according to FAA and USPS officials, the economic impact on the industry from such new requirements was not known. FAA was instead required to study such issues as mail reclassification and screening and report to the Congress on the best course of action.

FAA Initiates Changes to Improve Cargo and Mail Security

To improve cargo security, in July 1993, FAA issued requirements for air carriers to notify the freight forwarders with which they do business of their responsibility to implement an FAA model security program by January 31, 1994. Freight forwarders are required to respond by notifying FAA regional offices, which will then provide the forwarders with the model program. The carriers will be required to screen cargo from forwarders that fail to implement the FAA model security program. Additionally, FAA officials believe that requiring freight forwarders to provide a written certification to the carriers that all cargo security requirements have been met will heighten security awareness and give FAA a greater ability to identify and oversee freight forwarders.

Freight forwarders remain an elusive part of the aviation industry. Even though freight forwarder security regulations have existed since 1979, FAA acknowledged in its report that it does not know the identity of most freight forwarders. Although the President's Commission estimated that between 4,000 and 6,000 freight forwarders could be in business at any given time, FAA estimated that the actual number is closer to 1,200 and that the top 20 companies have 80 percent of the market. Freight forwarders were formerly certified by the now-defunct Civil Aeronautics Board. When the Board went out of existence, this oversight was lost. The last Board listing in 1978 included about 1,600 freight forwarders. Since then, FAA has made no systematic effort to track or identify freight forwarders.

With regard to mail, FAA concluded that the threat to civil aviation from the transportation of mail was as serious as that from either checked baggage or cargo. FAA noted that certain legal restrictions against inspecting mail, the lack of commercial processing standards, and a history of letter bombs

"combine to present vulnerabilities to civil aviation security at least as great as other aspects of aviation operations. The capability to use mail to transmit bombs which can activate on aircraft has been demonstrated."

Since 1970, mail has been used to introduce explosive devices onto commercial passenger aircraft on at least four occasions as table 2.1 indicates.

Table 2.1: Bombings of Commercial Aircraft Via Mail, 1970-92

Date	Airline	Flight plan	Casualties
Feb. 21, 1970	Austrian Airlines	Frankfurt-Vienna	None
Feb. 21, 1970	Swiss Air	Zurich-Tel Aviv	47 killed
Apr. 3, 1979	Lufthansa	Frankfurt-Tel Aviv	10 injured
Nov. 15, 1979	American Airlines	Chicago-Washington	None

Source: FAA.

Agreeing with the President's Commission, FAA urged USPS to reclassify mail that is "sealed against inspection" to allow for the screening of air parcels. USPS strongly disagreed with this approach for several reasons. First, USPS argued that mail reclassification is something that only the Congress can do. It is not, in USPS' view, within the agency's administrative domain to reclassify mail as FAA and the President's Commission have argued. Second, USPS was concerned that the security benefits resulting from the application of current screening technology would not outweigh the technological and operational costs for USPS. Lastly, USPS argued that the Fourth Amendment of the U.S. Constitution extends the same protections of privacy to mail as it does to peoples' homes.[13]

The FAA-USPS negotiation over mail screening lasted over a year and caused the FAA report to be delayed. FAA and USPS are developing a compromise airmail security program, and USPS has instituted some new procedures even though the agreement has not been signed by both agencies. Because of security concerns, the procedural details of the agreement are confidential and cannot be described in this report.

Differing institutional perspectives and distrust over an earlier agreement have strained FAA's and USPS' relationship. In 1979, after an explosive device in the mail detonated aboard an American Airlines flight, FAA and USPS entered into an agreement that established a "Parcel Mail Security Program." The program required USPS to "profile" mail originating in 40 different cities and divert suspicious items to surface transportation. But FAA and USPS officials acknowledge that neither agency implemented the provisions pursuant to their portion of the agreement and that the 1979 agreement was largely a failure.

[13]USPS acknowledges a distinction between the use of X-rays, which actually penetrate a parcel and other such explosive detection methods as using canines that detect particles being emitted from a parcel—the latter being considered constitutional.

Concerns Raised About Oversight of Cargo and Mail Requirements

Although FAA has strengthened its cargo security regulations, the success of the program will depend on the development of an effective inspection strategy to ensure that freight forwarders comply with their FAA-approved security plans. Similarly, FAA's and USPS' lack of success in implementing security procedures in 1979 and recent disagreements between the two agencies raise concerns about the successful implementation of the current agreement.

FAA regional offices will enforce the new cargo requirements through the review of freight forwarders' security plans submitted to them. Although acknowledging that they have not enforced the security regulations that have governed freight forwarders since 1979, FAA officials believe that the new and more explicit procedures that both carriers and forwarders will be required to follow give FAA greater administrative control over forwarders. In effect, requiring freight forwarders to provide a security certification to carriers creates an administrative procedure for FAA to audit. Although FAA plans to conduct random inspections of air carriers' and freight forwarders' facilities, the agency has not decided upon a strategy that outlines the frequency or rigor of these inspections. Without an effective inspection strategy, FAA cannot close the security gap identified by the Commission.

One inspection approach being considered is to combine hazardous material and security inspections. If FAA adopts this approach, it has to become much more aggressive in its oversight of both programs. For example, in fiscal year 1992, FAA inspected only 1 freight forwarder for hazardous material compliance out of a total of about 6,415 air carrier inspections for hazardous material. The lack of effective inspection efforts prompted the Aviation Security Advisory Committee to warn that, without a strong compliance and enforcement program, FAA's regulatory oversight of freight forwarders will continue to be ineffective.[14]

FAA has conducted security inspections of air carriers' cargo facilities located at airports but not freight forwarders' facilities "upstream"—those located closer to the origination of cargo. Until now, according to FAA officials, the large number of freight forwarders has made an inspection program problematic. But the new requirements, by making it easier for FAA to identify forwarders, should also make it easier for FAA to inspect them. However, an inspection strategy—a critical component of the program's success—has not been developed by FAA.

[14]The Aviation Security Advisory Committee, composed of representatives from industry and various government agencies, meets quarterly and advises FAA on a wide range of security matters.

The proposed FAA-USPS agreement to safeguard mail contains general provisions calling for joint programmatic audits to monitor compliance and effectiveness. In fact, USPS has already begun to audit the program, and FAA is expected to participate in subsequent audits. But FAA officials told us they are concerned that problems identified in the joint audits will not be adequately addressed. Because of differing institutional perspectives and the failure of a past agreement, FAA officials believe that if the two agencies cannot resolve problems identified in the joint audits, then such information should be reported to a third party that has oversight authority and the ability to resolve disputes to ensure USPS' implementation. USPS officials do not object to reporting to a third party but do not believe it is necessary at this time. FAA officials told us that the Office of Management and Budget would be an acceptable third party.

Conclusions

FAA has taken steps to respond to the Aviation Security Improvement Act, such as completing many of the organizational, personnel, and administrative requirements of the act. FAA has made progress in assessing category X airports and ensuring the security of mail and cargo carried on passenger aircraft. FAA has started to determine if a similar level of protection exists for U.S. citizens traveling on foreign airlines. However, in each of these efforts, additional steps need to be taken, and careful oversight of these initiatives is warranted.

The joint FAA-FBI assessments offer FAA a vehicle to gain valuable insights into the security of domestic airports and determine the overall effectiveness of airport security measures. Moreover, the assessments confirm the need for many of FAA's current procedures and policies, such as positive bag matching for international flights and new explosive detection equipment. However, the assessments did not analyze potential airport threats and the ability and intent of known threat groups to carry them out. Without information that matches vulnerabilities, known threats, and intentions, FAA cannot be assured that current technology and procedures are working as intended. Although the act calls for further assessments, it is not clear when or if they will be carried out.

A careful examination of foreign carriers' security programs and threats at specific airports would provide FAA with a better understanding of threats facing U.S. citizens traveling overseas. Currently, a disparity exists between standards for U.S. and foreign carriers serving the same foreign airport. This is important because, according to the State Department and FAA, some foreign carriers are facing threats equal to or greater than those

facing U.S. carriers. Similarly, U.S. carriers are concerned that differing requirements place them at a competitive disadvantage at many foreign locations. However, little data or analysis, by industry or FAA, exist to support or disprove this assertion. Determining if foreign carriers provide a similar level of protection is fluid and troublesome, and no early solution is likely. Sovereignty issues and the sensitivity of foreign governments to FAA's efforts will continue. Although close cooperation with foreign governments and joint audits may assist FAA, they will not answer questions about how FAA determines if a similar level of protection exists or its competitive implications.

FAA officials believe that most foreign carriers provide a similar level of protection. However, we believe that statements about a similar level of protection are premature because FAA has not completed its analysis of foreign carriers' security programs and countermeasures needed at specific airports. This complex issue will remain controversial with domestic carriers and poorly understood until FAA develops guidelines for its staff and the industry on how to gauge similarity and outline enforcement procedures.

FAA has taken several positive steps to enhance the security of mail and cargo. FAA has implemented new requirements for cargo that should help identify freight forwarders and may heighten security awareness in that industry. However, relying on air carriers to identify and communicate with freight forwarders only partially addresses the problem. Without an effective inspection strategy to ensure freight forwarders' compliance with the new requirements, FAA has not closed the security gap identified by the President's Commission. Plans submitted by freight forwarders offer FAA the necessary building blocks to develop a strategy. With regard to mail, FAA and USPS are developing an agreement that will require USPS to take additional steps to enhance the security of mail, if properly implemented. However, the proposed agreement is a product of difficult negotiations between the two agencies. These difficulties, coupled with institutional differences and questions about authority, make it imperative that a mechanism exists to resolve problems identified by the joint audits.

Recommendations

We recommend that the Secretary of Transportation direct the Administrator, FAA, to take the following steps:

- In conjunction with the FBI, develop information on threats and the individuals with the capability to carry them out for the 19 category X

domestic airports and a plan to reassess the 19 category X airports' security in light of this information.

- Develop guidelines for FAA organizations and the aviation industry on how the similar level of protection provision of the act is being defined, implemented, and enforced. The guidelines should also specify the manner in which similarity with requirements for U.S. carriers is ensured.
- Analyze the implications of imposing different requirements on U.S. and foreign carriers departing the same foreign airport.
- Use the security plans submitted by freight forwarders to develop a strategy, including the frequency and rigor of inspections, to ensure compliance with the plans.
- Report the results and effectiveness of the joint FAA-USPS programmatic audits of the new postal procedures to a third party, such as the appropriate oversight committees or the Office of Management and Budget.

Agency Comments

We discussed our findings and recommendations with DOT's Director and Deputy Director of Intelligence and Security, FAA's Acting Associate Administrator of Civil Aviation Security, FAA's Director for Policy and Planning for Civil Aviation Security, and other FAA security officials. Generally, these officials agreed with the information but offered the following observations.

According to DOT and FAA officials, the joint assessments of domestic airports did not consider the intentions or threat posed by terrorist groups to individual airports. They also pointed out that, although the World Trade Center bombing and conspiracy in New York City involved local elements, FAA cannot conclude that such actions represent a direct threat to aviation or indicate a preferred base of operation for a hijacking or aircraft bombing. Therefore, FAA takes the view that, absent information on a specific conspiracy or attack plan, the threat to civil aviation within the United States is essentially the same at all locations.

DOT and FAA officials also noted that passengers traveling on some foreign carriers where a very low threat exists may have a similar level of protection even if the countermeasures in place are much less stringent than those used by U.S. carriers because the perceived nationality of the carrier (not the presumed nationality of the majority of passengers) has often been the determining factor in instances where criminal acts have been carried out against airlines for political motives. FAA officials noted

that they could find no instance of a foreign carrier having been targeted by a terrorist group because the United States was the flight's destination.

FAA officials acknowledged that they are not optimistic that rapid progress can be made in some countries to ensure that foreign carriers provide a level of protection similar to that of U.S. carriers. FAA officials noted, however, that rapid progress is possible with carriers from countries that have not developed the sensitivities against the extraterritorial application of U.S. law. These officials also noted that they have a plan for working with foreign governments to resolve concerns. In addition, FAA and DOT officials pointed out that it is inappropriate to require security measures (or not to require them) on the basis of whether they constitute a competitive advantage or disadvantage. Indeed, FAA points out that raising this issue undermines the seriousness of security and plays into the hands of those foreign governments that believe the issue of a similar level of protection is a pretext for introducing nontariff trade barriers. In addition, the Director for Policy and Planning for Aviation Security noted that FAA's and other countries' security measures must not be used to achieve a commercial advantage for any sector of any industry, regardless of nationality, and that to do so would be a blatant violation of the General Agreement of Tariffs and Trade and U.S. law implementing that agreement.

Notwithstanding concerns about the competitive impact of differing requirements for foreign and domestic carriers, FAA is directed by law to ensure that a similar level of protection exists for U.S. passengers traveling on foreign airlines. Although FAA officials believe a similar level of protection generally exists, FAA does not, in our judgment, have sufficient information to make this determination. FAA has not yet started to work with foreign carriers to bring about needed improvements or completed its analysis of the additional countermeasures that individual foreign carriers will be asked to adopt. Moreover, FAA has no guidance or criteria that clearly outline what constitutes a similar level of protection. Until FAA (1) identifies specific countermeasures that foreign carriers will be asked to adopt and (2) develops guidelines that clearly define a similar level of protection, this issue will remain controversial with domestic carriers.

FAA officials reaffirmed their concerns about USPS' taking action to address problems identified by the joint audits. These officials noted, however, that in instances where FAA and USPS cannot come to an agreement on the appropriate action required, a third party may need to get involved. FAA officials suggested that such problems could be brought to the attention of

the Office of the Management and Budget, and we modified our recommendation to reflect their view.

Actions Needed to Ensure That FAA Meets Current and Future Threats

FAA could take other actions to enhance its aviation security efforts to meet current and future threats. These actions include: (1) carefully pilot-testing new security procedures before implementing them, (2) paying greater attention to human factors issues, (3) making better use of the wide range of information at FAA's disposal, and (4) providing security coordinators at category X airports with security clearances. Without careful attention to these issues, FAA's strategy of using agency and industry resources in a flexible and intelligent way to meet current and future threats may not succeed.

Pilot-Testing Could Benefit New Security Initiatives

Past FAA experience has demonstrated that concepts that make sense theoretically or in a laboratory may not work in an airport environment. In addition, the financial health of U.S. airlines, high expectations of the traveling public, and competition for scarce federal funds dictate that FAA ensure the effectiveness and efficiency of new procedures and equipment before requiring airlines and airports to purchase and use them. Industry officials with whom we spoke are willing to invest in new technology, especially explosive detection equipment, but question FAA's resolve to test new technology before mandating its widespread use. We recognize that changing world events, an increase in the terrorist threat, or other circumstances may force FAA to eschew pilot-testing of new security initiatives. Moreover, FAA needs to view new security procedures and technology from a systems perspective. In other words, FAA needs to carefully examine a new technology's synergistic impact on the entire security framework before implementing it systemwide.

FAA's access control rules, FAR 107.14, provide an example of how pilot-testing—even on a small scale—would have pointed out problems and may have saved the industry millions of dollars. In late 1989, FAA required domestic airports to install computer systems to prevent unauthorized access to the important areas of airports, such as runways. Computerized systems would replace lock-and-key doors and some procedures. Each airport employee would have an access card that would be used to enter the airport. An employee would gain access to a secure area by swiping an identification card in a card reader. The comings and goings of employees would be recorded in a central data base. FAA estimated that the total cost of the system for 270 airports would be about $170 million. Several airports argued for pilot-testing of the new systems during the rulemaking process.

The cost of computerized access systems has skyrocketed over FAA's initial estimates. Industry now estimates that these systems will cost about $700 million and that annual maintenance costs will be about $50 million. FAA estimates that total costs are under $500 million and noted that costs have skyrocketed for many reasons, including the failure of airports and contractors to control costs. One category X airport alone spent over $75 million to install an access system. DOT's Office of Inspector General recently demonstrated that these systems may not be as effective as FAA intended. At five category X airports, the Inspector General gained access to secure baggage-handling areas and, in some cases, the airport surface where passengers were boarding aircraft.[1]

Pilot-testing new systems would provide FAA with a better understanding of the cost of new systems and how they would work in an airport environment. Although FAA officials agree that pilot-testing new technology is important, many remain reluctant to test new technology under realistic airport conditions because of time and cost. FAA officials pointed out that pilot-testing without a defined end point could hamper or prevent the implementation of new technology. FAA has a $10 million test site at Baltimore/Washington International Airport that the agency can use to test new security systems. However, before Baltimore/Washington can be used in this fashion, several issues related to the cost and schedule of the project need to be resolved. FAA top management is not satisfied with the project's progress and has directed that new specifications for the test site be developed.

Human Factors Should Not Be Overlooked

The security of the traveling public rests on a careful blend of technology, procedures, and policies. Developing and fielding new explosive detection devices is only part of the solution—improving security also involves people. In FAA's, the FBI's, and other security experts' view, careful attention to human factors issues—such as the effectiveness of security screeners—is a necessary complement to technology. Moreover, the Aviation Security Improvement Act directed FAA to explore ways to enhance human performance in aviation security. We previously reported on the importance of effective training and attention to human factors in security.[2] During the course of this review, we identified several human factors issues—screeners' proficiency, airport employees' awareness of

[1]Audit of Airport Security, FAA, R9-FA-3-105, Sept. 20, 1993.

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

security concerns, and passenger profiling—that FAA must continue to address.

First, screeners have historically been viewed as a weak link in the security framework because of their low pay and high turnover. However, airport screeners are the first line of defense for aviation security. Since 1988, over 5.4 billion passengers have been screened and over 13,000 firearms and 312 explosive devices were detected, leading to over 6,500 arrests. Most, if not all, of the firearms and explosive devices were detected by screeners using X-ray equipment. During the same time, FAA inspected screening points over 26,000 times. Our analysis of FAA's data shows that screeners' performance in detecting FAA's test objects increased from about 91 percent in 1988 to about 94 percent in 1993. However, this percentage may be overstating the skill of screeners for several reasons. First, FAA officials told us that, during unannounced proficiency tests, screeners frequently recognize FAA inspectors. FAA's former Associate Administrator for Civil Aviation Security recognized this problem and noted that FAA inspectors have become too predictable. Therefore, screeners expect to find a test weapon. Second, many of FAA's test objects are obsolete. For example, one test object is a pipe bomb, while another is a hand grenade. Our analysis of FAA data shows that screeners have a high probability of detecting a pipe bomb but have difficulty detecting the relatively unsophisticated "alarm clock bomb" test object.

FAA officials told us that they are working to develop new test objects and expect to field-test them at airports by December 1993. According to these officials, it will then take at least 1 year to incorporate new test objects into FAA's inspection program. In addition, manufacturers of new X-ray equipment have begun developing test programs to be built into devices for screeners. One manufacturer has developed a system that can insert the image of a weapon or explosive in a piece of baggage on the screener's display. The screener is alerted by the computer that the image is a test object before any action can be taken. This type of test shows promise, but when it will be in widespread use is uncertain.

Second, FAA needs to enhance the overall awareness of airport employees to security concerns. FSMs and airport security officials at several category X domestic airports told us that airport personnel—ground crews and vehicle drivers—may be the last line of defense if unauthorized individuals gain access to critical areas of an airport. Our observations at several category X airports confirmed the importance of this and the need for

FAA's procedures. DOT's Inspector General also found that airport personnel were lax in challenging unauthorized personnel and taking timely action as required by FAA. In 1990, FAA established the Security Identification and Display Area training program to enhance airport employees' awareness of security and steps they should take if they notice something suspicious. This training was FAA's first major effort to enhance airport personnel's awareness of security concerns. Airport employees are required to challenge and report unauthorized persons to a supervisor or law enforcement officer. One airport has taken steps to ensure that all of its employees fully understand the need for such actions by providing training in several different languages. FAA will continue to face challenges in refining training and procedures for airport personnel to boost their awareness of and sensitivity to security.

Third, additional work on passenger profiling may offer some advantages for FAA. Profiling is a method of separating potential threat individuals from other travelers through an interview. Moreover, profiling is credited with preventing a terrorist act against a foreign carrier in 1986. Currently, profiling is done only on some international flights and is based on several key questions. One foreign airline known for its rigorous security programs—one of the few that profiles passengers—uses a much more detailed list of questions. Officials from one airline with whom we met is pilot-testing an automated profiling system that works from a new perspective—it seeks to eliminate nonthreat passengers. FAA recently began working with the airline to refine this system. FAA points out, however, that successful profiling rests largely on highly motivated and well-trained people.

As the President's Commission pointed out, FAA has not placed adequate attention to human factors issues and training. Although FAA is now more aware of human factors, airline and airport officials believe that top-level FAA management is preoccupied with finding technological solutions to security problems, such as developing new explosive detection systems. Conversely, FSMs and airline security directors believe that greater attention to human factors is needed, especially with respect to screeners' performance, profiling, and boosting airport personnel's awareness.

The responsibility for enhancing security through human factors research rests largely with FAA's Research, Engineering, and Development (RE&D) Program. As mentioned previously, the act directed FAA to explore both technological and human factor improvements to meet the terrorist threat. However, FAA has invested most of its RE&D funds toward developing

explosive detection equipment. Table 3.1 compares FAA's RE&D investment in human factors with other program areas prior to and since the passage of the Aviation Security Improvement Act.

Table 3.1: FAA's Security RE&D Budget

Dollars in millions

Program	1988	1989	1990	1991	1992	1993[a]	1994[a]
Explosive detection	$ 9.6	$9.9	$17.0	$28.2	$23.7	$22.7	$22.8
Weapons detection	0	0	0	2.1	3.6	3.7	0[b]
National air system security	0	0	0	2.0	4.2	4.0	2.5
Aircraft hardening	0	0	0	0	0	4.5	7.8
Human factors	0	0	0	0	0	1.0	2.8
Total	**$9.6**	**$9.9**	**$17.0**	**$32.3**	**$31.5**	**$35.9**	**$35.9**

Note: Data are shown by fiscal years.

[a]Appropriated dollars.

[b]In fiscal year 1994, FAA combined explosive and weapons detection into one account.

Source: GAO's analysis of FAA's data.

As table 3.1 shows, FAA's security research program has enjoyed significant growth since the Pan Am 103 incident (Dec. 1988). According to FAA officials, prior to Pan Am 103 and the act's passage, most research focused on weapons and explosives detection—not aircraft hardening or human factors. In fiscal year 1993, FAA spent about 3 percent of its RE&D funds on security-related human factors issues. FAA has had difficulty in developing an effective human factors security program because of high staff turnover in a key position at the FAA Technical Center. FAA plans to more than double its human factors effort in fiscal year 1994 to, among other things, enhance screeners' proficiency.

Human factors research will become critically important as new explosive detection devices are fielded to ensure that operators can effectively use the new equipment. However, measuring progress in enhancing human factors is difficult, and achieving improvement may take time. For example, although DOT's Inspector General found problems with FAA's security badging and training for airport employees, several FAA, airport, and airline officials believe that such actions enhanced employees' awareness of security issues.

FAA Can Make Better Use of Its Information

FAA collects a wide range of information from its inspection programs, SLOs, and FSMs. This information can be used to focus resources and spot emerging trends. Although it analyzes some inspection data, FAA is not analyzing the wide range of information it collects to shape the overall direction of its program and to identify problems. Moreover, additional actions are needed to ensure that FAA can identify emerging trends and problems before they become serious security issues.

According to terrorism experts, the threat to aviation remains real. FAA's efforts to respond to the act and prevent another Pan Am 103-type incident have strengthened aviation security. Moreover, State Department and FAA officials believe that countries that have traditionally sponsored terrorism are hampered from taking any major initiatives because of poor economic and political conditions. The changed international environment, along with improved security, leads State Department officials to conclude that, while not impossible, it would be more difficult to duplicate the downing of Pan Am 103 today.

In the long-term, however, the threat to civil aviation may be quite high. According to State Department and FAA officials, the ferocity of the threat depends largely on the (1) foreign policy initiatives pursued by the United States and (2) the U.S. government's success in fighting terrorism. Although the first factor is clearly outside FAA's control, it is important that FAA utilize the data at its disposal to anticipate events and be forward-looking as it carries out its security responsibilities. The extent to which FAA currently utilizes the information it collects and gets that information into the hands of the airports and carriers raises concerns about the agency's ability to assess future threats and counter current ones.

FAA records most of its data in the Civil Aviation Security Information System. Table 3.2 shows information we developed from CASIS on the total number and type of FAA inspections for domestic airports and carriers from 1988 to April 1993.

Table 3.2: Security Inspections for Domestic Airports and Carriers, 1988-93

Category	1988	1989	1990	1991	1992	1993[a]	Total
Air carrier	5,941	12,881	13,346	13,909	13,782	4,014	**63,873**
Screening point[b]	1,483	5,923	6,064	4,966	6,194	1,807	**26,437**
Airport	560	1,170	1,134	1,531	1,420	397	**6,212**
Total	**7,984**	**19,974**	**20,544**	**20,406**	**21,396**	**6,218**	**96,522**

Note: Data are shown by calendar years.

[a]Through April 1993.

[b]Refers to FAA's evaluation of screeners' proficiency in detecting FAA's test objects.

Source: GAO's analysis of FAA's data.

As table 3.2 illustrates, FAA conducted over 60,000 air carrier, almost 27,000 screening-point, and over 6,000 airport inspections from 1988 to 1993. Eighteen category X airports received the most security inspections. For example, almost half of all carrier and screening-point inspections over the past 5 years occurred at 18 category X airports. Similarly, FAA inspected the 18 category X airports over 950 times during the same period to determine the adequacy of, among other things, perimeter fencing, training, and signs. These figures do not take into account inspections of foreign carriers outside of the United States. (Ch. 2 discussed these inspections.)

FAA officials told us that they use CASIS to focus resources and spot emerging trends. FAA deployed CASIS in 1985; it contains information ranging from airport bombings to inspection results. Our analysis of CASIS' data from 1988 through April 1993 indicates several problems that need to be resolved before FAA can spot emerging trends and allocate its resources effectively. First, CASIS does not contain information on the severity of a deficiency or how it relates to airport security as a whole. FAA denotes inspection findings as satisfactory or unsatisfactory. According to officials, this has led to a "check-list" mentality in the FAA security workforce that focuses more on filling out the inspection form than seeking long-term solutions to pressing security problems. Table 3.3 provides information we developed from CASIS on the results of key elements of FAA's security inspection for air carriers and airports.

Table 3.3: FAA's Security Inspection Results, 1988-93

Inspection[a]	Percent satisfactory	Percent unsatisfactory
Air carrier station		
Carry-on baggage screening	97.3	2.7
Passenger screening	98.7	1.3
Access to air operations area	99.2	.8
Screener Proficiency Test	94.0	6.0
Airport		
Airport fences	95.7	3.3
Identification badge control (temporary)	94.4	5.6

Note: 1993 includes January through April.

[a]Refers to noncompliance with FAA's regulations.

Source: GAO's analysis of FAA's data.

As table 3.3 illustrates, although FAA inspects many aspects of security, CASIS indicates very few cases of regulatory noncompliance. For example, FAA examined carriers' carry-on baggage screening and found unsatisfactory conditions only about 2.7 percent of the time. Similarly, FAA examined access to air operations areas at carrier facilities—a major problem identified by DOT's Inspector General—and found unsatisfactory conditions less than 1 percent of the time. FAA's former Assistant Administrator for Civil Aviation Security acknowledged this problem and told us that, while CASIS can provide overall numbers of inspections, it cannot provide FAA management with important information on security at airports. These findings and the large number of security inspections FAA conducts each year raise questions about FAA's current domestic inspection strategy, the frequency of inspections, the training of the security workforce, and the manner in which FAA allocates resources.[3] FAA officials told us that they are developing new security inspection guidelines and expect to complete them in late fiscal year 1994.

Second, CASIS does not include information to determine whether the unsatisfactory conditions resulted from carelessness on the part of individuals or were symptomatic of much larger problems. According to FAA officials, CASIS was not developed to capture the state of security at the nation's airports. Instead, important information on the strengths and weaknesses of air carrier and airport security reside with individual FAA

[3]We did not examine FAA's overall inspection strategy, how inspector resources are allocated, or other workforce issues.

security inspectors. Moreover, FAA officials told us that most investigations—the analysis of alleged security violations—are initiated without the use of CASIS. FAA officials told us that they have recently revised CASIS to take into account inspectors' observations.

Third, the age of the data base and its incompatibility with newer systems make the analysis of CASIS data difficult for FAA managers and security inspectors. FAA headquarters staff responsible for managing security programs told us that they are handicapped by CASIS' age and lack of analytical capability. FAA regional security officers, about 75 percent of FAA's security workforce, cannot easily access CASIS and conduct routine analyses. Moreover, FAA officials told us that field inspectors spend about one-third of their time entering data into CASIS. Computer systems have made several advances in the past several years, such as advanced architecture designs, that FAA could take advantage of to enhance CASIS. FAA officials told us that they are exploring several ways to enhance CASIS but have not decided upon a specific approach.

FAA could make its program more effective by revamping CASIS. A first step would be to develop quantitative measures to analyze security inspection data. As noted earlier, most inspection results only indicate whether a satisfactory or unsatisfactory condition exists. A more analytical approach would provide FAA with better information to make decisions regarding security. For example, airport compliance with a specific security regulation could be evaluated in terms of a scale—"one" being problematic and "five" being in compliance. Inspectors of nuclear facilities use such a scale to determine compliance with federal regulations. FAA officials told us that they are reluctant to assign a numerical rating because they do not want to rank airports and risk having the information become publicly known. However, we believe a more analytical approach would help FAA spot potential problems and target its inspection resources.

Security Coordinators at Category X Airports Lack Needed Information

The timely flow of information to airlines, airports, and FAA is vitally important to ensure the security of the traveling public. Our discussions with FSMS and airport security coordinators—the officials responsible for security—indicated that the coordinators do not receive detailed information to carry out their responsibilities.

Sharing sensitive or secret information with the aviation community is difficult because many precautions must be taken to safeguard the information. Before FAA can release information developed by or obtained

from the intelligence community, it must receive authorization from the agency that obtained or developed the information. For example, if FAA obtains sensitive information from the FBI on a specific threat at a domestic airport and decides that it must disseminate the information widely, the agency must consult with the FBI and receive permission to release the information in a "sanitized" form.

However, airport security coordinators do not have security clearances. As a result, FAA cannot tell the coordinators about threats and could not provide a written copy of the joint FAA-FBI assessments because the coordinators lacked security clearances. Several FSMs were deeply concerned about this and believe it is a major obstacle to effective communication and security. FAA can sponsor the granting of security clearances to airport security coordinators; the Department of Defense or a similar agency would conduct the background investigations needed to grant access to classified material. Some airline security directors have security clearances and, therefore, have access to classified information.

According to FAA and industry officials, FAA's lack of experience in working with the U.S. intelligence community and sharing sensitive information with the industry has hindered efforts to get valuable information to the industry. In fact, industry officials said they rely more on their informal networks than FAA for important information on threats. DOT and FAA officials told us that they are working with the U.S. intelligence community to improve the processing of information and gain a better understanding of each other's needs. FAA officials point out that they have daily contact with the U.S. intelligence community.

FAA and DOT officials do not believe that airport security coordinators need security clearances. They cite the expense of doing a security check. They also are concerned that if critical information were given to the airport security coordinator, it would ultimately be made available to all airport staff, including screeners. In addition, FAA and DOT officials are concerned about the unauthorized release of information obtained from the U.S. intelligence community.

We disagree with DOT and FAA officials because, in our view, effective security hinges on the timely dissemination of information. For example, at one category X airport we visited, the FSM provided us with an example showing that the airport security coordinator could have benefited from receiving classified information by tailoring airport security to meet a potential threat. Because this information may still be classified, we are

precluded from discussing it in this report. In addition, a January 1993 evaluation of the FSM program conducted by the Evaluation and Program Analysis Division of FAA's Office of Civil Aviation Security found that "There are no mechanisms in place for FSMs to immediately and widely share classified intelligence information with principal members of the aviation community." The evaluation also noted that the improved release of important information could lead to more awareness and action. Additional information obtained by the airport security coordinator can be used to tailor airport security to a particular threat. Furthermore, airline security directors have security clearances and, therefore, have access to classified information.

Furthermore, cost is not a major obstacle. The initial cost of providing a security clearance for airport security coordinators at the 19 category X airports would be about $61,000. On the basis of our discussions with FAA officials, FAA's internal evaluation, and input from the industry, FAA is proposing a pilot study to evaluate the necessity and feasibility of granting security clearances to airport law enforcement officials. According to FAA officials, two or three airport officials will be given clearances on a temporary basis so that they may participate in the study.

Conclusions

Improving the nation's aviation security system over the next decade will be challenging and require careful thought. New measures and technology must be introduced in cost-effective ways that do not adversely affect the industry and traveling public. At the same time, FAA must be able to respond to changes in the nature of terrorist threats and adjust its program accordingly. Although important, developing and deploying new explosive detection systems is not a panacea. In our opinion, four factors can help FAA posture itself to be more forward-looking and introduce meaningful security improvements.

First, pilot-testing new technologies and systems in an airport environment, when conditions allow, will help FAA ensure that they work as intended. This will improve the effectiveness of new technologies and procedures and boost industry's confidence in their effectiveness. Second, focusing on human factors issues, such as screeners' performance, will pay long-term dividends for the aviation community. Third, FAA can take steps to focus its resources and identify trends by revamping its CASIS data base and bringing a level of analytical sophistication to its efforts. Last, providing airport security coordinators at the nation's category X airports

with a security clearance may enhance the flow of information and enhance cooperation between FAA and airports.

Recommendations

We recommend that the Secretary of Transportation direct the FAA Administrator to

- pilot-test new equipment and procedures to determine if they improve security before implementing them systemwide, unless threat levels or other factors warrant more rapid implementation;
- enhance the emphasis and priority placed on human factors, particularly screeners' performance, passenger profiling, and airport employees' awareness;
- improve FAA's security inspection and information system to identify trends and emerging problems before they become security issues; and
- take the required steps to obtain security clearances for security coordinators at the 19 category X airports.

Agency Comments

DOT and FAA officials generally agreed with our findings and recommendations and offered the following observations. FAA officials noted that passenger profiling is done only on some international flights and is not a universal requirement for all U.S. carriers departing from overseas locations. They also noted that FAA is continually working to improve passenger profiling. For example, FAA has a research project to explore the feasibility of various profiling approaches for domestic operations. They also noted that the Civil Aviation Security Program has more than RE&D activities focused on human factors issues.

In addition, although FAA had denoted inspection findings as satisfactory or unsatisfactory, in fiscal year 1994, the agency instituted three categories of inspection findings—violation, observation, and satisfactory. According to FAA officials, "observation" will be used to note items not technically in violation of federal aviation regulations but deserving further attention before they become violations.

However, FAA and DOT disagreed that airport security coordinators need security clearances. According to DOT and FAA officials, sanitized versions of threat information are routinely sent to airport officials. They also noted that the problem of having some personnel without clearances performing security functions would not go away even if several officials at every airport had a security clearance. These officials would still need to discuss

procedures with others at the airport who would not have security clearance and thus would have to rely on the very same sanitized versions of threat information. According to FAA officials, more than one individual at each airport would need to be cleared and therefore the cost would be more than $61,000 for obtaining clearances for 19 airport security coordinators.

We find FAA's nonconcurrence with our recommendation difficult to understand. First, FAA recognizes this as a problem and has proposed a pilot study at two or three airports to evaluate the merits of providing clearances to airport security coordinators. And second, FSMs and airport security coordinators with whom we spoke are concerned that airports are not receiving important information and strongly believe that providing security clearances to airport officials would lead to greater awareness, cooperation, and action.

FAA's Response to Key Provisions of the Aviation Security Improvement Act of 1990

Mandated Action	FAA/DOT Action
Establish the Director of Intelligence and Security within DOT (deadline: Nov. 1990)	Position established in June 1990
Annual report to the Congress on DOT's and FAA's security activities	1991 annual report provided to the Congress in June 1992; 1992 report provided to the Congress in June 1993
Change FAA's semiannual report on screening to annual	First annual report for calendar year 1990 issued in Apr. 1992. Calendar year 1991 report provided to the Congress in Aug. 1993
Establish the position of Assistant Administrator for Aviation Security	Position established in June 1990
Establish FSMs at category X domestic airports (deadline: Nov. 1991)	FSMs are in place at all 19 category X U.S. airports
Establish SLOs at high-risk foreign airports (deadline: Nov. 1992)	First 11 SLOs assigned in Sept. 1990; 6 additional SLOs established in May 1992
Report to the Congress on implementation plan for FSMs and SLOs (deadline: May 1991)	Submitted to the Congress in July 1991
Develop regulations to implement employment investigations including criminal history checks for air carrier and airport employees	FAA released a Notice of Proposed Rule Making in Feb. 1992 and received over 300 comments; FAA published a supplemental notice in Sept. 1992
Prescribe employment standards for air carrier and airport security employees (deadline: Aug. 15, 1991)	Standards published on Aug. 20, 1991; effective Sept. 19, 1991
Review human factors issues and prescribe changes to existing procedures	FAA has initiated human factors RE&D program
Prescribe education and training standards for air carrier and airport security personnel (deadline: May 15, 1991)	Proposed amendments to the Air Carrier Standard Security Program will take effect on Feb. 1, 1994
Review foreign air carrier security programs to determine whether they provide a similar level of protection (deadline: Nov. 18, 1991)	Review completed Nov. 12, 1991
Report to the Congress on the progress of foreign air carriers in attaining similar levels of protection	Report for calendar year 1991 was provided to the Congress in Apr. 1993; calendar year 1992 report is still in process
Issue regulations requiring a similar level of protection for foreign air carriers (deadline: May 15, 1991)	Regulations published July 1, 1991; effective July 31, 1991
Conduct joint FAA-FBI assessments of the domestic air transport system	FAA and FBI have completed assessments of 18 of the 19 category X airports in 1991 and 10 other airports in 1992
FAA-FBI determine and implement best method to continually analyze threats to aviation	This is an ongoing effort
For 1991 and 1992, report to the Congress on joint FAA-FBI assessments of domestic airports and make recommendations for improving security	In Mar. 1993, FAA forwarded its report to the Congress on 1991 assessments; as of Dec. 1993, the report on 1992 assessments was in coordination
Take actions to remedy weaknesses identified by FAA-FBI assessments	Actions to improve security are underway and will be monitored by FSMs
Accelerate RE&D programs to counteract terrorist acts	FAA Technical Center has expanded from 8 personnel in 1988 to 40; budget has grown from $8 million to $35 million
Intense review of terrorist threats for RE&D program (deadline: May 15, 1991)	Final report on threat review completed May 14, 1991
Focus and prioritize RE&D program on the basis of terrorist threats	Fiscal years 1992 and 1993 program priorities and fiscal year 1994 budget submission were based on threat review

(continued)

Mandated Action	FAA/DOT Action
Consult and coordinate RE&D program with other agencies and seek to share costs	In process through National Security Council Technical Support Working Group and other initiatives
Place in use equipment resulting from RE&D program (deadline: Nov. 1993)	Although some technologies show promise, development of detection systems has been more difficult than expected and has prevented FAA from implementing new equipment
Include both technological and human factors in RE&D program	Ongoing effort consisting of a focused human factors program that began in fiscal year 1993
Establish a scientific advisory panel as part of RE&D advisory committee	Security subcommittee of FAA of RE&D Advisory Committee created June 1990
Complete explosive detection systems certification using independent test protocols	National Academy of Sciences bulk test protocol released Sept. 1991; final certification criteria for bulk explosive detection systems published Sept. 1993
Develop guidelines for industry's reporting of threats to civil aviation	Guidelines incorporated into air carrier security programs in June 1990
FAA Administrator to cancel flights because of threats that cannot be countered	No action necessary; FAA believes it has the necessary authority
Develop guidelines for ensuring public notification of threats (deadline: May 15, 1991)	Completed in 1991 through Memoranda of Understanding with the Departments of State and Justice
Develop guidelines for notifying flight crews of threats (deadline: May 15, 1991)	Final rule published June 17, 1991; effective July 17, 1991
Develop guidelines to minimize the number of individuals that have access to threat information	Office of Civil Aviation Security and Intelligence completed action in June 1991, also addressed in Memoranda of Understanding with State and Justice
Develop guidelines for airport design and construction that allow for maximum protection	Joint FAA-industry study conducted—guidelines were published in Oct. 1993
Develop procedures to ensure free flow of information to DOT and FAA from the intelligence community	Completed in Nov. 1990
Establish Central Intelligence Agency senior staff liaison officer	Completed in Sept. 1990
Review all Memoranda of Understanding among DOT, FAA, and the intelligence community	Completed in June 1991
Study mail and cargo to determine if additional requirements should be imposed	Completed in May 1991
Report to the Congress on the results of mail and cargo study with recommendations on how to improve system (deadline: May 15, 1991)	Report sent to the Congress in Aug. 1992
Require all U.S. carriers to provide a passenger manifest to State Department within 1 to 3 hours of being notified (deadline: May 15, 1991)	Advance Notice of Proposed Rule Making published in Jan. 1991; in coordination as of Dec. 1993
Consider need for collecting passenger manifest before passengers board aircraft	Notice of Proposed Rule Making published in Jan. 1991; in coordination as of Dec. 1993
Develop anti-terrorism guidelines with the State Department for international travelers	Completed in Mar. 1991

Inspections of Foreign Carriers at Last Points of Departure

FAA region[a]	Total foreign air carriers	Number of foreign air carriers inspected	Percentage of inspections completed
Eastern	13	5	38.0
Europe	69	20	28.9
Northwest Mountain	3	3	100.0
Southern	45	41	91.1
Southwest	9	9	100.0
West Pacific	22	13	59.1
Total	**161**	**91**	**56.5**

[a]FAA collects these data by the FAA region responsible for the inspection—not by geographical location.

Source: GAO's analysis of FAA's data.

Major Contributors to This Report

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

Allen Li, Associate Director
Mary Ann Kruslicky, Assistant Director
Matthew E. Hampton, Evaluator-in-Charge
Steven Schamberger, Staff Evaluator
John Rehberger, Technical Advisor

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1000
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066.

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

[redacted]

Address Correction Requested

[redacted]