United States General Accounting Office

GAO

Report to the Subcommittee on Transportation and Related Agencies, Committee on Appropriations, House of Representatives

March 1995

AVIATION SECURITY

FAA Can Help Ensure That Airports' Access Control Systems Are Cost-Effective

GAO/RCED-95-25

GAO

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

Resources, Community, and
Economic Development Division

B-258317

March 1, 1995

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

On December 7, 1987, 43 people died when Pacific Southwest Airlines Flight 1771 crashed after a disgruntled former employee shot the pilots. This tragedy heightened the Federal Aviation Administration's (FAA) concern about the effectiveness of airport security because the former employee had, among other things, apparently used airline identification to bypass screening. In January 1989, as part of an effort to improve its overall strategy for preventing violent acts against airlines, FAA required that the nation's major airports install systems for controlling access to high-security areas where large passenger aircraft are located. These systems are eligible for funding under FAA's Airport Improvement Program (AIP).[1]

Your Subcommittee expressed concern about FAA's strategy because airports and airlines have complained that FAA greatly underestimated the costs of access control systems. Therefore, you requested that we (1) determine how much access control systems have and will cost and (2) identify what actions FAA could take to help ensure that systems are cost-effective in the future.

Results in Brief

The variety of systems—mostly computer-controlled—installed at airports to meet FAA's access control requirements cost far more than FAA anticipated. These systems include such equipment as closed-circuit television cameras and employee identification card readers on doors leading into secured areas. Updated data provided by FAA show that from 1989 through 1998, the actual and projected costs for systems at the 258 airports subject to FAA's requirements will total about $654 million in 1993 constant dollars—over three times FAA's initial estimate for that period. This amount includes $327 million in Airport Improvement Program funds,

[1]The AIP provides funds to help eligible airport sponsors plan and develop airport infrastructure. The airport sponsor is the public agency or private entity that owns or operates the airport.

or 50 percent of total costs. Furthermore, on the basis of updated data, FAA projects that systems will cost an additional $219 million in 1999 through 2003, half of which would be federally funded. FAA officials stated that the agency's initial cost estimate was low primarily because more access points were secured and more expensive equipment was installed than the agency anticipated in its analysis.

Although most airports have completed the installation of access control systems, they will need to modernize these systems as equipment wears out, additional equipment is needed, or equipment or software no longer has the capacity to meet security-related demands. FAA can help ensure that system modernization is cost-effective by (1) providing detailed guidance explaining where equipment should be located and (2) working with the industry to develop and implement standards that provide technical criteria explaining how systems should function to meet access control requirements. Absent detailed guidance, many airports, with FAA's approval, installed equipment at locations that the agency later determined did not need to be secured to meet its requirements. Also, with no standards for designing systems, airports had less assurance that systems would adequately function to meet FAA's requirements. An industry survey found that 21 major airports had to replace or significantly modify systems that did not operate adequately to meet those requirements. Additionally, without guidance and standards to serve as criteria for evaluating systems, it is difficult for FAA officials to ensure that Airport Improvement Program funds are used only for those system components necessary to meet FAA's access control requirements, as the agency's Airport Improvement Program funding policy directs.

FAA and the industry have several initiatives under way that provide opportunities to help ensure that systems are cost-effective. These initiatives include FAA's reviewing access control requirements and working with the industry to develop standards. We offer recommendations to assist these efforts.

Background

To help provide a safe operating environment for airlines, the Code of Federal Regulations (C.F.R.) title 14, part 107 requires that U.S. airports control access to secured areas.[2] Such controls are intended to ensure that only authorized persons have access to aircraft, the airfield, and certain airport facilities. Other security measures include requiring that airport

[2]Airports' secured areas are primarily the areas where large passenger aircraft are located.

and airline employees display identification badges and that airlines screen persons and carry-on baggage for weapons and explosives.

In January 1989, FAA made 14 C.F.R. part 107 more stringent by mandating that access controls to the secured areas of certain airports meet four broad requirements. Under the amendment—14 C.F.R. 107.14—access control systems must (1) ensure that only authorized persons gain access to secured areas, (2) immediately deny access to persons whose authorization is revoked, (3) differentiate between persons with unlimited access to the secured area and persons with only partial access, and (4) be capable of limiting access by time and date. According to FAA, these requirements are intended to prevent individuals, such as former airline employees, from using forged, stolen, or noncurrent identification or their familiarity with airport procedures to gain unauthorized access to secured areas.

All U.S. airports where airlines provide scheduled passenger service using aircraft with more than 60 seats must meet the requirements of 14 C.F.R. 107.14.[3] Beginning in August 1989, each of these airports had to develop an access control system plan for FAA field security officials to review and approve. Following approval, FAA gives airports up to 2-1/2 years to comply with the regulation, depending on the number of persons screened annually or as designated by FAA on the basis of its security assessment. FAA expects airports to maintain and modernize their systems to keep them in regulatory compliance. As of August 1994, 258 airports were subject to FAA's access control requirements. Appendix I lists these airports.

Access control systems are eligible for AIP funds. FAA administers the AIP and provides funds for airport planning and development projects, including those enhancing capacity, safety, and security. FAA's AIP Handbook (Order 5100.38A) provides policies, procedures, and guidance for making project funding decisions. According to the handbook's section on safety, security, and support equipment (section 7), only those system components and facilities necessary to meet the requirements of 14 C.F.R. 107.14 are eligible for AIP funds. The airports themselves must fund any additional equipment or software capability that exceeds these requirements. FAA airport programming officials approve AIP funding requests.

[3]In some cases, airlines assume responsibility for meeting the requirements in the operational areas they lease from airports, such as terminal gates, under an exclusive use area agreement.

Costs for Access Control Systems Greatly Exceed FAA's Initial Estimate

Airports have installed various systems—mostly computer-controlled—to meet FAA's four access control requirements. With FAA's approval, airports have taken the following approaches:

- Airports have placed the equipment for their access control systems in different locations. For example, some airports screen persons at checkpoints, while other airports have installed controls on doors beyond such checkpoints. Also, some airports have installed controls on both sides of doors leading into and out of secured areas.[4]
- Airports have installed different types of equipment. For example, to secure doors and gates, several airports use magnetic stripe card readers while others use proximity card readers.[5] One airport installed a reader that scans an individual's hand to determine the person's identity. Also, we visited one airport that has an "electronic fence" to segregate the commercial and general aviation operations areas;[6] another has a guard gate and magnetic stripe card reader to separate passenger and cargo operations areas. Additionally, some airports have mounted closed-circuit television cameras at doors and gates, while other airports have chosen not to install such technology.

According to FAA's data, most of the 258 regulated airports have now completed installing their systems, but they will need to modernize these systems in the future.[7] Modernization is necessary when equipment wears out, additional equipment is needed, or equipment or software no longer has the capacity to meet security-related demands. For example, in September 1994, FAA provided one airport that had an approved system with over $3 million in AIP funding to purchase closed-circuit television cameras, help construct a communications center, and make other system modifications to meet additional security needs.

The costs for access control systems are over three times greater than FAA expected. FAA initially estimated that the costs to install, operate, maintain,

[4]As of April 1993, FAA's policy states that access controls are not needed on doors leading from the secured area to meet the requirements of 14 C.F.R. 107.14.

[5]With a magnetic stripe card reader, the employee "swipes" the card through the reader to open the controlled door or gate. With a proximity card reader, the employee holds the card within a few feet of the reader to gain access.

[6]An electronic fence is an invisible barrier that uses sensors to detect movement and trigger an alarm to alert security personnel.

[7]On the basis of information provided by airports, a system's average lifecycle, or time until it must be replaced or significantly modified, is about 6-1/2 years. In contrast, security experts estimate that the average system's lifecycle is about 5 years.

and modernize systems at all regulated airports would total $211 million[8] from 1989 through 1998.[9] However, updated data provided by FAA show that actual and projected costs for the same period totaled about $654 million. This amount includes $327 million in AIP funds, or 50 percent of total costs over the 10-year period. As of August 1994, 177 (69 percent) of the 258 regulated airports received AIP funding to help pay for their access control systems. Furthermore, on the basis of the updated information, FAA projects that costs for systems in 1999 through 2003 will total an additional $219 million, half of which would be federally funded. Appendix II shows actual and projected access control costs in 1989 through 2003, including AIP funding.

According to FAA officials,[10] FAA's initial cost projection was low primarily because more access points were secured and more sophisticated and expensive equipment was installed than the agency's analysis considered. For example, FAA's analysis assumed that the largest airports would secure 128 access points on average. However, we found that these airports had initially secured about 390 points on average. Appendix III compares FAA's initial cost figures with the agency's updated actual and projected costs of access control systems.

FAA Could Help Ensure That Systems Are Modernized in a Cost-Effective Manner

Over the next several years, many access control systems will need to be modernized. FAA can help ensure that modernization is implemented in a cost-effective manner by providing detailed guidance and facilitating the development of standards explaining how to meet the requirements of 14 C.F.R. 107.14.[11] Without detailed guidance, many airports initially spent funds to secure access points that FAA later determined did not need to be secured to meet the agency's requirements. Also, without standards to guide the design of systems, some airports purchased systems that did not meet FAA's requirements. Additionally, without guidance and standards to

[8]All figures in this report are adjusted to constant 1993 dollar values. In January 1989, FAA reported its initial estimate as about $170 million in constant 1987 dollars.

[9]FAA separated its initial $211 million estimate into one-time installation costs and recurring annual costs to operate, maintain, and modernize systems. One-time installation costs included system planning, engineering site survey and design, initial procurement of computers and associated equipment, card readers, access cards, and employee training. Recurring costs included access card replacement, computer maintenance, software update and support, additional labor, and card reader maintenance every fourth year.

[10]These officials include the Manager of and Economists with the Regulation and Organizational Analysis Division, Office of Aviation Policy, Plans, and Management Analysis.

[11]Standards provide technical criteria explaining how equipment and software should function to meet requirements. Standards can also explain how to design, install, and test systems so that they will operate as intended.

serve as criteria, it was difficult for FAA to ensure that AIP funds were used only for the system components needed to meet the agency's access control requirements as directed by its AIP funding policy. FAA and the industry have several initiatives under way that could address these deficiencies and help ensure that systems are cost-effective.

FAA Has Not Developed Detailed Guidance and Standards Explaining How Airports Could Best Meet Access Control Requirements

FAA has not developed detailed guidance and standards to explain how systems could meet its four access control requirements in a cost-effective manner. Detailed guidance could help airports determine where equipment should be located. Standards could explain what functions equipment and software should perform and how quickly and reliably these functions should be done. For example, one of FAA's four access control requirements is that systems grant secured-area access only to authorized persons. Detailed guidance for computer-controlled access control systems could include the following:

- Additional equipment beyond a card reader, such as lights that flash when the door is not secured, should be used only if the access point is in a low-traffic area.
- Closed-circuit television cameras should be used only at access points where an analysis shows that it is less expensive to have the camera than to have security personnel respond to an alarm.

Standards for computer-controlled access control systems could include

- the period of time that a secured door or gate can remain open before security personnel are notified,
- the period of time that can elapse before a terminated employee's access code is invalidated,
- the percentage of time that the system is expected to be operable, and
- the frequency at which the system can misread a card.

Although developing guidance and standards for access control systems is a complex undertaking, FAA has provided airports and airlines with guidance and standards explaining how to meet other agency requirements that are similarly complex. For example, FAA has planning and design guidance explaining how terminals can be configured to accommodate the expected flow of passengers. The guidance recognizes that each airport has its own combination of individual characteristics that must be considered. FAA's standards for equipment include those to design, construct, and test lift devices for mobility-impaired airline passengers and

vehicles for aircraft rescue and fire fighting. Such standards do not specify what equipment airports should use, but rather how a vendor's equipment should perform to meet FAA's requirements. For software, FAA has developed standards for the software used in the Traffic Alert and Collision Avoidance System that it requires on most commercial passenger aircraft.

FAA requires that airports use its guidance and standards in order to receive AIP funds. In some cases, FAA certifies that equipment and software from certain manufacturers meet its standards, as it has done for the equipment used to screen persons and the Traffic Alert and Collision Avoidance System. However, similar standards and certifications do not exist for access control systems.

When FAA issued 14 C.F.R. 107.14 in January 1989, the agency did not conduct tests that could have provided the necessary knowledge to establish detailed guidance and standards for computer-controlled systems. Although airports and airlines suggested that FAA conduct tests at selected airports, the agency determined that nationwide implementation of the new requirements should proceed immediately. According to FAA officials,[12] the Office of the Secretary of Transportation attached a very high priority to implementing improved airport access controls. As a result, FAA decided not to delay implementing the new access control requirements by testing and evaluating systems.

Without Detailed Guidance and Standards, FAA Cannot Ensure That Systems Are Cost-Effective

According to security experts and airport and airline representatives,[13] detailed guidance and standards would help airports know which systems satisfy FAA's access control requirements in a cost-effective manner. Without detailed guidance and standards, it is difficult to determine if the many different systems installed at a wide range of costs are cost-effective. A November 1993 survey by the Airports Council International-North America of 63 airports (24 percent of all regulated airports) found that

[12]These officials include the Director of Civil Aviation Security Policy and Planning and the Director of Civil Aviation Security Operations.

[13]The security experts include the Executive Director and Director, Aviation Services, Counter Technology, Incorporated; the President, Franklin M. Sterling and Associates, Incorporated; the Aviation/Airport Program Manager, International Computers and Telecommunications, Incorporated; and the Vice President, International Security Concepts, Incorporated. The airport and airline representatives include the Senior Vice President, Technical and Environmental Affairs, Airports Council International-North America; the Director, Regulatory Affairs, American Association of Airport Executives; and the Managing Director, Security, Air Transport Association of America.

virtually no two have systems using the same equipment and software.[14] Also, a November 1993 survey by the Airport Consultants Council of 14 airports found that the installation cost per secured access control point ranged from $6,250 to almost $55,000; the average cost was over $30,000.[15]

Without detailed guidance, many airports installed access controls that FAA had approved but later had determined were not needed to meet its requirements. In April 1992, citing concerns about escalating costs, FAA clarified how airports could configure systems. FAA allowed airports that had installed systems to reduce the number of controlled access points if the reduction did not compromise security. According to FAA data, over 120 airports have reduced their number of controlled access points. For example, one airport reduced its total number of controlled access points by 26 percent (106 points) while still meeting FAA's requirements. Another airport now meets FAA's requirements with screening checkpoints at concourse entrances, although its initial system included both the checkpoints and card readers installed on both sides of 114 doors located beyond the checkpoints. FAA's Director of Civil Aviation Security Policy and Planning acknowledges that the agency must take a more proactive approach to ensure that airports meet access control requirements in a cost-effective manner by reducing the number of controlled access points where feasible without decreasing security.

Similarly, without standards on which to base system design, airports have incurred higher costs for systems that are based on proprietary software and a "closed architecture."[16] Many airports contracted with firms to install, maintain, and modify their systems using proprietary software and a closed architecture. In such cases, only the vendor providing the system is familiar enough with the system to effectively maintain or make changes to it. According to security experts, the use of proprietary software and a closed architecture can increase a system's lifecycle costs by as much as 100 percent, primarily because of higher maintenance and modification costs. These experts told us that appropriate standards could have provided for an access control system design based on an open architecture. An open architecture would have allowed different vendors

[14]Airports Council International-North America Technical Committee Survey on 14 C.F.R. 107.14 Security System Maintenance and Operations, dated November 29, 1993.

[15]Airport 14 C.F.R. 107.14 Security System Problems and Issues, dated November 1993.

[16]Proprietary software is owned or copyrighted by an individual or business and available for use only through purchase or permission by the owner. A closed architecture system is based on proprietary specifications that make it difficult or impossible for third parties to maintain or modify the system. In contrast, open architecture refers to computer systems whose hardware and software characteristics conform to specifications in the public domain and are not unique to a particular vendor or group of vendors.

to compete for system maintenance, thus decreasing costs. Also, according to security experts, standards would have reduced total system costs by allowing for economies of scale and easier incorporation of new technologies.

Furthermore, without standards on which to base system design, some airports purchased systems that did not meet FAA's requirements. When FAA issued 14 C.F.R. 107.14, airports looked to firms that had developed and installed access control systems at locations such as military facilities, prisons, hospitals, office buildings, and homes. According to security experts, in many cases it was difficult to transfer the security technology and operational knowledge used for such systems to the airport environment. The November 1993 survey by the Airport Consultants Council found that 21 major airports incurred costs to replace or significantly modify systems that did not operate adequately to meet FAA's requirements. For example, one such airport had to replace its inadequate system, including card readers, at a cost of over $1.5 million. According to security experts, well-defined standards could have guided vendors in developing systems and provided airports with greater assurance that the systems would meet FAA's access control requirements. Also, standards could have provided a basis for FAA to certify a vendor's system.

Finally, detailed guidance and standards could have provided criteria for FAA to use in evaluating airports' AIP funding requests for access control systems. Generally, FAA airport programming officials worked with FAA security officials to determine if AIP funding would be used only for the system components needed to meet FAA's requirements as directed by the agency's AIP Handbook. However, they both lacked well-defined criteria against which proposed access control systems could be compared and evaluated. This problem continues as airports request AIP funds to help modernize their systems. For example, one airport with an approved system requested $1.2 million in AIP funds to secure additional doors. An FAA regional Special Agent for security told us that the lack of criteria has caused her to be unsure how to determine if this funding request should be approved.

FAA and Industry Are Considering Changes in Their Approach to Access Control

In January 1994, FAA requested that the public identify up to three regulations that should be amended or eliminated to reduce undue regulatory burdens.[17] Both airports and airlines identified 14 C.F.R. 107.14 as one of the most costly and burdensome regulations imposed on them and stated that FAA should reassess how to control access in a more cost-effective manner without decreasing security. FAA's December 1994 response cites ongoing efforts to revise its security regulations and work with the industry to set standards for access control systems.[18]

FAA and the industry have three initiatives under way for considering changes to access control that could help ensure that systems are cost-effective. First, FAA is working with the industry to revise airport and airline regulations, including 14 C.F.R. 107.14. Specifically, FAA is reviewing its four access control requirements to determine how they help meet security needs as part of an overall security strategy. FAA plans to issue a Notice of Proposed Rulemaking on any revisions to its security regulations by mid-1995.

Second, through the Aviation Security Advisory Committee, FAA is working with the industry to consider the feasibility of implementing a system that would allow transient employees, such as pilots and flight attendants, to use a single card to gain access at all major airports—a universal access system.[19] Research on and testing of a universal access system is one method to help develop standards for access control technology. The Congress has directed that $2 million of FAA's fiscal year 1994 appropriation be used for the initial costs to develop and implement a universal access system. FAA and the industry are now working to evaluate how such a system could best be implemented.[20] Tests involving three major airlines and two high-security airports are scheduled to begin in March 1995.

[17]FAA's January 1994 request was in response to executive branch recommendations and directives from (1) the National Commission to Ensure a Strong Competitive Airline Industry, (2) the Vice President's National Performance Review, and (3) Executive Order No. 12866, "Regulatory Planning and Review," dated September 30, 1993.

[18]1994 Presidential Regulatory Review Final Report/Summary and Disposition of Comments, dated December 1994 and made available to the public on February 1, 1995.

[19]FAA and the industry established the Committee to address security issues. The Committee includes representatives from government, airports, airlines, unions, and other interested parties.

[20]According to FAA, the cost of a universal access system would depend on (1) whether a central control location is established, (2) how many airports and airlines agree to participate, and (3) how many doors are secured at participating airports.

Third, FAA is facilitating an ongoing effort with the industry to develop standards for systems that would comply with the requirements of 14 C.F.R. 107.14 and meet the needs of all regulated airports.[21] As of December 1994, this effort includes developing standards for how equipment and software should function to meet requirements. FAA and the industry also plan to (1) incorporate knowledge gained from testing the universal access system, (2) identify near-term approaches to make systems easier to maintain and equipment and software easier to modify, and (3) promote modernizing existing systems to the new standards. This effort is scheduled to be completed by October 1995.

Conclusions

Airport and airline security is of paramount importance. To this end, FAA and the industry plan to spend millions of dollars to modernize access control systems as part of an overall security strategy. At this time, however, FAA cannot ensure that these modernization efforts will result in the best use of limited federal and industry funds.

FAA and the industry have initiatives under way that provide a basis for helping to ensure that access control systems are cost-effective. Specifically, following 5 years of experience with installing and using systems, both FAA and the industry are in a good position to complete their current effort to review overall aviation security needs as they relate to access control requirements and to change the requirements if necessary. As a next step, FAA and the industry can complete their ongoing work to develop and implement standards explaining how equipment and software should function to meet access control requirements.

In addition to ongoing initiatives, FAA can help ensure that systems are cost-effective by developing and implementing detailed guidelines explaining where system equipment should be placed. FAA officials can use the detailed guidance and standards as criteria to evaluate AIP funding requests and help ensure that these funds are used only for the system components needed to meet access control requirements.

Recommendations

To help ensure that systems are cost-effective, we recommend that the Secretary of Transportation direct the Administrator, FAA, to develop and implement detailed guidance based on the agency's access control requirements that explains where system equipment should be located.

[21]These standards are being developed through RTCA, Incorporated Special Committee 183. RTCA, Incorporated is a federal advisory committee that works with government and industry representatives to develop technical standards for aviation.

FAA should incorporate these guidelines and the standards being developed into its review process for Airport Improvement Program funding requests.

Agency Comments

We discussed our findings and recommendations with FAA's Assistant Administrator for Civil Aviation Security; Director of Civil Aviation Security Policy and Planning; Director of Civil Aviation Security Operations; Manager, Programming Branch, Airports Financial Assistance Division; and other Department of Transportation officials. These officials provided us with clarifying information, and we revised the text as necessary.

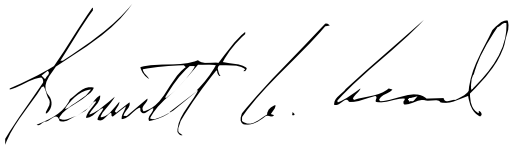
FAA officials were concerned that our statement that systems cost more than FAA initially had anticipated implies that the systems and the components used in them should have been less costly. We explained that our purpose is to present factual information on the different systems airports installed and that without detailed guidance and standards, it is difficult to determine if systems should have been less costly. FAA officials also stated their concern that achieving cost-effective systems means using the least expensive equipment. We stated that this is not our position and that systems may be cost-effective using equipment that is more expensive in the short term but lasts longer and performs better, resulting in less cost over time. FAA officials also expressed concern that using standards to assist in making AIP funding decisions would limit the agency's ability to accommodate security needs at individual airports. In our view, the standards would provide a baseline from which to begin evaluating funding requests and would not prohibit FAA from taking into account the access control needs of individual airports. Furthermore, FAA and the industry plan to develop standards that will accommodate the needs of all airports subject to access control requirements. Therefore, we believe that standards could allow for airport-by-airport decisions while still providing a tool to help ensure that systems are cost-effective. Finally, FAA officials noted that the appropriate use of access control systems by airport and airline employees is a critical factor in ensuring that such systems are effective. We concur with this position.

Scope and Methodology

We performed our review between October 1993 and January 1995 in accordance with generally accepted government auditing standards. All dollar amounts in this report have been adjusted to constant 1993 dollars. Additional details on our scope and methodology are contained in appendix IV.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 10 days after the date of this letter. At that time, we will send copies of this report to appropriate congressional committees; the Secretary of Transportation; the Administrator, FAA; the Director, Office of Management and Budget; and other interested parties. We will make copies available to others on request.

This report was prepared under the direction of Allen Li, Associate Director, who may be reached at (202) 512-3600. Other major contributors are listed in appendix V.



Kenneth M. Mead
Director, Transportation Issues

Contents

Letter	1
Appendix I 14 C.F.R. 107.14-Regulated Airports by FAA Region, as of August 1994	16
Appendix II Total Actual and Projected Costs for Access Control Systems by Year, as of August 1994	23
Appendix III Comparison of FAA's Initial Estimate for Access Control Systems With Airports' Actual and Projected Costs	24
Appendix IV Scope and Methodology	25
Appendix V Major Contributors to This Report	26

Abbreviations

AIP	Airport Improvement Program
C.F.R.	Code of Federal Regulations
FAA	Federal Aviation Administration
GAO	General Accounting Office

14 C.F.R. 107.14-Regulated Airports by FAA Region, as of August 1994

Alaskan Region

Anchorage International Airport
Aniak Airport
Barrow/Wiley Post-Will Rogers Memorial Airport
Bethel Airport
Cold Bay Airport
Cordova/Merle K. Smith Airport
Deadhorse Airport
Dillingham Airport
Fairbanks International Airport
Galena Airport
Juneau International Airport
Ketchikan International Airport
King Salmon Airport
Kodiak Airport
Kotzebue/Ralph Wien Memorial Airport
Nome Airport
Petersburg Airport
Saint Mary's Airport
Sitka Airport
Unalakleet Airport
Unalaska Airport
Wrangell Airport
Yakutat Airport

Central Region

Cedar Rapids Municipal Airport
Des Moines International Airport
Kansas City International Airport
Lambert-Saint Louis International Airport
Lincoln Municipal Airport
Omaha/Eppley Airfield
Sioux City/Sioux Gateway Airport
Springfield Regional Airport
Wichita Mid-Continent Airport

Eastern Region

Albany County Airport
Allentown/Bethlehem/Easton/Lehigh Valley International Airport
Atlantic City International Airport
Baltimore-Washington International Airport
Binghamton Regional Airport-Edwin A. Link Field
Charleston/Yeager Airport

Charlottesville-Albemarle Airport
Elmira/Corning Regional Airport
Erie International Airport
Greater Buffalo International Airport
Greater Rochester International Airport
Harrisburg International Airport
Huntington/Tri-State Airport-Milton J. Ferguson Field
Islip/Long Island MacArthur Airport
Ithaca/Tompkins County Airport
John F. Kennedy International Airport
La Guardia Airport
Lynchburg Regional Airport-Preston Glenn Field
Newark International Airport
Newburgh/Stewart International Airport
Newport News/Williamsburg International Airport
Norfolk International Airport
Philadelphia International Airport
Pittsburgh International Airport
Richmond International Airport-Byrd Field
Roanoke Regional Airport-Woodrum Field
Syracuse Hancock International Airport
Utica/Oneida County Airport
Washington Dulles International Airport
Washington National Airport
White Plains/Westchester County Airport
Wilkes-Barre/Scranton International Airport

Great Lakes Region

Akron-Canton Regional Airport
Appleton/Outagamie County Airport
Bismarck Municipal Airport
Champaign/University of Illinois Airport-Willard Field
Chicago Midway Airport
Chicago O'Hare International Airport
Cleveland-Hopkins International Airport
Dayton International Airport
Detroit City Airport
Detroit Metropolitan-Wayne County Airport
Duluth International Airport
Evansville Regional Airport
Fargo/Hector International Airport
Flint/Bishop International Airport

Fort Wayne International Airport
Grand Forks International Airport
Grand Rapids/Kent County International Airport
Greater Peoria Regional Airport
Greater Rockford Airport
Green Bay/Austin-Straubel International Airport
Indianapolis International Airport
Kalamazoo/Battle Creek International Airport
La Crosse Municipal Airport
Lansing/Capital City Airport
Madison/Dane County Regional Airport-Truax Field
Marquette County Airport
Milwaukee/General Mitchell International Airport
Minneapolis/Saint Paul International Airport
Minot International Airport
Moline/Quad City Airport
Mosinee/Central Wisconsin Airport
Oshkosh/Wittman Regional Airport
Port Columbus International Airport
Rapid City Regional Airport
Rochester Municipal Airport
Saginaw/Tri-City International Airport
Sioux Falls/Joe Foss Field
South Bend/Michiana Regional Transportation Center
Springfield/Capital Airport
Toledo Express Airport
Traverse City/Cherry Capital Airport
Youngstown-Warren Regional Airport

New England Region

Bangor International Airport
Boston/General E. L. Logan International Airport
Bradley International Airport
Burlington International Airport
Chicopee Airport
Manchester Airport
Portland International Jetport
Providence/Theodore F. Green State Airport
Tweed-New Haven Airport
Worchester Municipal Airport

Northwest Mountain Region

Aspen-Pitkin County Airport-Sardy Field
Bellingham International Airport
Billings Logan International Airport
Boise Air Terminal-Gowen Field
Bozeman/Gallatin Field
Butte/Bert Mooney Airport
Casper/Natrona County International Airport
City of Colorado Springs Municipal Airport
Denver International Airport
Denver/Stapleton International Airport
Durango-La Plata County Airport
Eagle County Regional Airport
Eugene/Mahlon Sweet Field
Grand Junction/Walker Field
Great Falls International Airport
Gunnison County Airport
Hayden/Yampa Valley
Helena Regional Airport
Idaho Falls/Fanning Field
Jackson Hole Airport
Kalispell/Glacier Park International Airport
Lewiston-Nez Perce County Airport
Medford-Jackson County Airport
Missoula International Airport
Moses Lake/Grant County Airport
Pasco/Tri-Cities Airport
Portland International Airport
Pueblo Memorial Airport
Redmond/Roberts Field
Salt Lake City International Airport
Seattle-Tacoma International Airport
Spokane International Airport
Yakima Air Terminal

Southern Region

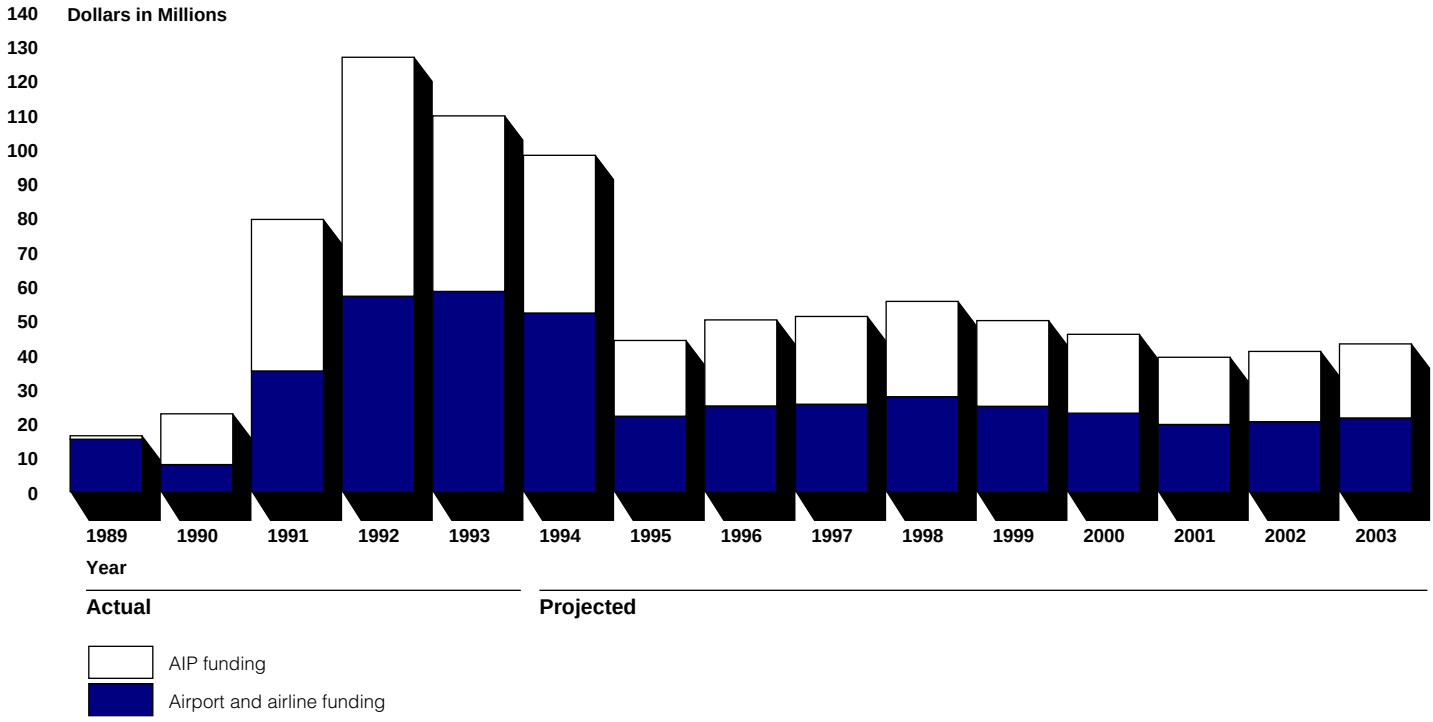
Aguadilla, Puerto Rico/Rafael Hernandez Airport
Asheville Regional Airport
Augusta/Bush Field Municipal Airport
Birmingham International Airport
Bristol/Johnson/Kingsport/Tri-City Regional Airport
Charleston International Airport
Charlotte Amalie, Virgin Islands/Cyril E. King Airport

Charlotte/Douglas International Airport
Chattanooga Metropolitan Airport
Christiansted, Virgin Islands/Alexander Hamilton Airport
Cincinnati/Northern Kentucky International Airport
Columbia Metropolitan Airport
Columbus Metropolitan Airport
Daytona Beach Regional Airport
Elgin Air Force Base
Fayetteville Regional Airport-Grannis Field
Fort Lauderdale-Hollywood International Airport
Fort Myers/Southwest Florida International Airport
Gainesville Regional Airport
Greensboro/Piedmont Triad International Airport
Greenville-Spartanburg Airport
Gulfport-Biloxi Regional Airport
Huntsville International Airport-Carl T. Jones Field
Jackson International Airport
Jacksonville/Albert J. Ellis Airport
Jacksonville International Airport
Kinston Regional Jetport
Knoxville/McGhee Tyson Airport
Lexington/Blue Grass Airport
Louisville/Standiford Field
Mayaguez, Puerto Rico/Eugenio Maria de Hostos Airport
Melbourne Regional Airport
Memphis International Airport
Miami International Airport
Mobile Regional Airport
Montgomery Airport-Dannelly Field
Myrtle Beach Jetport
Nashville International Airport
Orlando International Airport
Palm Beach International Airport
Panama City-Bay County International Airport
Pensacola Regional Airport
Ponce, Puerto Rico/Mercedita Airport
Raleigh-Durham International Airport
Saint Petersburg-Clearwater International Airport
San Juan, Puerto Rico/Luis Munoz Marin International Airport
Sarasota Bradenton International Airport
Savannah International Airport
Tallahassee Regional Airport

	Tampa International Airport
	The William B. Hartsfield Atlanta International Airport
	Wilmington/New Hanover International Airport
Southwest Region	Albuquerque International Airport
	Amarillo International Airport
	Austin/Robert Mueller Municipal Airport
	Baton Rouge Metropolitan Airport
	Corpus Christi International Airport
	Dallas/Fort Worth International Airport
	Dallas-Love Field
	El Paso International Airport
	Harlingen/Rio Grande Valley International Airport
	Houston Intercontinental Airport
	Houston/William P. Hobby Airport
	Lafayette Regional Airport
	Laredo International Airport
	Little Rock/Adams Field
	Lubbock International Airport
	McAllen-Miller International Airport
	Midland International Airport
	Monroe Regional Airport
	New Orleans International Airport-Moisant Field
	Oklahoma City/Will Rogers World Airport
	San Antonio International Airport
	Shreveport Regional Airport
	Tulsa International Airport
	Waco Regional Airport
	Wichita Falls Municipal Airport
Western-Pacific Region	Agana, Guam/Guam International Air Terminal
	Arcata/Eureka Airport
	Bakersfield/Meadows Field
	Burbank-Glendale-Pasadena Airport
	Elko Municipal Airport-J. C. Harris Field
	Fresno Air Terminal
	Hilo International Airport
	Honolulu International Airport
	Johnston Atoll Airport
	Kahului Airport

Keahole-Kona International Airport
Lake Tahoe Airport
Lanai Airport
Las Vegas/McCarran International Airport
Lihue Airport
Long Beach Airport-Daugherty Field
Los Angeles International Airport
Metropolitan Oakland International Airport
Monterey Peninsula Airport
Obyan, Northern Mariana Islands/Saipan International Airport
Ontario International Airport
Pago Pago, American Samoa/Pago Pago International Airport
Palm Springs Regional Airport
Phoenix Sky Harbor International Airport
Reno Cannon International Airport
Sacramento Metropolitian Airport
San Diego International Airport-Lindbergh Field
San Francisco International Airport
San Jose International Airport
Santa Ana/John Wayne Airport
Santa Barbara Municipal Airport
Tucson International Airport

Total Actual and Projected Costs for Access Control Systems by Year, as of August 1994



Comparison of FAA's Initial Estimate for Access Control Systems With Airports' Actual and Projected Costs

Dollars in millions[a]

Year	FAA's initial estimate	Airports' actual and projected costs[b]
1989	$ 28.4	$ 16.4
1990	60.0	22.7
1991	27.4	79.3
1992	25.9	126.7
1993	10.9	109.6
1994	11.7	98.1
1995	12.1	44.1
1996	11.9	50.1
1997	10.9	51.1
1998	11.7	55.6
Total	$211.0	$653.6

[a]Figures include airlines' costs. Figures for years 1989 through 1993 are actual. Figures for years 1994 through 1998 are projected.

[b]Figures do not sum to total because of rounding.

Source: FAA.

Scope and Methodology

To address our objectives, we performed work at FAA headquarters in Washington, D.C. We also met with officials at FAA's Central Region in Kansas City, Missouri; its Northwest Mountain Region in Seattle, Washington; Southern Region in Atlanta, Georgia; and Western-Pacific Region in Los Angeles and San Francisco, California. We visited 17 airports of varying size throughout the country. We interviewed executives and former executives of aviation industry associations, including those representing the interests of airports, airlines, and pilots. We attended a major conference in Nashville, Tennessee, at which we communicated our understanding of access control issues and sought the knowledge of airport managers.

We attended meetings of the Aviation Security Advisory Committee; the Committee's Universal Access System subgroup; and RTCA, Incorporated Special Committee 183. We conferred privately with these groups' members, which included senior FAA officials, aviation industry representatives, and system experts. At our request, FAA surveyed all 258 regulated airports to gather detailed data on the costs that airports and airlines have incurred to date and on costs that they anticipate incurring through the year 2003 for access control systems. We worked closely with FAA during all phases of its survey to understand the validity of the information. Finally, we reviewed the agency's regulations, policies, and procedures governing access control systems.

Major Contributors to This Report

Resources, Community, and Economic Development Division, Washington, D.C.	Robert E. Levin, Assistant Director M. Aaron Casey Charles R. Chambers
Seattle Regional Office	Randall B. Williamson, Assistant Director Lisa C. Dobson Dana E. Greenberg

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 1100
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, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (301) 258-4097 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Mail
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested