United States General Accounting Office

GAO

Report to the Chairman and Ranking Minority Member, Committee on Science, House of Representatives

May 2000

COMPUTER SECURITY

FAA Is Addressing Personnel Weaknesses, But Further Action Is Required

G A O

Accountability * Integrity * Reliability

G A O
Accountability * Integrity * Reliability

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

Accounting and Information
Management Division

B-285276

May 31, 2000

The Honorable James F. Sensenbrenner, Jr.
Chairman
The Honorable Ralph M. Hall
Ranking Minority Member
Committee on Science
House of Representatives

Electronic information and automated systems are essential to virtually all major federal operations. If agencies cannot protect the accessibility, integrity, and, in some cases, the confidentiality of this information, their ability to carry out their missions could be severely impaired.

The successful operation of the National Airspace System (NAS)—the network supporting U.S. aviation operations that includes navigation facilities, airports, equipment, services, and information and rules—is dependent on the Federal Aviation Administration's (FAA) air traffic control (ATC) computer systems. These systems provide information to air traffic controllers and aircraft flight crews to ensure safe and expeditious movement of aircraft. Failure to adequately protect these systems, as well as the facilities that house them, could cause nationwide disruption of air traffic or collisions.

As requested, this report assesses FAA's efforts to address personnel security issues. FAA's personnel security policy requires that background searches be conducted for all FAA federal employees and for contractor employees who have some level of risk associated with their positions. In December 1999, we reported that the agency had not performed risk assessments as required by the policy nor had it performed background searches on all contractor employees.[1] In response to your subsequent February 2000 request, our objectives on this current review were to determine (1) the factors that contributed to FAA's failure to adhere to the requirements of its personnel security program which requires background searches—investigations or checks—of contractor employees commensurate with the risk level of the tasks to be performed; (2) whether

[1] *Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software* (GAO/AIMD-00-55, December 23, 1999).

FAA's "five layers of system protection" concept[2] is a generally accepted security framework reflective of its security policies and procedures; and (3) the extent of FAA's compliance with the requirements of its personnel security program concerning background searches for FAA and contractor employees at all agency facilities.

Results in Brief

Key factors contributing to FAA's failure to comply with its policy on personnel security were (1) insufficient management support, (2) insufficient user awareness and training on personnel security, and (3) inadequate policy enforcement activities. FAA has since made progress in addressing these shortcomings. As a result of our prior review, agency management issued a memorandum promoting adherence to the policy and has worked with security personnel to revise applicable contract provisions and conduct briefings to make staff aware of the policy and its requirements. In addition, security personnel have been tasked with conducting compliance audits semi-annually beginning in September 2000 to determine adherence to the policy. Nevertheless, FAA still lacks a personnel security training program and quality assurance function to ensure consistency in policy implementation and to prevent noncompliance.

Although FAA did not comply with key requirements of its personnel security policy, FAA concluded that the risk of intrusion is extremely low because of the agency's five layers of system protection concept. This concept is currently being promoted by FAA's Chief Information Officer (CIO) and is expected to be used as the future basis for addressing information systems security within the agency. While this concept is not a generally accepted security framework supported entirely by policies and procedures, it appears to be a logical overview to understanding computer security at FAA. However, there are known weaknesses within each individual layer that could negatively affect the operational efficiency of the NAS.

As for the agency's compliance in implementing its personnel security policy requiring background searches on FAA and contractor employees, the agency is making progress but still needs to complete the required background searches for a substantial number of contractor employees.

[2] FAA's Chief Information Officer introduced the five layers of system protection concept as an approach to understanding how the agency protects its systems.

According to its records, which we did not verify, FAA has completed the required background searches for 98 percent of its approximately 48,000 federal employees, but does not yet know the full extent of contractor employees who lack the necessary background checks. Because determining who needs a background search is a time-consuming process, FAA has chosen to focus on contracts supporting its 435 mission-critical systems. While FAA has not yet completed this exercise, the agency has identified 435 positions that warrant some form of background search—90 percent of which require only a fingerprint check. Each of these positions may correspond to several individuals, and it is now up to the contractors to determine the number of employees in these positions and to obtain the necessary information to initiate the background searches. FAA's contracting organization plans to complete its risk assessment activities by September 2000 for all contracts. However, the actual background searches, which can take anywhere from 1 week to 4 months, will still need to be completed by either the Office of Personnel Management or the Federal Bureau of Investigation. Until this effort is completed, FAA's facilities, information, and resources will remain exposed to contractor employees who have not received the required background searches.

Given FAA's past personnel security problems and the fact that much remains to be done to implement its policy, we are making recommendations to develop, implement, and require official training on personnel security; to establish a quality assurance process to oversee and ensure effective implementation of its personnel security policy throughout the contracting process; and to evaluate the adequacy of staffing and resources to ensure implementation and enforcement of this policy. In commenting on a draft of this report, senior Department of Transportation (DOT) and FAA officials generally agreed with our recommendations in these areas and plan to implement the necessary corrective actions.

Background

FAA's primary mission is to ensure safe, orderly, and efficient air travel throughout the United States. Its ability to fulfill this mission depends on the adequacy and reliability of the nation's ATC system, a vast network of computer hardware, software, and communications equipment that provides information to air traffic controllers and aircraft flight crews. The ATC network is an enormous, complex collection of interrelated systems, including navigation, surveillance, weather, and automated information processing and display systems that reside at, or are associated with, hundreds of facilities. Complex communications networks that separately transmit both voice and digital data interconnect these systems and facilities. As we reported in 1997 and 1999, while the use of interconnected systems promises significant benefits in improved government operations, it also increases vulnerability to anonymous intruders who may manipulate data to commit fraud, obtain sensitive information, or severely disrupt operations.[3]

Within the agency, three organizations have a role in implementing FAA's personnel security policy. The Office of Human Resource Management is responsible for determining the type of background search to be conducted for federal employees based on their position descriptions and then forwarding this information to the Office of Civil Aviation Security. The Office of Research and Acquisitions is responsible for ensuring that risk assessments and position risk forms are completed for all contractor employees and forwarded to the Office of Civil Aviation Security. The Office of Civil Aviation Security wrote the policy and is responsible for implementing it by coordinating with outside investigative entities to ensure that background searches are conducted and the results are entered into the appropriate database.

In December 1999, we reported that FAA was not following sound personnel security practices and, as such, had increased the risk that inappropriate individuals may have gained access to its facilities, information, or resources.[4] FAA's policy requires system owners and users to prepare risk assessments for all contractor tasks, and to conduct background investigations for all contractor employees in high-risk positions. The policy requires more limited background checks for moderate- and low-risk positions. However, we found that FAA did not perform all the necessary risk assessments and was unaware of whether it or the contractor had performed background searches on all of the contractor employees. Further, we found instances where background searches were not performed. For example, no background searches were performed on 36 mainland Chinese nationals who reviewed the source code of eight mission-critical systems.

[3] *High-Risk Series: Information Management and Technology* (GAO/HR-97-09, February 1997) and *High-Risk Series: An Update* (GAO/HR-99-1, January 1999).

[4] GAO/AIMD-00-55.

To address these issues, we made recommendations to the FAA Administrator to improve the agency's security controls, identify the risk of malicious attacks on critical systems, and mitigate this risk. FAA agreed with these recommendations and is working to address them.

Several Factors Contributed to FAA's Noncompliance With Its Personnel Security Policy

FAA did not consistently adhere to the requirements outlined in its personnel security policy for three key reasons—insufficient management support, lack of user awareness and training on the policy's requirements, and inadequate policy enforcement. According to FAA security officials, the agency's contracting office had not previously encouraged contracting officers in headquarters to adhere to the requirements outlined in the policy regarding contractor personnel suitability.[5] These security officials noted that management should have been aware of the policy requirements because FAA's policy approval process requires each line of business to review the policy, provide comments, and sign-off on the final policy denoting review and understanding. They noted, however, that there has been internal resistance to implementing the security measures within the policy because of the amount of time and resources required. According to security officials, contracting personnel may be concerned that the security office will impede FAA's ability to meet its commitments because key documents must be reviewed and approved by security personnel, and there is currently only one security staff person performing these reviews. However, there has been progress in gaining management support for personnel security. As a result of our prior review, the contracts organization directed its personnel to adhere to the policy and issued a memorandum outlining the priority of tasks to be performed.

As for FAA's lack of awareness and training on personnel security, the Special Assistant to the Director of Contracts noted that security management had not made staff aware of the policy requirement and that the policy had not been included in the Acquisition Management System, an online tool used by FAA's contracting officers. Further, there was no training related to implementation of the policy. Specifically, this individual noted that the policy was confusing and did not clearly delineate the tasks to be performed for contractor employees. To ensure policy adherence, FAA has since revised one key contract provision to outline the tasks to be performed by both the contractors and FAA's contracting officers. Also,

[5] According to FAA security and contracting officials, there has been greater adherence to the policy by the regions and centers than at FAA headquarters.

security officials have held awareness briefings to provide an overview of the requirements of the policy; however, these briefings do not provide detailed guidance on the specific tasks to be performed and, according to FAA, are not considered official training. The purpose of training is to teach individuals the skills that will enable them to perform their jobs—what they need to do and how to do it. With adequate training, individuals are more likely to perform their duties appropriately and consistently.

As for FAA's lack of policy enforcement, senior security officials acknowledged that there has been no formal enforcement of the policy. The Associate Administrator for Civil Aviation Security stated that his enforcement authority extends only to regulated entities, not to internal FAA organizations. He maintained that only the FAA Administrator has the authority to enforce policy within the agency. Further, officials within the security operations group stated they do not have the staff or resources to conduct reviews or quality assurance activities to ensure that contracting officers have evaluated all contractor positions to determine if background searches are needed and if the correct forms have been provided to security.

In response to our December report, the security operations group is planning to conduct compliance reviews every 6 months to determine policy compliance. The security office will begin developing its plans for conducting these audits in July 2000, with the expectation of conducting its first review in September 2000. However, according to security officials, they will be unable to conduct these audits unless additional staff are made available.[6]

While FAA's compliance audits, if conducted, will likely provide valuable information on its efforts to implement the personnel security policy, an effective quality assurance process could prevent instances of noncompliance from initially occurring. An effective quality assurance function would ensure that appropriate coordination occurs between the security and contracting functions before a contract is awarded. This coordination would enable both the security and contracting functions to discuss and implement the requirements of the policy prior to actual contract award. The compliance audit would then be more meaningful in

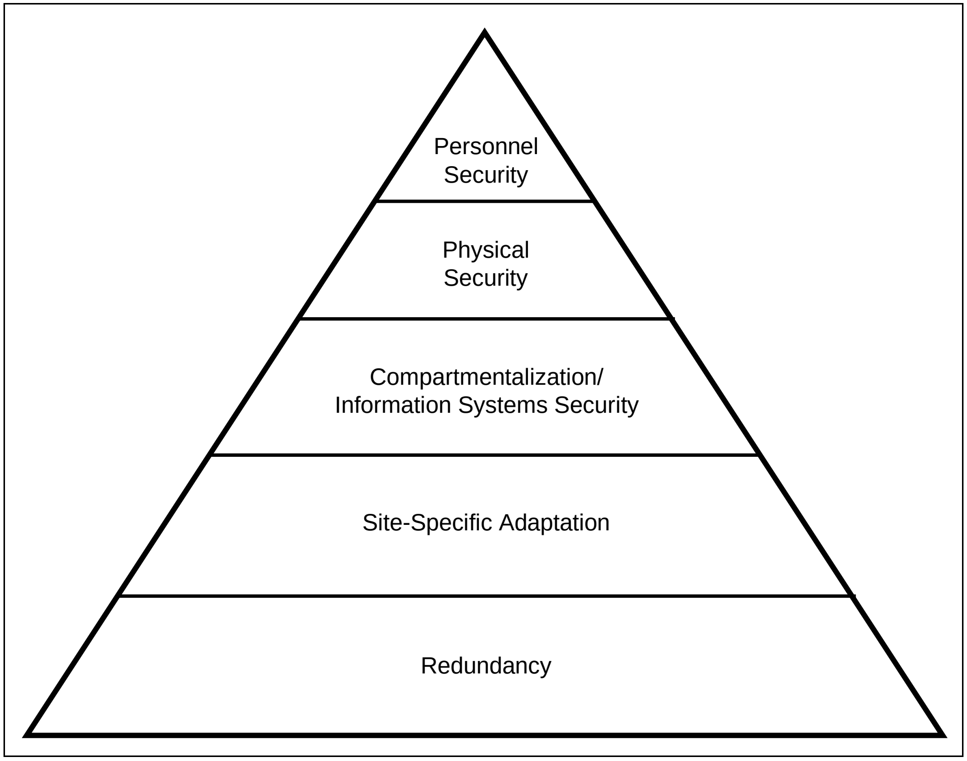
[6] The organization responsible for performing these compliance audits has three employees, with only one individual responsible for reviewing key documents (e.g., risk assessments for each contractor position).

confirming whether this coordination occurred and that all security requirements were implemented in accordance with the policy. However, FAA currently has no plans to implement a comprehensive quality assurance function.

FAA's Five Layers of System Protection Is a Concept That Partially Reflects Security Policies

Although FAA did not comply with its policy requiring background searches for contractor employees, the agency concluded that the risk of intrusion was extremely low because of its five layers of system protection. The CIO explained the five layers of system protection using a diagram developed specifically for the House Committee on Science in December 1999. According to the CIO, the five layers of system protection concept is an approach to understanding how the agency protects its systems. Two of the five layers (physical and personnel security) are based on policies, while one layer (compartmentalization/information systems security) is based on both the unique nature of the ATC environment and policy. The remaining two layers (site-specific adaptation and redundancy) reflect the unique nature of the ATC environment rather than policies. Figure 1 illustrates the five layers.

Figure 1: FAA's Five Layers of System Protection



The following provides a brief description of each layer:

- Personnel security is designed to ensure that personnel who have sensitive roles or access to sensitive information are trustworthy, which would include ensuring that appropriate background searches on contractors and subcontractors have been conducted.
- Physical security is designed to ensure that FAA facilities are safe from unauthorized physical access and physical harm. Unescorted access should only be allowed for properly authorized and screened personnel.

- In the compartmentalization/information systems security layer, compartmentalization refers to the unique design of the ATC system which prevents a breach of one facility from impacting other facilities. For example, each of the 20 centers that manage long-distance air traffic operates collaboratively but independently. According to the CIO, this means that if one center was disabled, the other 19 would still operate. Information systems security is based on a policy dated February 7, 1989, covering automated information systems security.[7]
- Site-specific adaptation refers to “preference settings” or adjustments that are made at each facility to meet its specific requirements, such as runway headings or aircraft displays. These adaptations do not change the computer source code, but rather allow each site to adapt or configure the system to meet its specific requirements. FAA officials acknowledge that inaccurate data can be input into the system and that a system could fail as a result of an intrusion; however, these officials said that actual computer source code could not be changed.
- Redundancy refers to the fact that there is no single point of failure within the NAS. There are primary and secondary systems, as well as manual procedures for backup. FAA officials acknowledged that switching from a primary system to a backup system or to manual procedures often results in delays, but stressed that they would not compromise aviation safety.

FAA’s CIO stated that despite the geometric shape, each layer is considered equally important in addressing security and that the combination of all five layers provides robust security for the NAS. The CIO is working to promote this concept from an idea to a more generally accepted framework and expects this concept to be used in planning future systems. In addition, the CIO believes that this approach is transferable to other government agencies and is currently working on an article for a National Research Council publication to introduce this concept. However, although the CIO has asserted that each layer is equally important, FAA’s use of a pyramid to visually depict this concept could make it appear that personnel security is the least important layer.

[7] An updated order has been developed and is expected to be issued mid-year 2000, according to the CIO. This new order establishes a high-level Information Systems Security Program policy and assigns organizational and management responsibilities that ensure implementation of the Computer Security Act of 1987.

In addition, the CIO has acknowledged that there is currently greater security at the lower layers of the pyramid than at the top, and that personnel security is the easiest layer to breach. FAA management has also acknowledged that as systems become more interconnected, inherent protections derived from the unique nature of the ATC environment (e.g., compartmentalization) will be lost. Accordingly, it will be imperative that FAA's computer security program (i.e., personnel, physical, and information systems security) has been effectively implemented to prevent unauthorized access to facilities, information, and resources.

While the concept of having a combination of security layers is a logical approach to understanding and addressing computer security at FAA, there are known weaknesses within each individual layer of the pyramid. For example, as evidenced by this review and our December 1999 report, FAA has failed to comply with its personnel security policy thereby increasing the risk that inappropriate individuals may gain access to its facilities, information, or resources.[8] Further, in May 1998, we reported that FAA was not effectively managing physical security at ATC facilities, placing property and the safety of the flying public at risk.[9] With regard to compartmentalization, the failure of any one facility potentially affects the operational efficiency of the NAS resulting in flight delays, possibly even cancellations, and customer dissatisfaction. Also, while site-specific adaptations may add a measure of system protection, FAA officials have acknowledged that intrusions could occur and that these intrusions could result in system failures potentially affecting NAS operations. As for redundancy, the failure of primary systems can and generally does impact the operational efficiency of the NAS. For example, the recent radar failure at Logan International Airport in Boston resulted in flight delays and cancellations—the number of landings per hour was reduced by half.

In commenting on a draft of this report, senior DOT and FAA officials acknowledged that weaknesses within the individual layers could negatively impact operational efficiency, but reiterated that the combination of all five layers of the pyramid provides robust security for the NAS. These officials emphasized that the primary focus of their security efforts is safety. We will continue to evaluate the five layers of system

[8] GAO/AIMD-00-55.

[9] *Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety* (GAO/AIMD-98-155, May 18, 1998).

protection as part of our ongoing review of the agency's progress in addressing computer security weaknesses.

FAA Has Made Progress in Implementing Its Personnel Security Policy, But Much Remains to Be Done

FAA's personnel security policy requires that background searches be conducted for all federal employees and for contractor employees who have some level of risk associated with their positions. Agency reports show that FAA is largely in compliance internally and is making progress to ensure compliance for contractor employees; however, much remains to be done to implement the policy.

Agency reports show that FAA has complied with the policy for the vast majority of its federal employees. The agency maintains investigation status information in its Consolidated Personnel Management Information System which, as of April 12, 2000, showed background searches had been completed for all but 879 (1.83 percent) of FAA's approximately 48,000 federal employees. FAA officials were unable to explain why there were no records on clearance status for these individuals, but committed to providing an explanation by June 15, 2000.

As for contractor employees, potentially thousands have not yet undergone the required background searches. In January 2000, FAA estimated that it had over 28,000 existing contracts and purchase orders under which approximately 38,000 contractor employees were engaged. However, according to the agency's database on contractor personnel, background searches have been performed for only 16,000 contractor employees since 1996, which—even with the unlikely assumption that all of these people are still employed—is less than half of the current contractor employee population. FAA could not provide an exact estimate of how many individuals still lack the required background searches because it has not yet completed assessing the risk associated with contractor employees' positions.

While FAA acknowledged that it did not consistently comply with the requirements of its personnel security policy, security and contracting officials stated that the agency now firmly requires that all new contracts meet the policy. Further, FAA is working to implement the policy requirements on the backlog of active contracts that do not meet the requirements. While the agency plans to eventually bring all active contracts into compliance with its policy, since December 1999, FAA's contracting office has primarily focused its efforts on the agency's 435 mission-critical systems.

Bringing these contracts into compliance is a complicated and time-consuming process. The contracting office must first identify the contracts supporting these mission-critical systems. The office then must assess the sensitivity of the contract tasks, and if there is a degree of sensitivity, the applicable FAA contracting officer must prepare a form describing the risk associated with each specific position description. This position-specific risk assessment determines which type of background search is required. For example, a low-risk position warrants a fingerprint check, a medium-risk position warrants a more thorough background check, and a high-risk position warrants a complete background investigation. Once this position assessment has been completed, these forms are sent to the contractor to compile the necessary information on all individuals under that position description. Upon receipt of this information, the security office will forward the information to the appropriate investigative agency—the Federal Bureau of Investigation or the Office of Personnel Management. It is only then that the appropriate background search can be initiated.

As of May 2000, FAA has been able to identify contracts supporting 255 of its 435 mission-critical systems.[10] Of the 255 systems, FAA officials have determined that 98 systems have contracts of sufficient sensitivity to warrant position-specific risk assessments. FAA has completed this effort on 69 of the 98 systems, triggering 435 position-specific risk assessment forms—most of which have been deemed low risk. Because more than one individual can have the same position description, this may involve performing background searches for more than 435 individuals. To date, FAA's security office has received the completed background forms needed to conduct the background searches for only 100 individual contractor employees. FAA's contracting organization plans to complete its risk assessment activities by September 2000 for all contracts. However, the actual background searches, which can take anywhere from 1 week to 4 months, will still need to be completed by either the Federal Bureau of Investigation or the Office of Personnel Management. Until this work is completed, contractor employees who have not received background searches will continue to have access to FAA's facilities, information, and/or resources.

[10] For the remaining 180 mission-critical systems, FAA is working to identify the contracts associated with these systems.

Conclusions

FAA failed to comply with its personnel security program because of insufficient management support, insufficient user awareness and training, and inadequate policy enforcement. While the agency is working to address these shortcomings and to bring the agency's many contracts into compliance with the personnel security policy, much remains to be done. Specifically, the agency does not have a training program or quality assurance function to ensure policy implementation and enforcement. In addition, while the five layers of system protection concept may be a logical overview of security at FAA, there are known weaknesses within each layer. Further, the agency does not know the full extent of the number of contractor employees needing background searches. Accordingly, FAA remains at risk that inappropriate individuals may gain or continue to have access to its facilities, information, or resources. Fully addressing this risk and ensuring implementation and enforcement of security policies will take time and resources.

Recommendations

In order to address weaknesses in the implementation and enforcement of its personnel security program, we recommend that the Secretary of Transportation direct the FAA Administrator to:

- establish a user awareness and training program that clearly delineates the requirements of the policy and directs staff in the tasks to be performed in adherence to the policy. All staff responsible for implementation of the policy should receive the baseline training as well as periodic updates on the security requirements, especially when policy changes occur.
- establish a quality assurance process that will focus on implementation of the requirements outlined within the personnel security policy. This process should ensure that all contract tasks and the respective contractor positions are evaluated in terms of risk and that the appropriate forms are completed and background searches are initiated and completed for the contractor employees assigned to perform work under the contract.
- evaluate resource needs for ensuring implementation and enforcement of security policies (e.g., user awareness and training, review of position risk designation forms, compliance audits).

Agency Comments and Our Evaluation

Senior DOT and FAA officials, including a representative from DOT's Office of the Chief Information Officer and FAA's Chief Information Officer and Associate Administrator for Civil Aviation Security, provided comments on a draft of this report. These officials generally agreed with our findings and recommendations and offered suggestions on how they plan to implement the necessary corrective actions. They also offered specific comments, which we have incorporated as appropriate throughout the report.

Objectives, Scope, and Methodology

Our objectives were to determine what factors contributed to the agency's noncompliance with its personnel security program, whether FAA's five layers of system protection is a generally accepted security framework reflective of its security policies and procedures, and the extent of FAA's compliance with its personnel security program concerning background investigations for FAA and contractor employees.

To determine what factors contributed to FAA's noncompliance with its personnel security policy, we met with officials in the Office of Civil Aviation Security and the Office of Research and Acquisitions, and requested explanations as to why the policy was not adhered to. We also analyzed information on plans to change the requirements outlined within the policy and the respective clauses, as well as the agency's plans to conduct training and compliance audits. To determine whether FAA's five layers of system protection concept was a generally accepted security framework reflective of its security policies and procedures, we met with officials within the offices of Information Services/Chief Information Officer and Air Traffic Services to discuss the concept and its applicability to FAA's security program, and analyzed information applicable to each individual layer to assess its effectiveness. To assess the extent of the agency's compliance with its personnel security program concerning background investigations for FAA and contractor employees, we analyzed information detailing the status of risk assessments and background searches provided by agency officials within the offices of Civil Aviation Security; Research and Acquisitions; Human Resource Management; and Policy, Planning, and International Aviation.

We conducted our work at FAA headquarters in Washington, D.C. from March through May 2000 in accordance with generally accepted government auditing standards. We provided a draft of this letter to DOT and FAA for comment and have incorporated their comments as appropriate throughout this report.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this report. At that time, we will send copies to Senator Slade Gorton, Senator Frank R. Lautenberg, Senator Joseph I. Lieberman, Senator John D. Rockefeller IV, Senator Richard C. Shelby, and Senator Fred Thompson, and to Representative James A. Barcia, Representative John J. Duncan, Representative Steven Horn, Representative William O. Lipinski, Representative Constance A. Morella, Representative Martin O. Sabo, Representative Jim Turner, and Representative Frank R. Wolf in their capacities as Chair or Ranking Minority Member of Senate and House Committees and Subcommittees. We are also sending copies of this report to the Honorable Rodney E. Slater, Secretary of Transportation; the Honorable Jane F. Garvey, Administrator of the Federal Aviation Administration; and the Honorable Jacob J. Lew, Director of the Office of Management and Budget. Copies will be made available to others upon request.

If you have any questions on matters discussed in this report, please call me at (202) 512-6408 or Colleen Phillips, Assistant Director, at (202) 512-6326. We can also be reached by e-mail at *willemssenj.aimd@gao.gov* and *phillipsc.aimd@gao.gov*, respectively. Key contributors to this assignment were Nabajyoti Barkakati, Cynthia Jackson, and Keith Rhodes.

Joel Willemssen

Joel C. Willemssen
Director, Civil Agencies Information Systems

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

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 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

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 (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with “info” in the body to:

info@www.gao.gov

or visit GAO’s World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- Web site: http://www.gao.gov/fraudnet/fraudnet.htm
- e-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

PRINTED ON ♻ RECYCLED PAPER

[redacted]