

GAO

Report to the Committee on Science,
House of Representatives

August 2000

FAA COMPUTER SECURITY

Concerns Remain Due to Personnel and Other Continuing Weaknesses





B-285620

August 16, 2000

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

The Federal Aviation Administration (FAA) continues to face challenges in the area of computer security in general and personnel security in particular. In recent years, we have issued three reports¹ disclosing significant weaknesses in key components of FAA's computer security program and, at your request, our work in this area is continuing. We are currently assessing the effectiveness of FAA's overall computer security program.

As requested, the purpose of this report is to provide an interim update on the status of FAA's computer security efforts. Specifically, our objectives are to discuss (1) FAA's history of computer security weaknesses, as described in our May 1998 and December 1999 reports, and our prior recommendations to address those weaknesses, (2) FAA's progress in implementing our recommendations and its own personnel security policy, including our assessment of the adequacy of these actions, and (3) the preliminary results of our ongoing work.

Results in Brief

FAA has a history of computer security weaknesses in a number of areas, including its physical security management at facilities that house air traffic control (ATC) systems, systems security for both operational and future systems, management structure for implementing security policies, and personnel security. Over the last 3 years, we have made 22 recommendations to FAA to address these security weaknesses.

¹*Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety* (GAO/AIMD-98-155, May 18, 1998), *Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software* (GAO/AIMD-00-55, December 23, 1999), and *Computer Security: FAA Is Addressing Personnel Weaknesses, But Further Action Is Required* (GAO/AIMD-00-169, May 31, 2000).

While FAA is working to address computer security weaknesses, its progress has been slow in key areas. Our ongoing work is finding that FAA still has much to do in the areas of physical, systems, and personnel security. Specifically, the agency has not yet completed efforts to accredit its facilities and systems as secure, and has not yet completed background checks on thousands of contractors actively working on FAA contracts. Until it does so, the agency will continue to have undue exposure to intrusions and malicious attacks on its facilities, information, and resources. We will continue to evaluate FAA's progress in addressing our recommendations and to determine whether additional recommendations are warranted.

FAA's Computer System Integrity: A Cornerstone of the National Airspace System

FAA's primary mission is to ensure safe, orderly, and efficient air travel throughout the United States; its ability to do this 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. It is this system upon which the National Airspace System—NAS—depends.² The ATC network is an enormous, complex collection of interrelated systems—including navigation, surveillance, weather, and automated information processing and display—located at or associated with hundreds of facilities. These systems and facilities are linked by complex communications networks that separately transmit both voice and digital data. As we reported in 1997 and 1999, while such interconnectivity offers significant benefits in improved government operations, it also increases vulnerability to intruders who may manipulate data to commit fraud, obtain sensitive information, or severely disrupt operations.³ Failure to adequately protect these systems, and the facilities that house them, could increase the risk of regional or nationwide disruption of air traffic—or even aircraft collisions.

Responsibility for security within FAA is dispersed: The Office of Civil Aviation Security is responsible for physical and personnel security policy; the Chief Information Officer (CIO) is responsible for information systems

²NAS is the network that supports U.S. aviation operations—facilities, airports, equipment, services, information, and rules.

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).

security; and the individual lines of business are responsible for implementing security policies. Without adequate coordination, this dispersed responsibility adds to security risk.

FAA Has a History of Computer Security Weaknesses

In 1997, amid concerns over unauthorized access to FAA's ATC systems and facilities, we were asked to determine whether the agency was effectively managing computer security. On April 29, 1998, we issued a "Limited Official Use" report that discussed FAA's computer security weaknesses in detail. We subsequently summarized these weaknesses in a publicly available report,⁴ as follows:

- Physical security management and controls at facilities that house ATC systems are ineffective;
- Systems security—for both operational and future systems—are ineffective, rendering systems vulnerable; and
- FAA's management structure for implementing and enforcing computer security policy is ineffective.

For example, known physical security weaknesses at one ATC facility included unauthorized personnel being granted unescorted access to restricted areas. Further, FAA did not know about vulnerabilities at some 187 other facilities because security controls had not been assessed since 1993. In the area of systems security, FAA was in violation of its own policy; as of 1996, it had performed the necessary analysis to determine system threats, vulnerabilities, and safeguards on only 3 of its 90 operational ATC computer systems. FAA was likewise not effectively managing the security of future ATC systems modernization efforts because it did not consistently include well-defined security requirements in its specifications, as its policy mandates. Further, FAA's overall management structure and implementation of policy for ATC computer security was not effective. Responsibilities were dispersed among three entities within the agency, all of which were remiss in their ATC security duties.

More recently, we evaluated FAA's status on another element of computer security—personnel security—in our December 1999 report. That report disclosed that FAA was not following its own personnel security practices and, thus, had increased the risk that unauthorized individuals may have

⁴GAO/AIMD-98-155, May 18, 1998.

gained access to its facilities, information, or resources.⁵ FAA's policy requires system owners and users to prepare risk assessments for all contractor tasks, and to conduct background investigations of all contract employees in high-risk positions; it requires less thorough background checks for moderate- and low-risk positions. FAA did not, however, perform all required risk assessments, and was unaware of whether background searches had been performed on all contract employees. We found instances in which background searches were not performed—including on 36 mainland Chinese nationals who reviewed the computer source code of eight mission-critical systems as part of FAA's effort to ensure Year 2000 readiness. By again not following its own policies, FAA increased the exposure of its systems to intrusion and malicious attack.

In our 1998 and 1999 reports, we made 19 recommendations to, among other things, address weaknesses in

- physical security—by inspecting all ATC facilities that had not been recently inspected, correcting any identified weaknesses, and accrediting these facilities;⁶
- operational ATC systems security—by assessing, certifying, and accrediting⁷ all systems by April 30, 1999, and at least every 3 years thereafter, as required by federal policy;
- future ATC systems security—by including well-formulated security requirements in the specifications for all new ATC systems;
- security management—by developing an effective CIO management structure for implementing and enforcing computer security policy; and
- personnel security—by tightening controls over contract employees by ensuring that appropriate background searches are performed.

⁵GAO/AIMD-00-55, December 23, 1999.

⁶At the time of our review, FAA's policy required that ATC facilities be inspected to determine if they met physical security standards. This inspection then served as the basis for accrediting a facility—concluding that it is secure.

⁷System certification is the technical evaluation that is conducted to verify that FAA systems comply with security requirements. Certification results are one factor management considers in deciding whether to accredit systems. Accreditation is the formal declaration that the appropriate security safeguards have been properly implemented and that the residual risk is acceptable.

FAA Is Acting to Reduce Vulnerabilities, But Critical Steps Unfinished

FAA is acting to address our recommendations, but its progress in some areas has been slow. As a result, a great deal must still be accomplished to reduce FAA's exposure to intrusions or malicious attacks on its facilities, information, and resources.

Progress Noted in Physical Security, Systems Security, and Security Management, Yet Important Work Remains Incomplete

FAA has made progress since our 1998 report, but much still remains to be done. In the area of physical security, FAA has inspected the remaining facilities that had not been assessed since 1993 and has accredited 297 key facilities. However, in March 1999, FAA implemented a new policy governing the accreditation of its facilities, which requires that a facility undergo a more stringent, detailed assessment prior to its accreditation. Accordingly, FAA officials noted that all facilities that had been inspected and accredited under the prior policy will need to be assessed and reaccredited under the revised policy. According to FAA officials, as of June 12, 2000, 223 staffed ATC facilities⁸ have been assessed and 9 have been accredited under the new policy. These officials noted that the 223 facilities that have been assessed include all of the larger ATC facilities. While FAA officials determined that the number of ATC facilities that have not yet been assessed is too sensitive to release publicly, they acknowledge that the agency still has to assess and accredit many facilities under its new policy. According to FAA officials, the agency expects to complete all of its facility assessments by the end of 2002 and has set a goal of accrediting 66 facilities by September 30, 2000,⁹ and the remaining facilities by 2005. Until its assessments and accreditations are completed, FAA cannot ensure that the appropriate controls are in place to prevent loss or damage to FAA property, injury to FAA employees, or compromise of FAA's capability to perform critical air safety functions.

In the area of operational systems security, FAA is working to identify and address systems vulnerabilities. As part of this effort, the agency is proceeding to perform risk assessments on ATC systems, and then to

⁸ATC facilities include towers, terminal radar approach control facilities, en route centers, center approach control facilities, radar approach control facilities, flight service stations, and radar sites.

⁹FAA's goal of accrediting 66 facilities includes both ATC and non-ATC facilities, such as office buildings.

certify and accredit them. However, out of about 90 operational ATC systems, only 37 have had some form of risk assessment,¹⁰ 9 have been certified, and 8 have been accredited. Further, although FAA's information security policy requires that each system have a risk assessment, a security plan, a mitigation plan, and a contingency plan prior to accreditation, five of the eight accredited systems were granted interim, 1-year accreditations because they lacked one or more of the required documents. Because FAA has made little progress in assessing and accrediting its operational systems, the agency does not know how vulnerable many of its systems are and has little basis for determining what additional protective measures are required. As a result, operational ATC systems may not be adequately protected from intrusion and malicious attacks.

In response to our recommendation to include well-formulated security requirements in the specifications for all new ATC systems, FAA has drafted information security requirements and an information systems security architecture. Both are intended to provide guidance for building security into new systems. We are continuing to evaluate FAA's progress in this area.

Finally, to address security management weaknesses, FAA has established a CIO position and a management structure in which the CIO reports directly to the Administrator. Further, the CIO was given responsibility for developing and implementing FAA's information security policy and for overseeing its information security budget. As a result, FAA now has a central focal point for its information security program. The CIO office has issued a new information systems security policy and has drafted an information systems security architecture.

Federal Employee Background Searches Appear to Be Virtually Complete

In addition to its efforts on facilities and systems security, FAA is working to ensure personnel security among its federal employees. FAA's personnel security policy requires that (1) background searches be conducted for all federal employees and (2) the type of search performed be appropriate for each individual's position. Specifically, the agency requires a minimum of a National Agency Check and Inquiries (NACI) for all low- and moderate-risk

¹⁰FAA officials reported that they have completed comprehensive risk assessments on 8 operational systems and that another 12 systems' assessments have been initiated but have not yet been completed. FAA also performed more limited risk assessments on 17 other operational systems, although agency officials acknowledged that these systems will need to undergo comprehensive risk assessments prior to certification and accreditation.

positions. A NACI entails checking prior and current residences, previous employment, references, law enforcement records, and fingerprints. Higher risk positions warrant even more thorough background investigations.

Agency reports show that FAA has largely complied with the segment of its policy requiring checks for all federal employees. According to its records, FAA has completed background searches for 98 percent of its approximately 48,000 federal employees.¹¹

Determining whether FAA performed the appropriate type of background search is more complicated. According to FAA records, the agency conducted NACI checks or more thorough background investigations on over 95 percent of its federal employees. We reviewed the documentation associated with 30 individuals¹² and found that they appear to have received the proper background checks. Given the limited number of records we have reviewed to date, our results are not projectable to the larger population of FAA's federal employees. As part of our ongoing work, we are continuing to assess the appropriateness of FAA's background searches on its federal employees.

Contractor Background Searches: A Key Area of Exposure

While FAA reports that it has performed background checks on the majority of its federal employees, the same cannot be said for its many thousands of contract employees. FAA's personnel security policy requires that background searches be conducted for contractor employees who have some level of risk associated with their positions. In January 2000, FAA estimated that it had over 28,000 existing contracts and purchase orders under which approximately 38,000 contract employees were engaged. However, according to the agency's database on contract personnel, background searches have been performed for only 16,000 contract employees since 1996, which—even with the unlikely assumption that all of these people are still employed—is less than half of the current contract employee population. As of May 2000, FAA could not estimate how many individuals lacked the required background searches because it had not yet completed assessing the risks associated with contract employees' positions.

¹¹We did not verify FAA's data on its 48,000 employees.

¹²We selected 30 individuals based on the availability of their personnel files. We could not select a statistically valid sample because FAA was reviewing many of its personnel files and they were not available to us for our review.

While acknowledging that FAA did not in the past consistently comply with the requirements of its personnel security policy, FAA security and contracting officials stated that the agency now firmly requires that all new contracts comply with the policy. Further, these officials noted that FAA is working to implement the policy requirements on the backlog of active contracts that did not meet the requirements. However, bringing these prior contracts into compliance with FAA policy is a complicated and time-consuming process.

On June 12, 2000, FAA officials provided updated information on the agency's efforts to bring contracts into compliance with the personnel security policy. These officials stated that, based on a recent review, only 3,000 of the agency's 28,000 existing contracts and purchase orders would require security reviews, and that of these, they have completed about 2,700 reviews. Officials further explained that these reviews resulted in the identification of 14,000 people who require background searches, and that 8,000 of these searches had already been completed. As a result, 6,000 contract employees still require background searches, in addition to any individuals identified during FAA's 300 remaining contract security reviews.

Looked at another way, a key subset of FAA's 28,000 existing contracts are those that support FAA's mission-critical systems. As of June 12, 2000, FAA officials stated that they had been able to identify contracts supporting 425 of the 435 mission-critical systems.¹³ Of the 425 systems, FAA officials determined that 128 had contracts of sufficient sensitivity to warrant position-specific risk assessments. These officials also stated that FAA completed this effort on 72 of the 128 systems, triggering the need for background searches on 622 positions. However, because more than one individual can have the same position description, this may involve performing background searches for more than 622 people.

In order to perform these background searches, contract employees must provide completed background forms which FAA then submits to the Office of Personnel Management or the Federal Bureau of Investigation. These agencies can take from 1 week to 4 months to perform the background searches, depending on the complexity of the review. As of our May 2000 report, FAA's security office had received the completed background forms for only 100 individual contract employees in the

¹³FAA is working to identify the contracts associated with the remaining 10 mission-critical systems.

622 positions that require background searches. Until the required background searches are completed, contract employees who have not received background clearances will continue to have access to FAA's facilities, information, and/or resources.

In seeking to identify some of the root causes of FAA's personnel security problems, we found that three key factors contributed to FAA's noncompliance with its personnel security policy. These were

- insufficient management support,
- insufficient user awareness and training, and
- inadequate policy enforcement.

Management support is critical to any major organizational undertaking, including security. Security experts agree that an effective computer security program begins with top management understanding the risks and committing to support computer security initiatives. However, according to FAA security officials, the agency's contracting office had not previously encouraged headquarters contracting officers to adhere to the policy requirements regarding contract personnel suitability.¹⁴ These security officials noted that management of the contracting office 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 approve the final policy, denoting review and understanding. These officials cited internal resistance to implementing the security measures within the contracting office, however, due to the amount of time and resources required.

According to security officials, contracting personnel may also have been concerned that the security office would impede FAA's ability to meet its commitments because key documents had to be reviewed and approved by security personnel, and currently only one security staff person is performing these reviews. Progress has been evident, however, in gaining management support for personnel security: As a result of our previous review, FAA's contracts organization has directed its personnel to adhere to the policy and has issued a memorandum outlining the priority of tasks to be performed.

¹⁴According to FAA security and contracting officials, there has been greater adherence to the policy at the regions and centers than at headquarters.

As for the second factor, 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 on-line 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 contract employees. To ensure policy adherence, FAA has since revised one key contract provision to outline the tasks to be performed by both contractors and FAA's contracting officers, and security officials have held awareness briefings to provide an overview of the policy requirements. These briefings do not, however, provide detailed guidance on the specific tasks to be performed and, according to FAA, are not considered official training—which should teach individuals the skills that will enable them to perform their jobs.

Finally, senior security officials acknowledged that no formal enforcement of the policy has occurred. 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 that they do not have the staff or resources to conduct reviews or quality assurance activities to ensure that contracting officers have evaluated all contract positions to determine if background searches are needed and whether the correct forms to initiate them have been provided to security.

In response to our December report, the security operations group is planning to conduct policy compliance audits every 6 months. This group expects to develop its plans for conducting these audits this month, with the expectation of conducting its first audit in October. However, according to security officials, the group will be unable to conduct these audits unless additional staff are made available.¹⁵

While FAA's compliance audits, if conducted, would likely provide valuable information on its efforts to implement personnel security policy, an effective quality assurance process could prevent instances of

¹⁵The 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 contract position).

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 even awarded, thus making the compliance audit more meaningful in confirming whether such coordination occurred and whether all security requirements were implemented in accordance with the policy. However, as of May 2000, FAA had no plans to implement a comprehensive quality assurance function.

Our May 2000 follow-up report made three specific recommendations to FAA to (1) establish a user awareness and training program, (2) establish a quality assurance process that will ensure compliance with the personnel security policy, and (3) evaluate resource needs to ensure its personnel security policy is implemented and enforced. On June 12, 2000, FAA officials told us that they will (1) institute personnel security training for all contracting personnel, (2) establish a quality assurance process, to be managed jointly by FAA's contracting and security offices, to ensure that background searches are completed, and (3) provide adequate resources for compliance audits.

Preliminary Results of Ongoing FAA Security Review: Key Vulnerabilities, Concerns Remain

The focus of our ongoing review of FAA's security program is to determine whether (1) the agency has taken adequate steps to prevent unauthorized access to data and (2) it has implemented effective processes for detecting, responding to, and reporting on instances of anomalies and computer misuse. In doing so, we are reviewing FAA's overall information technology security management, personnel security, security awareness and training, physical access, and systems security. While our work has not yet been completed, preliminary information shows:

- As previously noted, FAA has much work to do to complete its efforts to assess and accredit its many ATC facilities.
- FAA still has to assess, certify, and accredit the majority of its operational systems. One key aspect of this effort is identifying the universe of systems that need to be accredited. In early June 2000, FAA reported that it had identified 147 systems to date and acknowledged that more must be done to establish a complete list of systems. As a point of comparison, FAA tracked over 600 systems under its Year 2000 program. FAA's CIO noted that the 147 systems his office identified have the highest priority for accreditation.
- FAA's own system penetration testing and vulnerability assessments demonstrate significant areas of weakness. Because of the sensitivity of

this information, we do not publicly disclose details on these weaknesses. FAA officials report that they are working to address them.

- While, according to FAA, the CIO has budgetary control and oversight responsibility for information security, his office currently has no enforcement or reporting mechanism to ensure that security policies and tasks are implemented.

Conclusions

FAA has a history of computer security weaknesses. Over the past 3 years, we have made over 20 recommendations to FAA to address these weaknesses in the areas of physical security of facilities, systems security, security management, and personnel security. While the agency is making progress in each of these areas, much work remains to be done to assess risks and to adequately protect critical ATC facilities, information, and resources. Until this work is completed, FAA will remain noncompliant with its own security policies and the systems on which the flying public depends will continue to have vulnerabilities that are not being expeditiously identified and corrected. As part of our ongoing review of FAA's computer security program, we will (1) continue evaluating FAA's progress in addressing our recommendations and (2) determine whether additional recommendations are warranted to improve the agency's program.

Agency Comments

Senior FAA officials, in commenting on a draft of this report, generally agreed with our findings. In addition, detailed comments were provided, which we have incorporated as appropriate throughout this report.

Objectives, Scope, and Methodology

Our objectives were to discuss (1) FAA's history of computer security weaknesses and our prior recommendations to address those weaknesses, (2) FAA's progress in implementing our recommendations and its personnel security policy, including our assessment of the adequacy of these actions, and (3) the preliminary results of our ongoing work on FAA's overall computer security program.

To address these objectives, we summarized key findings and recommendations from our reports on FAA's computer security program in general and its personnel security program in particular.¹⁶ We also obtained updated information from key FAA officials—including officials from the Offices of Civil Aviation Security Operations and Information Services—on the status of the agency's efforts to assess and accredit ATC facilities and systems. In addition, we analyzed updated policies on physical security of facilities and information systems security.

Regarding FAA's progress in implementing a CIO management structure, we met with the CIO to discuss his roles and responsibilities and to determine his plans for addressing computer security vulnerabilities. We also reviewed FAA's draft information systems security architecture.

To gain insight into whether FAA conducted appropriate background searches on federal employees, we reviewed the position risk descriptions and background search documentation for 30 individuals. We were unable to select a statistically valid sample because FAA is currently reviewing many of its personnel files and they were not available to us for our review. Instead, we selected a proportionate number of individuals from each of the types of background checks that FAA performs and then sought files on individuals within these categories. If an individual's file was not available, we sought a replacement. Because our review of these files was based on a nonstatistical selection, the results are not projectable to the population of FAA's personnel files.

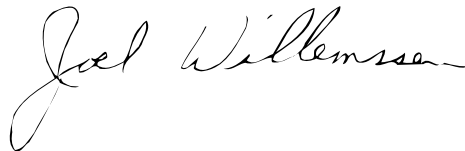
In addition, we obtained oral comments on a draft of this report from FAA officials, including the Administrator's Chief of Staff, the Chief Information Officer, the Deputy Associate Administrator for Research and Acquisitions, and the Deputy Associate Administrator for Civil Aviation Security, and incorporated these comments as appropriate throughout the report.

We performed our work in Washington, D.C., from March through June 2000, in accordance with generally accepted government auditing standards.

¹⁶GAO/AIMD-98-155, May 18, 1998; GAO/AIMD-00-55, December 23, 1999; and GAO/AIMD-00-169, May 31, 2000.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from its date. 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, Senator Fred Thompson, 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 *willemsenj.aimd@gao.gov* and *phillipsc.aimd@gao.gov*, respectively. Key contributors to this report included Nabajyoti Barkakati, Michael Fruitman, David Hayes, and Cynthia Jackson.



Joel C. Willemsen
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)

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

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

<p>Bulk Rate Postage & Fees Paid GAO Permit No. GI00</p>

