

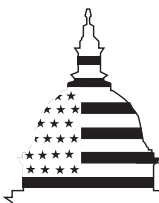
GAO

Report to the Chairman, Committee on
Government Reform, House of
Representatives

November 2002

U.S. POSTAL
SERVICE

More Consistent
Implementation of
Policies and
Procedures for Cash
Security Needed



G A O

Accountability * Integrity * Reliability

Contents

Letter		1
	Results in Brief	1
	Background	3
	Scope and Methodology	4
	Established Remittance Control Procedures Are Not Consistently Followed	5
	Background Checks Not Updated Before Employees Process Remittances	9
	Training May Not Be Adequate	10
	Recent Service Efforts to Improve Remittance Security	11
	Conclusions	12
	Recommendations for Executive Action	12
	Agency Comments and Our Evaluation	13

Appendix I	GAO Contacts and Staff Acknowledgments	15
	GAO Contacts	15
	Acknowledgments	15

Abbreviations

FBI	Federal Bureau of Investigation
OIG	Office of Inspector General, U.S. Postal Service
OPM	Office of Personnel Management
PPO	Postal Police Officer



United States General Accounting Office
Washington, DC 20548

November 15, 2002

The Honorable Dan Burton
Chairman, Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

In fiscal year 2001, the United States Postal Service (the Service) reported that it lost about \$6.3 million in remittances (cash and checks) to robberies, internal theft, and mishandling.¹ One particular loss—a June 2001 theft of over \$3.2 million from a Phoenix, AZ, postal facility by a career Service employee—received considerable media attention. Pursuant to your request, we agreed to review Service policies and procedures for the security of remittances by addressing the following questions:

- Does the Service have reasonable physical controls and security to safeguard its remittances?
- Does the Service have policies for conducting background checks of employees who process remittances?
- Does the Service provide training to its employees who process remittances?

The Service considers the specific policies and procedures for securing and transferring its remittances from postal retail facilities to banks as law enforcement sensitive information. Therefore, these policies and procedures are not described or discussed in detail in this report. Similarly, for the same reason, our specific observations and information that the United States Postal Inspection Service included in its reports we reviewed relating to instances where Service policies and procedures were not followed are described only in general terms in this report.

Results in Brief

The Service has policies and procedures for physically controlling and securing remittances. These include a number of control activities that, if properly implemented, would be effective in helping to safeguard

¹According to the Service, a substantial portion of these initial losses was eventually recovered.

vulnerable assets, such as cash. The control activities include, among others, requirements for continuous individual accountability of remittances. However, Service management does not always provide appropriate oversight of these activities and Service employees do not always follow the Service's policies, procedures, and activities for controlling and physically securing remittances. For example, the Postal Inspection Service found that the June 2001 employee theft of remittances in Phoenix occurred and was not promptly identified and reported because established control procedures were not followed. This occurred even though the previous failure of employees to follow established policies and procedures had been brought to the attention of the facility's management by the Postal Inspection Service prior to the incident. Further, at selected postal facilities, we observed that Service policies and procedures for controlling and securing remittances were not always followed, and accountability for remittances was not always maintained. Over the last few years, the Postal Inspection Service has made similar observations at numerous postal facilities throughout the country.

The Service requires a background check as part of a suitability test for all prospective new employees. The background check includes a review of any criminal or military records, a fingerprint check by the Federal Bureau of Investigation (FBI), and a drug screening. Although only career employees are allowed to process remittances, there is no requirement to update the background checks of these employees regardless of how much time has elapsed since the initial check was performed.

The Service's training for postal employees who process remittances includes both on-the-job training and the use of self-paced training and development manuals related to the control and security of remittances. However, the Service's training manuals have not been appropriately updated, and in August 2001, the Service's Chief Postal Inspector cited the lack of training as a possible condition leading to the Postal Service's remittance losses.

The Service has recently initiated efforts to strengthen security for remittances. However, until these policies and procedures are effectively implemented, the Service's remittances remain at risk. Accordingly, we are making recommendations to the Postmaster General concerning the need to (1) more rigorously reinforce to managers and employees the importance of and need to follow Service policies and procedures for controlling and physically securing remittances and hold managers and employees accountable for following the policies and procedures, (2) reassess its policies for updating background checks on employees

selected to process remittances, and (3) update its training manuals and determine whether additional training on the control and security of remittances is needed.

The Service agreed with our recommendations and stated that it is already well on the way to implementing procedures that will fully address them. It said it had some legal and cost concerns relating to updating background checks of career employees and said that it would need to consider these issues as it studies this matter. We agree that the issues the Service identified are valid concerns that should be considered.

Background

Traditionally, the Service's local post offices deposited their daily remittances of coin, cash, and checks in accounts with local banks. Before 1997, according to the Service's Assistant Treasurer for Banking, the thousands of individual retail postal units deposited their daily remittances in some 9,300 bank accounts with 5,500 banks across the country. In 1997, to help reduce banking costs and improve funds availability, the Postal Service implemented consolidated banking—a Service-wide process whereby the daily remittances from the Service's retail postal facilities are consolidated and transferred by armed bank couriers to a relatively few commercial banks for deposit.

The Postal Inspection Service, one of the nation's oldest law enforcement agencies, is the Postal Service's law enforcement arm. With a force of about 1,400 uniformed Postal Police Officers (PPOs), over 1,900 postal inspectors, and five forensic crime laboratories, the Postal Inspection Service is responsible for ensuring the safety and security of postal employees, facilities, and assets. PPOs provide security at postal facilities where the Postal Inspection Service has determined that risk and vulnerability demonstrate a need for this level of security. Postal inspectors help enforce and investigate infractions of over 200 federal laws applicable to crimes that adversely affect or involve fraudulent use of the U.S. mail. Matters investigated include criminal incidents, such as mail theft, robberies, burglaries, and embezzlement; and the criminal use of the mail for money laundering, fraud, child exploitation, and the movement of illegal drugs.

The Postal Inspection Service periodically performs reviews of remittance-processing procedures at selected individual postal facilities or at a cross section of facilities within a postal district. These reviews are security reviews focused primarily on compliance with the applicable policies and procedures to help prevent instances of mishandling and losses. Results of

these reviews are reported to the appropriate postal district manager, and districtwide review results are reported to the appropriate postal area manager. According to the Postal Inspection Service, although its reports apprise postal officials of its findings and recommend corrective action(s), district and area managers are not required to implement these recommendations.

Scope and Methodology

To meet our objectives, we obtained and reviewed Service policies and procedures for controlling and securing remittances and for requiring background checks and training for employees who work with remittances. We used the *Standards for Internal Control in the Federal Government*, as well as the *Internal Control Management and Evaluation Tool*,² to help assess the Service's policies and procedures. We also obtained and reviewed applicable training manuals, orders, directives, and handbooks. Also, for each of our objectives, we discussed the applicable policies, procedures, and practices with appropriate Service officials, including headquarters officials in Postal Operations, Corporate Accounting, Corporate Treasury, Human Resources, Network Operations Management, and the Postal Inspection Service. Further, we had similar discussions with postal facility managers, supervisors, employees who process remittances, and Postal Inspection Service inspectors in the various field locations we visited.

We did not review all aspects of the Service's internal controls or its systems for accounting for remittances. For example, we did not evaluate the Service's assessment of the risks that it faces from both internal and external sources or perform a comprehensive assessment of the Service's security for its post offices or processing centers.

To help determine how well the Service's policies, procedures, and control activities are working, we obtained and reviewed Postal Inspection

²GAO issues standards for internal control in the federal government as required by the Federal Managers' Financial Integrity Act of 1982. See 31 U.S.C. 3512(c). GAO first issued the standards in 1983. GAO revised the standards and reissued them as *Standards for Internal Control in the Federal Government* ([GAO/AIMD-00-21.3.1](#), November 1999). These standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance challenges and areas at greatest risk for fraud, waste, abuse, and mismanagement. GAO issued its *Internal Control Management and Evaluation Tool* ([GAO-01-1008G](#), August 2001) to assist agencies in maintaining or implementing effective internal control and, when needed, to help determine what, where, and how improvements can be implemented.

Service reports of investigations and other Postal Inspection Service reports dating back to fiscal year 1999. We judgmentally selected reports for review on the basis of our discussions with Postal Inspection Service officials about the remittance loss history of the various postal districts and to provide geographic dispersion. We also visited Service facilities at six locations—three in Arizona; one in Texas; one in Maryland; and one in Washington, D.C.—to observe Service policies and procedures in practice.³ The facilities in Arizona were chosen because they were at or near the location where a postal employee stole a substantial amount of remittances in June 2001. The other facilities were chosen to provide geographic dispersion for our observations. We performed our work between July 2001 and November 2002 in accordance with generally accepted government auditing standards. We obtained comments on a draft of this report from the Postal Service.

Established Remittance Control Procedures Are Not Consistently Followed

The Service's policies and procedures include a number of remittance control activities that, if properly implemented, would help prevent remittance losses. However, Service employees are not always following established policies and procedures, and Postal Service management does not appear to have taken effective actions to address this problem.

Service Policies and Procedures for Controlling and Securing Remittances

The GAO-issued *Standards for Internal Control in the Federal Government* defines the minimum level of acceptable internal controls in government. Although the standards provide a general framework, the management of each agency is responsible for developing the detailed policies, procedures, and practices to fit its operations. For example, one of the standards for internal control states that internal control activities—the policies, procedures, techniques, and mechanisms that enforce management directives—should be effective and efficient in accomplishing the agency's control objectives. A key control activity includes establishing physical control to secure and safeguard vulnerable assets, including limiting access to such assets and ensuring that they are periodically counted and compared with control records. Thus, effective control activities at the Service would be expected to include such

³The specific locations we visited are not provided because of security concerns expressed by the Service.

reasonable activities as are necessary to physically secure, safeguard, and account for its remittances.

Service policies and procedures incorporate a number of activities for controlling and securing remittances that we believe, if effectively implemented, would help prevent loss of these assets. The Service's control activities or procedures include, among others, the requirement that there is to be continuous individual accountability of remittances, including hand-to-hand exchanges at all transfers. In addition, employees are to document the progress of remittances moving through the system to banks and notify the Postal Inspection Service immediately when discrepancies or losses are noted. Finally, postal district accounting personnel are to reconcile the electronic record of each post office's daily sales with the bank information showing remittance deposits received from each post office.

Service Policies and Procedures for Controlling and Securing Remittances Are Not Always Followed

Our observations and the findings of the Postal Inspection Service show that many of these policies, procedures, and activities for controlling and securing remittances are not always followed or practiced by employees at numerous postal facilities across the country. In addition, even though the Postal Inspection Service has brought this issue to the attention of Service management over a period of several years, it appears that the Service has not taken effective actions to address the problem.

In July 2002, we visited three locations in the Service's Arizona district. At each location, Postal Inspection Service officials accompanied us. The officials agreed with our observations that at each of these locations, Service employees carried out a number of practices that are inconsistent with Service policies and procedures for controlling and securing remittances.

Each year, the Postal Inspection Service reviews control and security procedures at selected postal districts and facilities throughout the country to identify opportunities for security improvements and to measure and improve compliance with the Service's policies and procedures. A primary goal of these reviews is to help protect remittances from mishandling, loss, and theft. The findings from these reviews are reported to Service management at the respective districts. We reviewed a number of Postal Inspection Service reports on the results of these reviews, which were completed in fiscal years 1999, 2000, 2001, and 2002.

A May 1999 Postal Inspection Service report on performance audits performed at various postal facilities in the Service's Northeast Area found that a number of policies and procedures for processing and securing remittances were not being followed. Specifically, the Postal Inspection Service found that individual accountability for remittances was not being maintained as required by Service policy and procedures. Also, in a February 1999 performance audit report, the Postal Inspection Service found that at a California postal district, postal personnel were handling remittances without signing for and accepting accountability for them.

Postal Inspection Service reports of districtwide reviews conducted during May through July 2000 in six districts in the Service's Western Area disclosed that local post offices in each of these districts often failed to take the appropriate actions required for ensuring that remittances could always be accounted for. For example, remittances were sometimes left unattended and unsecured. Also, certain restricted access areas were not locked, and unauthorized personnel were permitted entry.

In August 2001, the Postal Inspection Service reviewed remittance-handling practices at 25 post offices in a district in the Service's Southeast Area. Its report on these reviews stated that losses due to internal causes (employee theft and mishandling) in the district during fiscal year 2001 to date totaled about \$150,000, an increase of 375 percent over the previous year's total. The report said that these losses were attributable to practices in the district that failed to establish individual accountability for remittances and to properly secure them.

During the period from early September through late December of 2001, the Postal Inspection Service reported visiting over 2,000 postal facilities nationwide and observed 252 lapses of remittance security. Its inspectors also found lapses in individual accountability of remittances and instances of unauthorized access into postal facilities through unsecured doors, including doors that were propped open and left unattended.

Service Management Has Not Effectively Addressed Weaknesses in Remittance Controls

An important internal control standard established in the *Standards for Internal Control in the Federal Government* pertains to the control environment. It states that management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management. However, it appears that even though significant weaknesses in the Service's controls over its remittances have been brought to the attention of Service management by the Postal Inspection Service

numerous times over the last few years, Postal Service management has not taken effective action to address these weaknesses—leaving its remittances vulnerable to theft or loss. For example, during our visit to the Phoenix mail processing facility, a manager acknowledged that there had been deficiencies and that compliance with procedures had probably been lax for several years.

In August 2001, after the theft in Phoenix, the Chief Postal Inspector, who is the head of the Postal Inspection Service, wrote to the Postal Service's Chief Operating Officer about the Postal Inspection Service's concern over continuing problems with remittances. The Chief Postal Inspector pointed out that losses had begun to increase in late fiscal year 1999 and were continuing to increase. He stated that since 1997, the Postal Inspection Service has frequently brought proper procedures and policy to the attention of postal management through its investigations and other reviews, and the intention of management to adopt the recommendations of the Postal Inspection Service appears genuine. He stated, however, that the implementation of proper procedures and ongoing security of remittances continue to erode and that causes could include the following:

- Postal Service management has been unable or unwilling to comply with procedures that will properly secure remittances. Some postal district managers have refused to comply with certain procedures to protect remittances. (In our discussions with the Postal Inspection Service, we were told that some postal district managers balked at implementing certain remittance handling procedures because they believed that the procedures would result in additional costs that would have to be absorbed by each Service district.)
- Other postal areas have not implemented Postal Inspection Service recommendations to improve the security of remittances. For example, in 2000 a report was issued to the manager of the Phoenix facility that detailed security issues that, had they been corrected, the Postal Inspection Service believes could have deterred or prevented the June 2001 loss of over \$3 million.
- Historically, employees have not been held accountable for mishandling and subsequently losing remittances. For example, in the Postal Inspection Service's Mid-Atlantic Division, an employee left remittances in a 24-hour lobby after the post office had closed. The remittances were stolen, but no disciplinary action was initiated against the employee.
- Employees may not be trained properly in processing remittances. For example, in a Washington, D.C., postal facility, a training course for clerks was discontinued in 1986. Although a reliable Service-wide sample has not been taken, the Postal Inspection Service sees this lack of training as a

common inadequacy throughout the Postal Service. Certain reference material has not been updated since 1982.

- During a postal reorganization, a key supervisor position was abolished, leaving employees without direct supervision.
- The security of remittances or prevention of losses was never an established goal for postal management, unlike overnight and 2- to 3-day mail delivery scores. Therefore, compliance is not a priority. He said that a measurable security goal that includes the security of remittances should be considered.

He closed by stating that the Postal Inspection Service is committed to assisting the Postal Service through aggressive remittance loss and other investigations and initiatives. He said that the Postal Inspection Service recognizes the risk this matter poses to Service employees and to the Service, and he wants to ensure this risk is minimized through proper remittance handling procedures.

In December 2001, the Service's Chief Operating Officer issued a memorandum to the Service's Area Vice Presidents; District Managers; Processing and Distribution Center Plant Managers; and the Manager, Capital Metro Operations, stating that the Postal Inspection Service's recent oversight work had repeatedly found that remittances were not always being controlled and protected as required. He said that this was not an issue of incidental oversight, but rather a condition in which "basic work processes were either not in place, or were being routinely compromised." He concluded by pointing out that postmasters and postal employees are personally responsible for depredation or loss of remittances due to negligence or disregard of instructions and asking the addressees to ensure that appropriate controls are in place throughout their respective operations.

Background Checks Not Updated Before Employees Process Remittances

The Service performs background checks for all prospective employees as part of a suitability test to identify applicants who possess the necessary skills, abilities, and qualifications to perform specific jobs in the Postal Service. The Service does not, however, require updated background checks for employees who are selected to process remittances.

The employee suitability test is a two-part review. The first part includes an examination, which tests memorization and provides a behavioral rating; veterans' preference check; criminal records check; military records review; drug screen; driving record review; and interview.

The second part of the review takes place after the job offer and includes a medical assessment, fingerprint and Office of Personnel Management (OPM) Special Agency Check, and an evaluation that places the employee into a 90-day probationary period during which he/she receives orientation and whatever training is needed.

Our review of summary documentation on remittance losses during 2001 and discussion with Postal Inspection Service officials did not indicate that updated background checks of employees selected to process remittances would have prevented any losses that have occurred. However, because employees' background checks could have been performed years earlier, when they were initially hired, additional or updated background checks for employees before they are allowed to process remittances might reduce the risk of theft to an asset as vulnerable as cash.

In our discussions of this issue with Postal Service officials, they pointed out that the Service had legal concerns about its authority to unilaterally impose a requirement for updated employee background checks on bargaining unit employees and that such a requirement would be subject to collective bargaining with various postal employee unions. They also said that certain employment law issues would have to be considered, such as the permissibility of drug testing and the use of arrest and conviction information. We agree that these types of issues would need to be considered in any reassessment the Service would do in connection with requiring updated background checks for employees processing remittances. However, we believe that such a reassessment is warranted given the higher risk levels associated with responsibilities that involve processing remittances. Furthermore, if the Service determines that requiring employees to undergo periodic background check updates is subject to the collective bargaining process, the issue could be raised by the Service during negotiation of the next collective bargaining agreement.

Training May Not Be Adequate

The Service provides training to its employees who process remittances. However, the training materials for clerks and supervisors are outdated. In addition, the Postal Inspection Service has indicated that a lack of training could be contributing to remittance losses.

Postal career employees who apply for the job are selected to process remittances on the basis of their seniority. There are no special skills or abilities required for selection other than those required of a mail distribution clerk. Those who are selected are to be trained in the specific

roles they will be performing with remittances. Unit supervisors are responsible for ensuring that the employees in their units are trained. The training includes on-the-job training as well as a requirement that the employees complete self-paced training manuals pertaining to their specific responsibilities.

Service training manuals have not been updated to address the processing of remittances. For example, one of the Service's principal policy handbooks for operations that include processing remittances was updated in 1997; however, the training manual that addresses certain remittance processing procedures has not been similarly updated.

Although we cannot say that the failure of employees to follow Service policies and procedures for securing remittances that we observed was the result of inadequate or incomplete training, the Chief Postal Inspector stated in his letter to the Postal Service's Chief Operating Officer mentioned earlier that a lack of employee training in proper handling of remittances was among the conditions contributing to remittance losses.

Recent Service Efforts to Improve Remittance Security

Within the last year, the Service established a team to develop a standard operating plan that provides detailed policies and procedures for processing remittances. According to the Service, the draft plan was recently completed, and the plan should be approved by, and implementation should begin in, November 2002. The plan is to become the national standard for processing remittances through the Service. The Service's new policies and procedures do not address the issue of background checks for employees.

According to the Service, Area managers will have responsibility for ensuring that field management train and hold accountable employees who process remittances, and all deviations from the plan are to be reported and approved by Area management. All approved deviations are to be submitted to Service headquarters. In addition, according to the Service, it is in the process of redesigning training for employees who process remittances. It said that the new training manuals and handbooks would incorporate the new policies and procedures for processing remittances. Finally, according to the Service, the Service's Chief Operating Officer will disseminate the new plan through formal channels of the organization to the Area Vice Presidents, who will be instructed in their responsibility for providing the proper training in policies and procedures to employees who process remittances. In addition, the message to the Area Vice Presidents is to be reinforced by having

employees watch a recently developed video that pertains to their areas of responsibility, and all training is to be documented by management.

The establishment of these new policies and procedures for processing remittances is an important step in the right direction. Also, it is particularly encouraging that the Service plans to emphasize management accountability for implementing the new policies and procedures. However, until these new policies and procedures are finalized and address the remittance control problems we have identified, employees are trained in how to follow them, and they are effectively implemented, the Service's remittances continue to be at risk.

Conclusions

The Service has policies and procedures that, if properly implemented, would help to control and physically secure its remittances. However, the Service's policies, procedures, and control activities are not consistently followed by employees and it appears that Service management has not taken effective actions to address the problem. The Chief Postal Inspector has cited a lack of (1) training, (2) adequate supervision, (3) postal management follow-through, and (4) accountability as contributing factors. The Service has not updated its relevant training manuals and does not update background checks for employees selected to process remittances—thus possibly subjecting the Service to increased vulnerability to the theft of its cash. Until Service management actively addresses the problems of controlling and securing its cash remittances, widely identified throughout the Service by the Postal Inspection Service and by us at locations we visited, its remittances will continue to be vulnerable to mishandling, loss, and theft.

Recommendations for Executive Action

We recommend that the Postmaster General

- more rigorously reinforce to managers and employees at facilities throughout the Postal Service the importance of following Service policies and procedures for controlling and securing remittances;
- hold Service managers and employees accountable for following Service policies and procedures for controlling and securing remittances and correcting the control problems identified by the Postal Inspection Service;
- include adherence to policies and procedures for securing remittances and minimizing remittance losses in its organizational goals and performance management and pay systems and define and enforce supervisory responsibilities to achieve these reinforcement and accountability objectives;

-
- reassess current Service policy of not updating background checks of career employees prior to their being selected to process remittances; and
 - update applicable training manuals that predate the Service's adoption of its consolidated banking policy and determine whether additional training for managers and employees on the Service's policies and procedures for physically controlling and securing remittances is needed and, if so, see that such training is developed and provided.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Postal Service's Chief Operating Officer. In his comments he stated that the Service appreciated the thoroughness of our review and the disclosure of some shortfalls in the physical security of postal remittances. He said that our findings are extremely serious, and the Service is committed to improving the current process. He said that to that end, management teams from several departments have already developed changes in procedures to address our findings, including improvements to the procedures to secure and account for remittances. He said that the Service is well on the way to implementing procedures that will fully address the recommendations contained in our report. For example, he said that the Service is establishing an internal control unit in each district office to assess risk and compliance with remittance handling as well as other financial and operational policies and procedures. He further said that the Area Vice Presidents will be held responsible for ensuring that field managers provide training to all employees who process remittances.

Specifically regarding our recommendation that the Service reassess its current policy of not updating background checks of career employees prior to their being assigned to process remittances, he said the Service is already in continuing discussion with its General Counsel on the matter. He said that the Service has legal concerns about its authority to unilaterally require updated background checks on bargaining unit employees because such a requirement could be viewed as a "term or condition of employment" subject to collective bargaining. Also, he said that it would be very costly to periodically recheck the thousands of employees who process remittances. He stated that with implementation of the new standardized remittance-processing procedures, the Service believes that it will have in place compensating controls that will be more cost effective than periodic background checks.

We agree that all of these issues are important issues for the Service to consider as it reassesses its background check policy. If the Service determines that requiring periodic updated employee background checks

is subject to the collective bargaining process, that issue could be addressed when the collective bargaining agreement comes up for renewal. As to the issue of the cost involved in periodically rechecking the backgrounds of thousands of employees, we believe that the Service's reassessment could include considering updating the background checks only for employees who process high-value remittances. As for the issue of the Service having in place compensating controls that will be more cost effective than periodic background checks, we plan to do future follow-up work to determine the effectiveness of the new standardized remittance-processing procedures once they are in place. (Written comments received from the Chief Operating Officer are not included in this report because they contain information the Service considers law enforcement sensitive.) Other Service officials suggested technical changes, including the exclusion of information that the Service considers law enforcement sensitive, to our draft report. We have made these changes where appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Ranking Minority Member of your Committee; the Chairman and Ranking Minority Member of the Senate Subcommittee on International Security, Proliferation, and Federal Services; the Chairman and Ranking Minority Member of the Senate Subcommittee on Treasury and General Government; the Chairman and Ranking Minority Member of the House Subcommittee on Treasury, Postal Service and General Government; and the Postmaster General. We also will make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

Major contributors to this report are acknowledged in appendix I. If you have any questions about this report, please contact me on (202) 512-2834 or at ungarb@gao.gov.

Sincerely yours,



Director, Physical Infrastructure Issues

Appendix I: GAO Contacts and Staff Acknowledgments

GAO Contacts

Bernard L. Ungar (202) 512-2834
Sherrill H. Johnson (214) 777-5600

Acknowledgments

In addition to those individuals named above, Tyrone Griffis, Michael J. Fischetti, Gladys Toro, Heather Dunahoo, Walter Vance, and Donna Leiss made key contributions to this report.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
 TDD: (202) 512-2537
 Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548