GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-284836

April 19, 2000

Mr. Dennis H. Smith
Director, VA Maryland Health Care System
Department of Veterans Affairs
10 North Greene Street
Baltimore, Maryland 21201

Subject: VA Systems Security: Information System Controls at the VA Maryland Health Care System

Dear Mr. Smith:

As part of our review of computer security at the Department of Veterans Affairs (VA), we assessed the effectiveness of information system general controls[1] at the VA Maryland Health Care System (VAMHCS). Our review of VA computer security was performed in connection with the department's required annual financial statement audit for fiscal year 1999.

The purpose of this report is to advise you of the weaknesses we identified at VAMHCS and the status of corrective actions. In discussions with your staff, we offered specific recommendations for mitigating these weaknesses. The results of our evaluation were shared with VA's Office of Inspector General for use in its audit of VA's consolidated financial statements for fiscal year 1999.

In evaluating information system general controls, we identified and reviewed VAMHCS's information system control policies and procedures. We also tested and observed the operation of information system general controls over VAMHCS's financial systems to determine whether they were in place, adequately designed, and operating effectively. These controls, however, also affect the security and reliability of nonfinancial information, such as the medical support systems maintained at this center. Our evaluation of information system general controls was based on our

[1]General controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They include security management, operating procedures, software security features, and physical protection designed to ensure that access to data and programs is appropriately restricted, only authorized changes are made to computer programs, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations.

Computer Security Weaknesses at VAMHCS That Remain Open

This enclosure summarizes the information system control weaknesses we identified during our work at VAMHCS that remained open at the completion of our 1999 site visit. For each weakness, the enclosure provides recommended actions and management's response. These weaknesses are grouped based on the type of controls identified in our FISCAM.

Network Access Controls

A basic management objective for any organization is to protect its data from unauthorized access and to prevent improper modification, disclosure, or deletion of financial and sensitive information. To reduce the risk of unauthorized access, organizations need to sufficiently protect access to their networks. Because of VA's highly interconnected environment, the failure to control access to any one system connected to the network exposes all systems and applications attached to the network even if each of the remaining VAMHCS systems have ample security. As a result, financial information and sensitive veteran medical information could be at increased risk of unauthorized modification or disclosure occurring without detection. At VAMHCS we identified, for example, the following security weaknesses.

1. **Weakness:** System settings on one of the network servers could permit individuals to establish connection without entering a valid user account name and password combination (authentication). Through this connection, an unauthorized individual could gain access to information contained in the system which would allow the individual to understand the network environment, including user account names, password properties, and account policy details. The unauthorized user could then, with password cracking software, target users who have access to financial and sensitive information.

   Recommendation: Change system settings to prohibit individuals from gaining unauthorized access to system information.

   Management Response: VAMHCS officials told us that by November 30, 2000, they would change the system settings to correct this problem.

2. **Weakness:** Excessive user rights were granted on three network systems, which could compromise the integrity of the operating system. On these systems, all users, regardless of their job responsibilities and access needs, were granted access to sensitive system directories that would allow users to create files and subdirectories, and to delete files, subdirectories or the current directory. Before completion of our fieldwork, VAMHCS restricted user access on one of these three network systems.

Recommendation: Restrict such broad access to sensitive system directories and files to those individuals who need such access to perform their duties.

Management Response: VAMHCS officials told us that they had restricted access to the sensitive system directories on all system servers and planned to review all systems to ensure compliance by March 31, 2000.

3. **Weakness:** The network system was not set to display a warning banner on the initial log-on screen to any system. As a result, VAMHCS may be unable to prosecute or take disciplinary action against individuals who misuse its system.

   Recommendation: Create a warning banner to be displayed on the initial log-on screen for all systems.

   Management Response: VAMHCS officials told us that by September 30, 2000, they would develop specific warning banners for each system that specify fully the complete legal language required to properly notify employees of actions that can be taken in case of a security breach.

Network ID and Password Management Controls

It is important to actively manage user IDs and passwords to ensure that users can be identified and authenticated. To accomplish this objective, organizations should establish controls to maintain individual accountability and protect the confidentiality of passwords. These controls should include requirements to ensure that IDs uniquely identify users; passwords contain specified numbers and types of characters and not common words; and default IDs and passwords are changed.

We found several areas where VAMHCS was not adequately controlling IDs and passwords, including the following.

4. **Weakness:** Over 80 percent of the network IDs, including the network administrator ID, were vulnerable to abuse because passwords were common words or characters that could be easily guessed. In addition, 253 accounts had passwords of fewer than six characters. Also, 94 accounts did not require passwords. VAMHCS did not have its network system parameters set to require minimum password lengths nor was it reviewing passwords to ensure compliance with VA password guidelines. Prior to completion of our fieldwork, VAMHCS changed its system settings to require a minimum password length.

   Recommendation: Increase employee awareness of VA's password guidelines and periodically review passwords to ensure compliance with VA password guidelines.

   Management Response: VAMHCS officials told us that the minimum password length has now been set to six characters and must be alphanumeric. This action

was completed in January 2000. Beginning in April 2000, password guidelines would be emphasized during security awareness training during new employee orientation, service level training, and annual awareness training.

5. **Weakness:** On one network system, at least 880 passwords were set to never expire. In addition, 19 system user accounts with special access privileges had passwords that were set to never expire or had an excessive password life of 180 days or more. Consequently, there is greater risk for these passwords to be compromised, potentially leading to unauthorized use of passwords and user accounts to gain access to system resources.

   Recommendation: Change password settings to require passwords to expire periodically.

   Management Response: VAMHCS officials told us that by April 30, 2000, password settings would be changed to require passwords to expire at least every 90 days.

6. **Weakness:** Network system settings allowed unlimited log-on attempts. The setting that allows an account to be locked out after a specified number of unsuccessful log-on attempts was not enabled. Without this feature enabled, an unauthorized user could make an unlimited number of attempts to gain access to the system.

   Recommendation: Update system settings to lock out accounts after a specific number of unsuccessful logon attempts.

   Management Response: In March 2000, VAMHCS officials told us that they changed the system settings in January 2000 to lock out accounts after five unsuccessful log-on attempts.

7. **Weakness:** Generic user IDs were being shared by an indeterminable number of users. VAMHCS was not periodically reviewing the use of shared IDs. Use of these shared IDs undermines the effectiveness of monitoring because individual accountability is lost.

   Recommendation: Remove generic IDs from the system and periodically review user accounts for use of shared IDs.

   Management Response: VAMHCS officials told us that generic user IDs would be reviewed and their access rights restricted by August 31, 2000. In addition, they told us that a process would be established to periodically review user accounts for use of shared IDs.

8. **Weakness:** One network system included files that stored passwords in clear text. In addition, the network password file was accessible to all users. As a

result, VAMHCS was at increased risk that unauthorized users could gain access to financial and other sensitive resources.

Recommendation: Delete the system files that allow passwords to be viewed in clear text and limit the number of users with access to the password file.

Management Response: VAMHCS officials told us that they would delete the files that allow passwords to be stored in clear text and would limit the users with access to the password files by April 30, 2000.

9. **Weakness:** Forty-five active network IDs belonging to terminated or transferred employees were not disabled. There were 11 instances in which these accounts were used after the employee's termination date by either terminated employees or active staff. If IDs are not promptly disabled when employees are terminated, current or terminated employees could use them to sabotage or otherwise disrupt VAMHCS operations.

   Recommendation: Disable IDs of terminated or transferred employees and periodically review all IDs to identify terminated or transferred employees.

   Management Response: VAMHCS officials told us that by May 31, 2000, they would remove the IDs of terminated or transferred users from their systems and develop a process to periodically review and remove IDs of terminated and transferred employees.

10. **Weakness:** About 400 network IDs and over 1,500 system IDs had not been used for over 90 days. This situation poses the unnecessary risk that unneeded IDs will be used to gain unauthorized access to VAMHCS computer resources.

    Recommendation: Periodically review user accounts to identify accounts unused for long periods and disable unneeded IDs.

    Management Response: VAMHCS officials told us that they were identifying users who had not signed onto the system within 90 days and were collaborating with other VA components to ensure that this issue was adequately addressed. In addition, VAMHCS officials told us that they would develop guidelines to regularly review user accounts and disable those that had not been used for a long time. Actions to address these issues would be completed by July 31, 2000.

Remote Access Controls

Organizations must control access to computer resources from remote locations to protect sensitive information from improper modification, disclosure, or destruction by hackers. Because allowing dial-in connections from remote locations significantly increases the risk of unauthorized access, such access should be limited, justified, approved, and periodically reviewed. Organizations should also control all modems and telephone lines centrally, establish controls to verify that dial-in connections are authorized, and test for unauthorized modems.

11. **Weakness:** VAMHCS had not established remote access control policies or procedures to require that dial-in connections to internal systems and the network be authorized and to prohibit employees from connecting unauthorized modems to network workstations. VAMHCS had not established formal procedures for periodically testing dial-in connections or validating users with remote access privileges to ensure that those connections and privileges were authorized and appropriate.

    Recommendation: Establish and implement policies and procedures to authorize and review dial-in connections.

    Management Response: VAMHCS officials told us that a policy would be developed and implemented by August 31, 2000, to address dial-in access use for the VA network.

Network Security Monitoring

To reduce the risks created by network access control problems, organizations need to establish proactive network monitoring programs. These programs require organizations to promptly identify and investigate unusual or suspicious network activity indicative of malicious, unauthorized, or improper activity, such as repeated failed attempts to identify systems and services on the network, connections to the network from unauthorized locations, and efforts to overload the network to disrupt operations. Network monitoring programs should also include provisions for logging and regularly reviewing network access activities. Without such controls, organizations have little assurance that unauthorized access to systems on its network would be detected in time to prevent or minimize damage.

12. **Weakness:** VAMHCS did not have a proactive network monitoring program to identify unusual or suspicious activities. Although VAMHCS was logging certain system activities and periodically reviewing some of the logs, VAMHCS did not have procedures for logging system events and maintaining audit trails of access activities that would warrant further review. As a result, while VAMHCS was logging some of its network activities, these logs were not reviewed regularly and for those that had been reviewed, VAMHCS had not retained documentation showing the results of its review. Such reviews should be done routinely to track and analyze activities that could be indicative of unusual or suspicious activities.

Recommendation: Establish a proactive network monitoring program to identify unusual or suspicious activities.

Management Response: VAMHCS officials told us that they would establish a proactive network monitoring program that would include logging system events and developing criteria to identify unusual or suspicious activities. VAMHCS expects to complete this action by August 31, 2000.

System User Access Controls

Organizations can reduce the risk that unauthorized changes or disclosures occur by (1) granting employees authority to read or modify only those programs and data that are necessary to perform their duties, (2) periodically reviewing their authority and modifying it to reflect changes in job responsibilities, and (3) monitoring the use of the authority granted to ensure that it is being used only for the purposes authorized. Without effective access controls, the reliability of computer system data cannot be maintained, sensitive information data can be accessed and changed, and information can be inappropriately disclosed.

13. **Weakness:** VAMHCS allowed 12 Information Resource Management (IRM) staff to have special access privileges that allowed each of them to have access to the system account. With this system account, each of these users could obtain access to all financial and sensitive veteran information. While it is appropriate for selected computer staff to have broad access authority, we found that VAMHCS did not have procedures to ensure that these IDs were adequately controlled. Specifically, VAMHCS had not established the following control procedures:
    - Provide specific criteria for granting broad system access authority.
    - Require and maintain authorization documentation for all programmers as a permanent record of valid and approved access authority, including the purpose and time frames needed.
    - Periodically review each ID and recertify the continued need for this broad access.
    - Routinely monitor user access activities to ensure that these powerful IDs are being used only for their intended purposes.

    Recommendation: Establish and implement procedures to ensure that IDs with special access privileges are limited to those necessary and that usage is adequately controlled.

    Management Response: VAMHCS officials told us that by April 30, 2000, they would establish and implement a system to periodically review special access IDs to ensure that (1)such access is granted only to those staff that need it to perform their job assignment and (2) these powerful IDs are used only for their intended purpose.

14. **Weakness:** VAMHCS did not adhere to formally documented procedures for granting access to VAMHCS users. Specifically, VAMHCS did not ensure that system user access authorizations were maintained for all VAMHCS system users. We could not find access authorizations for 24 of 26 users tested. In addition, VAMHCS was not performing periodic reviews or recertifications of user access to ensure that individual business needs for system access continued to exist.

    Recommendation: Establish and implement procedures to periodically review system user access to ensure that proper authorizations are maintained for all users and that system access is still needed.

    Management Response: VAMHCS officials told us that by April 30, 2000, they would update policies to require maintenance of user access authorizations and establish procedures for periodic review and recertification of all system users to verify that system access is still needed.

Segregation of Duties

One fundamental technique for safeguarding programs and data is the appropriate segregation of duties and responsibilities of computer and financial personnel to reduce the risk of errors or fraud or that any such attempts will go undetected. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed.

15. **Weakness:** Eleven staff involved with procurement were granted system access which allowed them to initiate a purchase order, approve the same order, and complete the receiving report for the original order. Such access is contrary to the internal control standard on segregation of duties which prescribes that key duties and responsibilities, such as those described above, need to be divided among different people to reduce the risk of error or fraud. VAMHCS management indicated that there may be situations where this type of access may be needed. Such a practice should be strictly limited to medical and operational emergencies and be subsequently reviewed. This authority should be limited to only those individuals needing such access and should be approved by VA management as prescribed by VA policy. Further, there is no policy that specifically requires management to monitor any activity where such combined access is used. We found no evidence of VA management approval for this access, nor did we find mitigating controls to alert management of purchases made in this manner. The continued practice of allowing procurement staff to have total control of purchases without mitigating controls increases the risk that inappropriate or fraudulent transactions could be processed, possibly without detection.

    Recommendation: Establish and implement a policy to (1) limit system access that allows an individual to control all elements of a transaction, including requesting, approving, and recording the receipt of items and (2) ensure that when this type of system access is granted, it is approved by VA management. Develop a program to notify management when purchases are made in this manner.

Management Response: VAMHCS officials told us that they would develop and implement a policy to limit the granting of system access that would allow an individual to request, approve, and receive items. The policy will include provisions for higher level review in those limited cases where such access may be required. VAMHCS would conduct periodic reviews of individuals who need this access and establish a system to monitor the purchasing activity of those individuals who have this access. These actions are scheduled to be completed by April 30, 2000.

Application Development and Change Control

Application development and change controls should be designed and implemented to prevent use of unauthorized programs or modifications to an existing program from being implemented. This is accomplished by instituting policies, procedures, and techniques that ensure that all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs are carefully controlled. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced.

16. **Weakness:** There were no procedures for periodically reviewing Veterans Health Information Systems and Technology Architecture (VISTA) programs to ensure that only authorized program code is implemented. Consequently, VAMHCS increases its risk that unauthorized changes could be introduced into locally developed programs after they have been tested and approved but before they have been implemented. VAMHCS has access to a utility program that will allow it to identify unauthorized program changes that have been made to the VISTA production programs.

    Recommendation: Establish and implement procedures for periodically reviewing VISTA programs to ensure that only authorized program code is moved into production.

    Management Response: VAMHCS officials told us that by August 30, 2000, they would develop and implement procedures to periodically review the VISTA programs to ensure that only approved program changes are made and implemented.

Service Continuity

Service continuity controls should be designed to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected. These controls include (1) procedures designed to protect information resources and minimize the risk of unplanned interruptions and (2) a well-tested plan to recover critical operations should interruptions occur. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which

can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

17. **Weakness:** The VAMHCS disaster recovery plan did not include all key elements of a comprehensive disaster recovery plan. Specifically, the plan did not include detail recovery procedures for each system, priority order for system restoration, a list of key facility staff, and a list of outside agency and vendor contacts and their responsibilities, requirements for testing the plan, and provisions for periodically reviewing and updating the plan. In addition, the plan did not consider risks that may affect computer operations in meeting business operations. As a result, VAMHCS may not be able to recover all critical operations in the event of a disaster.

    Recommendation: Develop a comprehensive disaster recovery plan that is risk based and includes all the key elements of a comprehensive disaster recovery plan.

    Management Response: VAMHCS officials told us that they would develop a new disaster recovery plan by October 31, 2000. This plan would include risks that may affect the facility; a process for recovering each system; a list of key disaster recovery staff; a priority for restoring systems; requirements for plan testing; and provisions for periodically reviewing and updating the plan.

18. **Weakness:** VAMHCS was not performing periodic walk-throughs or unannounced tests of its disaster recovery plan. Conducting these types of tests provides a scenario that may be encountered in the event of an actual disaster.

    Recommendation: Perform periodic walk-throughs and unannounced tests of the disaster recovery plan.

    Management Response: VAMHCS officials told us that they would schedule periodic walk-throughs and unannounced tests and begin the testing by October 31, 2000.

Physical Security Access

Important information system controls for protecting access to data are the physical security control measures, such as locks, guards, and surveillance equipment that an organization has in place. Such controls are critical to safeguarding critical financial and sensitive information and computer operations from internal and external threats. At VAMHCS, we identified several areas where physical security could be improved.

19. **Weakness:** No formal procedures had been developed for granting access to the computer room or periodically reviewing user access. We found that all staff in the Information Resource Management office and two maintenance staff at the Baltimore Rehabilitation and Extended Care Center had keys to the computer

room. As a result, staff could obtain access or continue to have access to sensitive areas even though their job responsibilities may not warrant this access.

Recommendation: Develop and implement formal procedures for granting and periodically reviewing access to the main computer room and for removing any access that is not warranted.

Management Response: VAMHCS officials told us that by May 31, 2000, they would develop and implement guidelines that would allow only authorized personnel to access the computer and related telecommunications areas. In addition, they would establish a system to periodically review access to the computer room and related areas to remove access that is not warranted.

20. **Weakness:** Access to critical computer support facilities was not adequately secured. We found that (1) the door to the telecommunication room was often unlocked, (2) control and maintenance consoles to the site's telecom system were unattended and were left logged on to the system's main menus, and (3) the video conference console and an NT workstation were logged on and unattended. As a result, employees or intruders with malicious intent could gain improper access to sensitive information or disrupt hospital operations. VAMHCS did not have a procedure to periodically inspect physical access to its sensitive computer resources to ensure that they were adequately secured.

    Recommendation: Develop and implement a procedure to periodically review the adequacy of physical access to all sensitive computer resources.

    Management response: VAMHCS officials told us that by May 31, 2000, they would develop a system to periodically review the adequacy of physical access to all sensitive computer resources.

21. **Weakness:** There were no procedures to periodically account for all keys to the computer room. At Perry Point, the Engineering Division is responsible for maintaining control of all facility keys. However, we found that this division could not account for all master and submaster keys, including those that open the doors to the main computer room and telecommunication wiring closets. Until procedures are developed to routinely account for all keys, VAMHCS is at increased risk that physical security to the computer and telecommunication rooms at Perry Point will be compromised.

    Recommendation: Establish procedures to periodically account for all keys to computer rooms at Perry Point.

    Management Response: VAMHCS officials told us that by May 31, 2000, they would update VAMHCS policy and implement procedures to control all master keys and institute procedures to periodically account for all keys.

22. **Weakness:** During a tour of the computer room at the Perry Point facility, we found that two doors to the main computer room that were accessible to any one with access to the building were left unlocked. The weather stripping around one of these doors was improperly installed and, as a result, this door could not be locked. The second door was intentionally left unlocked. VAMHCS does not have procedures to periodically inspect physical access to its computer resources at the Perry Point facility. Without adequate protection of its physical computer assets, VAMHCS increases the risk of inadvertent or deliberate destruction of sensitive information or computer equipment.

    Recommendation: Develop and implement a process to periodically review the adequacy of physical access procedures to all sensitive computer resources at Perry Point.

    Management Response: VAMHCS officials told us that by April 30, 2000, they plan to develop and implement a process to periodically review the adequacy of physical access procedures to all sensitive computer resources at Perry Point.

Computer Security Management

Our May 1998 study of security management best practices found that a comprehensive computer security management program is essential to ensure that information system controls work effectively on a continuing basis. Under an effective computer security management program, staff (1) periodically assess risks, (2) implement comprehensive policies and procedures, (3) promote security awareness, and (4) monitor and evaluate the effectiveness of the computer security environment, which includes an incident reporting program. In addition, a central security function is maintained to provide computer security guidance and oversight.

Although VAMHCS has developed a security awareness program, it is lacking several key elements of a comprehensive security management program including the following areas.

23. **Weakness:** VA policy requires that risk assessments be performed every 3 years or when significant changes are made to a facility or its computer systems. VAMHCS had not performed a risk assessment of all its major systems within the last 3 years. In addition, VAMHCS had no process to assess risks when significant changes are made to its systems. For example, in the past 2 years, VAMHCS had upgraded its computer hardware and added network capabilities to the computer environment. Each of these events would have warranted a separate risk assessment.

    Recommendation: Perform a risk assessment of all major systems and establish a process for assessing risk when significant system changes occur, as required by VA policy.

Management Response: VAMHCS officials told us that by May 31, 2000, they would develop and implement a system for assessing risk, using its automated risk assessment tool, when any new systems are added or changes occur on the VA network.

24. **Weakness:** The information security officer who was responsible for security oversight of VAMHCS' various computer networks as a collateral duty had not received security training in these systems. Without adequate training in computer networks, including a comprehensive understanding of network security controls, the information security officer will be hampered in providing adequate security oversight.

    Recommendation: Establish a technical security training program for the information security officer.

    Management Response: VAMHCS officials told us that they plan to establish a full-time information security officer position by September 30, 2000. To fully support this position, technical training will be provided in NT, VISTA, and other key computer environments.

25. **Weakness:** VAMHCS had not established a program to routinely monitor and evaluate the effectiveness of information system controls. Our May 1998 study of security management best practices found that an effective control evaluation program includes processes for (1) monitoring compliance with established information system control policies and guidelines, (2) testing the effectiveness of information system controls, and (3) improving information system controls based on the results of these activities.

    As discussed in previous sections of this letter, we found weaknesses that included inadequately limiting access to the network and not maintaining effective user IDs and passwords. These weaknesses could have been identified and corrected if VAMHCS had been monitoring compliance with established procedures. For example, periodically reviewing the network parameters for security vulnerabilities would have allowed VAMHCS to discover and fix the type of network access control weaknesses we identified. Likewise, routinely reviewing passwords to monitor compliance with VA guidelines that prohibit the use of common words would mitigate some of the password security exposures we found.

    Recommendation: Establish and implement a program to routinely monitor and evaluate the effectiveness of the information system controls.

    Management Response: VAMHCS officials told us that by April 30, 2000, they would establish and implement a program to evaluate the effectiveness of their information system controls and compliance with policies and guidelines.

26. **Weakness:** VAMHCS did not have a formal incident response plan and a formal response team in place to respond promptly and efficiently to information system security incidents, whether an incident was caused by a computer virus, other malicious codes, or a system intruder. Without a formal response plan and team, VAMHCS cannot assure its users that data would be protected, that security incidents would be handled quickly and efficiently, and that corrective actions would be implemented.

    Recommendation: Develop and implement a formal incident response plan and team to support VAMHCS operations around the clock, 7 days a week.

    Management Response: VAMHCS officials told us that by April 30, 2000, they would develop and implement an incident response plan to include the establishment of an incident review team and guidelines for the team. This plan would support VAMHCS around the clock.

Enclosure 2

GAO Contact and Staff Acknowledgments

GAO Contact

David W. Irvin, (214) 777-5716

Acknowledgments

In addition to the contact named above, Lon C. Chin, Denise Fitzpatrick, Jeffrey Knott, Harold Lewis, Norman Poage, Charles M. Vrabel, and Christopher J. Warweg made key contributions to this report.

(919470)

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

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested