United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Health, Committee on Ways and Means, House of Representatives

For Release on Delivery
Expected at 3:00 p.m.
Tuesday, July 20, 1999

MEDICARE

HCFA Needs to Better Protect Beneficiaries' Confidential Health Information

Statement of Leslie G. Aronovitz, Associate Director
Health Financing and Public Health Issues
Health, Education, and Human Services Division

GAO/T-HEHS-99-172

Medicare: HCFA Needs to Better Protect Beneficiaries' Confidential Health Information

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss how the Health Care Financing Administration (HCFA) protects personally identifiable health information on Medicare beneficiaries. HCFA, an agency of the Department of Health and Human Services (HHS), possesses the nation's largest collection of health care data, with information on 39 million Medicare beneficiaries. To operate the Medicare program, HCFA must collect personally identifiable information on Medicare beneficiaries, such as their names, addresses, and health insurance claims numbers, as well as their diagnostic and treatment information. HCFA uses this information for a variety of purposes, including paying approximately 900 million Medicare claims annually and conducting health-related research to improve quality of care. When a person signs up for Medicare, he or she might not realize the variety of uses HCFA makes of his or her personally identifiable information or that this personal information may legitimately be disclosed by HCFA outside the agency.

The personally identifiable information that HCFA collects on Medicare beneficiaries is protected by the Privacy Act of 1974. This law, which governs the collection, maintenance, and disclosure of federal agency records, balances the government's need to maintain information about individuals with their right to be protected against unwarranted invasions of their privacy. State laws also protect the privacy of certain personally identifiable medical information, and vary significantly in their scope and specific provisions. To create a more uniform set of protections, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that, unless Congress enacts a health privacy law establishing standards for the electronic exchange of health information by August 21, 1999, HHS must promulgate such standards within the following 6 months.

Today, we are releasing a report you requested that focuses on four areas related to HCFA's use of personally identifiable information.[1] They are:

- HCFA's need for personally identifiable health information to manage the Medicare program;
- HCFA's policies and practices regarding disclosure of information on Medicare beneficiaries to other organizations;

[1]MEDICARE: Improvements Needed to Enhance Protection of Confidential Health Information (GAO/HEHS-99-140, July 20, 1999).

- The adequacy of HCFA's safeguards for protecting the confidentiality of electronic information and its monitoring of other organizations that obtain information on Medicare beneficiaries; and
- The effect on HCFA of state restrictions on the disclosure of confidential health information.

To develop our findings, we interviewed HCFA officials and reviewed documents HCFA provided on its confidentiality policies and procedures. We also reviewed guidance from the Office of Management and Budget (OMB) related to the Privacy Act, financial statement audits of HCFA from the HHS Office of the Inspector General (OIG), and HCFA's plan for addressing problems identified in the OIG audits. In addition, we examined the privacy protections of a number of state laws and obtained comments from HCFA officials about the effects of such laws on the management of the Medicare program.

In summary, we found that personally identifiable information on Medicare beneficiaries is vital to the operation of the Medicare program, and that HCFA can disclose such information to other organizations consistent with provisions of the Privacy Act. HCFA has policies and procedures for evaluating requests for disclosure of personally identifiable health information, but HCFA's confidentiality practices have a number of weaknesses. These weaknesses include HCFA's inability to easily provide beneficiaries with an accounting of disclosures made of their personal information and failure to always give them clear notification of the purposes for which their personal information may be disclosed outside of HCFA as required by the Privacy Act. Although few complaints of violations have been reported to date, the OIG also continues to report vulnerabilities in HCFA's safeguards for confidentiality of electronic information. These vulnerabilities could lead to unauthorized individuals reading, disclosing, or altering confidential information. Finally, potential conflicts exist between HCFA and state laws regarding the disclosure of sensitive health information. To date, conflicts have been minimal and the administration of Medicare has not been hindered, according to HCFA officials, because all states permit release of information for health care treatment and payment. However, if the same data elements were not available from all states, it might compromise HCFA's ability to conduct research and analysis to improve Medicare policies.

Background

In protecting the confidentiality of beneficiaries' health information, HCFA's activities, like those of other federal agencies, are governed by the Privacy

Act of 1974. The Privacy Act requires that agencies limit their maintenance of individually identifiable records to those that are relevant and necessary to accomplish an agency's mission. Federal agencies store personally identifiable information in systems of records. A system of records is a group of records under the control of a federal agency from which information can be retrieved using the name of an individual or an identifier such as a number assigned to the individual. The Privacy Act defines a record as any item, collection, or grouping of information maintained by an agency that contains an individual's name or other identifying information. A record, for example, could include information on education, financial transactions, or medical history. Under the Privacy Act, federal agencies must inform the public when they create a new system of records or revise an existing system. This is done through publication in the Federal Register. A new system of records is announced when an agency wishes to collect new data. Sixty-two of HCFA's 81 systems of records relate directly to Medicare beneficiaries and include personally identifiable data on a Medicare beneficiary's enrollment and entitlement to benefits; demographic information such as age, race, ethnicity, and language preference; and diagnostic and treatment information. HCFA's systems of records contain information stored in electronic and paper forms.

The Privacy Act generally prohibits the disclosure of individuals' records without their consent. However, it allows the disclosure of information without an individual's consent under 12 circumstances called conditions of disclosure. One example is disclosure by a federal agency to its employees based on their need for the records to perform their duties. Another condition of disclosure allows an agency to establish routine uses under which information can be disclosed to a data requestor. One routine use, for example, could be disclosure to an individual or organization for a research project related to an agency objective, such as prevention of disease or disability in HCFA's case. To establish a routine use, the agency must determine that a use is compatible with the purposes for which the information was collected and they must publish the notice of the routine use in the Federal Register. While the Privacy Act permits agencies to disclose information, it does not require that they do so; they can, for example, determine that in a particular case, the individual's privacy interest outweighs the public interest in disclosure.

HCFA Needs Personally Identifiable Information on Medicare Beneficiaries

Personally identifiable information is essential to HCFA's day-to-day administration of the Medicare program. Of primary importance is the need of the agency and its contractors to use personally identifiable information on Medicare patients to pay approximately 900 million fee-for-service claims annually. HCFA also uses this information to determine the initial and ongoing eligibility of Medicare beneficiaries, determine risk-adjusted payments, make monthly payments to about 400 Medicare managed care plans, and track which managed care plans have been selected by over 6 million Medicare beneficiaries. HCFA and its contractors use beneficiary claims data containing personally identifiable information to prevent fraud and abuse; administer the Medicare Secondary Payer program;[2] develop fee schedules and payment rates used in fee-for-service claims processing; review the access, appropriateness, and quality of care received by beneficiaries; and conduct research and demonstrations including the development and implementation of new health care payment approaches and financing policies.

HCFA Discloses Information About Beneficiaries for Authorized Purposes

In screening requests for identifiable information, HCFA determines whether disclosure is authorized by the Privacy Act. It also has different levels of review depending upon the type of organization making a request for information. HCFA's policy and practice is generally to limit disclosures to information needed to accomplish the requestor's purposes. However, we found weaknesses in its recordkeeping system for tracking and reporting on disclosures and its notices to beneficiaries that their information could be disclosed.

HCFA Screens Requests for Personally Identifiable Information

In making decisions about whether to disclose information, HCFA's primary criterion is whether the disclosure is permitted under a routine use or one of the 11 other Privacy Act conditions of disclosure. HCFA can disclose information under routine uses to publicly and privately funded researchers and to public agencies such as the Agency for Health Care Policy and Research for health services research projects; to qualified state agencies for the purposes of determining, evaluating, or assessing cost, effectiveness, or quality of health care services provided in a state;

[2]The Medicare Secondary Payer provision limits payment under Medicare for otherwise covered items or services if that payment has been made or can be reasonably expected to be made from another source such as under a workmen's compensation law, automobile or liability insurance policy, or certain health plans. In such cases, Medicare payments for items or services are conditional payments and Medicare is entitled to reimbursement from the other sources for the full amount of Medicare payments.

and to insurers, underwriters, employers who self-insure, and others for coordination of benefits with the Medicare Secondary Payer program.

When deciding whether to disclose personally identifiable information, HCFA has different levels of review depending on the type of organization making a request for information. According to HCFA policy, HCFA employees and claims administration contractors are provided access to personally identifiable information only when they require such information to perform their official duties. Other federal agencies and organizations, such as state governments and law enforcement agencies seeking information on Medicare beneficiaries, must submit documentation, such as a signed data use agreement that indicates their acceptance of the confidentiality requirements of the Privacy Act and HCFA's data use policies and procedures. These policies and procedures include a requirement that the data user will not publish or release information that could allow deduction of a beneficiary's identity. When reviewing documentation from requestors, HCFA determines whether the disclosure is permitted under a routine use for a system of records or other condition of disclosure, as allowed by the Privacy Act. In screening requests from outside researchers, HCFA also requires the submission of a detailed study protocol. Further, researchers must receive approval from the HCFA Administrator when they request the names and addresses of Medicare beneficiaries they intend to contact to collect new data.

HCFA Generally Limits Disclosures to Information Needed to Accomplish Purposes

HCFA officials told us their practice is to disclose the least amount of personally identifiable information that will accomplish the purpose of the individual or organization making the request. HCFA generally provides one of three types of data files—public-use files, beneficiary-encrypted files, and files which contain explicitly identifiable information. Public-use files are stripped of identifying information on beneficiaries and usually are summarized data. Beneficiary-encrypted files are data sets in which HCFA has encoded or removed the health insurance claim number, date of service, beneficiary name, or beneficiary zip code. Explicitly identifiable files contain such information as beneficiary names, addresses, and health insurance claim numbers. HCFA officials said they direct requestors whenever possible to either public-use files or to beneficiary-encrypted files rather than to the files containing more identifiable beneficiary information. However, when HCFA does disclose data files with personally identifiable information, it generally does not customize them for the specific purpose of reducing the amount of information disclosed. HCFA officials told us that to do so would be a resource-intensive process;

however, they are now developing software that will permit them to easily customize data elements in the future.

HCFA's Recordkeeping System for Tracking and Reporting Has Weaknesses

Although Medicare beneficiaries have the right under the Privacy Act to ask for and receive an accounting of disclosures of their personally identifiable information and to examine or amend their individual records, HCFA's recordkeeping system is incapable of readily providing an accounting of disclosures to beneficiaries. The Act requires that the accounting include information on the nature and purpose of the disclosure and the name and address of the person or organization to whom the disclosure was made. HCFA officials told us that the agency's computerized system for tracking disclosures cannot easily generate information for an individual beneficiary on disclosures made from HCFA's system of records. Weaknesses in HCFA's recordkeeping system also affect its ability to report on its Privacy Act activities to oversight agencies such as OMB.

HCFA officials also told us that they are working on improving their recordkeeping system to better account for disclosures of personally identifiable information made by the agency. HCFA officials said that, as directed by OMB, they have begun reviewing their recordkeeping for Privacy Act activities. In January 1999, OMB released guidance based on a May 14, 1998, presidential memorandum directing each agency to review its information practices to ensure compliance with the Privacy Act. HCFA has begun to address OMB guidance and officials told us that they are reviewing routine uses that allow disclosure of Medicare beneficiaries' information. In May 1999, HCFA established an executive-level Beneficiary Confidentiality Board to review strategic confidentiality issues including HCFA's policies and procedures for disclosing personally identifiable information.

Weaknesses Exist in Notifications to Beneficiaries That Their Information Could Be Disclosed

The Privacy Act requires federal agencies to permit an individual to find out what records pertaining to him or her are collected, maintained, used, or disseminated by the agencies. The Act requires an agency to notify individuals of the following when it collects information: (1) the authority under which the agency is collecting the information, (2) the principal purpose for the information, (3) routine uses that may be made of the information, and (4) whether the individual is required to supply the information and the effects on the individual of not providing it.

HCFA officials told us they use more than a dozen different Privacy Act notifications when collecting information from beneficiaries. Individuals' first exposure to a Medicare-related Privacy Act notice is usually at the time of their application for Social Security retirement benefits, when they are provided with a multi-page Privacy Act notice. Approved Social Security retirement benefit applicants are automatically enrolled in Medicare at age 65. Beneficiaries should receive other Privacy Act notifications whenever HCFA collects information about them—for example, if they separately enroll in Supplemental Medical Insurance (Medicare Part B), receive medical care, or participate in a survey or a demonstration project.[3]

While some of the HCFA Privacy Act notification forms we reviewed contain the required information, we found that others do not tell beneficiaries the purposes for which their information may be disclosed outside of HCFA, or they do so in an unclear fashion. For example, a form for beneficiaries receiving services in skilled nursing facilities provided the required information, but the Privacy Act notice for Medicare Part B enrollment did not identify the routine uses that would be made of the beneficiary's information and provided only a vague reference to the Federal Register as a source for such information. We found similar problems in a form used to collect information on end-stage renal disease beneficiaries.

Inadequate HCFA Safeguards Could Compromise Confidentiality

Although the procedures specified in HCFA's systems security manual generally adhere to OMB's guidance for safeguarding electronic information, the OIG has identified serious control weaknesses with HCFA's safeguarding of confidential information.[4] The OIG's audits of fiscal years 1997 and 1998 financial statements identified a variety of problems with HCFA's safeguards for electronic information at HCFA's central office and for selected Medicare claims administration contractors. The OIG reported the need for HCFA to implement an overall security structure and discussed weaknesses in the following areas: computer access controls (techniques to ensure that only authorized persons access the computer system),

[3]Medicare Part B helps pay for doctors, outpatient hospital care, and other medical services such as physical and occupational therapy.

[4]HHS/OIG, Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1996 (CIN: A-17-95-00096, July 17, 1997); HHS/OIG, Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1997 (CIN: A-17-97-00097, Apr. 24, 1998); HHS/OIG, Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1998 (CIN: A-17-98-00098, Feb. 26, 1999). See also Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, Sept. 23, 1998).

segregation of duties (the division of steps among different individuals to reduce the risk that a single individual could compromise security), and service continuity (the ability to recover from a security violation and provide service sufficient to meet the minimal needs of users of the system). The OIG also reported problems with controls over operating system software integrity and application development and change controls. However, HCFA has reported few complaints of potential Privacy Act violations.

When the OIG conducted work at 12 Medicare contractors for its fiscal year 1998 audit, auditors were able to penetrate security and obtain access to sensitive Medicare data at 5 of them. The auditors' ability to do so without using their formal access privileges is of particular concern because unauthorized users can exploit this security weakness in several ways and compromise confidential medical data.

Agency officials told us they are in the process of taking action to correct the weaknesses identified by the OIG. However, HCFA's ability to make progress is currently affected by the agency's efforts to address computer requirements for the year 2000 so that there will be no interruption of services and claims payments. HCFA, consistent with priorities established by OMB, has a moratorium on software and hardware changes until it is compliant with year 2000 computer requirements. During its fiscal year 1999 financial statement audit, the OIG will evaluate the effectiveness of any corrective actions that HCFA is able to implement.

HCFA Does Not Systematically Monitor How Organizations Protect the Confidentiality of Medicare Data

Although HCFA has a process for monitoring systems security at its claims administration contractors, agency officials told us that competing demands and resource constraints have prevented them from monitoring whether these organizations follow OMB guidance for protecting the confidentiality of information. HCFA officials told us that, other than OIG reviews, there were no explicit on-site reviews of contractors' security protections in fiscal years 1997 and 1998 because of resource constraints and the assignment of staff to assess contractor year 2000 computer requirements. However, HCFA did initiate reviews of network security in 1998 for 12 Medicare contracts at 4 of its 60 claims processing contractors.

In addition, HCFA officials told us that they do not have a system for monitoring whether organizations outside of HCFA have established safeguards for personally identifiable information received from the agency. When organizations sign data use agreements with HCFA, they

agree to establish appropriate administrative, technical, and physical safeguards, providing a level and scope of security that is not less than the level and scope established by OMB. Data use agreements also include requirements that those receiving information from HCFA use the data only for their HCFA-approved purpose and that the data be returned to HCFA or destroyed upon completion of the project. HCFA does not systematically monitor how the data are being used. Although the agency follows up on expired data use agreements, HCFA currently has a backlog of about 1,400 expired agreements. It expects to reduce the backlog by one-half by September 30, 1999.

HCFA's failure to monitor contractors and others who use personally identifiable Medicare information hampers HCFA's ability to prevent the occurrence of problems and to provide timely identification and corrective action for those that have occurred.

Few Complaints of Privacy Act Violations Reported

The agency identified 7 complaints of potential violations of the Privacy Act it has received and resolved in the past 4 years. Six complaints involved contractors conducting research for HCFA, health data organizations, and individual researchers; the seventh complaint was made by a Medicare beneficiary's attorney. The first six complaints were raised by similar organizations or other researchers and involved posting of potentially identifiable Medicare billing information on an Internet website, using and publishing data in a second research project without authorization from HCFA, and offering to share Medicare files at a national research conference. In the first six cases, HCFA provided direction on Privacy Act requirements to those involved. In the seventh case, HCFA provided the beneficiary's attorney with a letter addressing the issues raised.

HCFA reported only one internal disciplinary action within the past 5 years relating to violations of HCFA's confidentiality policies. This incident involved an agency employee who was accessing beneficiary files more frequently than appeared necessary for performing his job. The employee admitted to looking at files of famous people. He was placed on administrative leave and later signed an affidavit stating that the files had not been sold or shared with other persons; accordingly, he was allowed to resign.

Some States Restrict Disclosure of Sensitive Confidential Information

In its oversight of the Medicare program, HCFA necessarily deals with beneficiaries and providers from every state. States have laws governing the confidentiality of health information. For example, in Florida, mental health records are confidential and may be disclosed only under limited circumstances. State laws vary significantly, resulting in what has been called a patchwork system of protections.

Conflicts between HCFA and the states involving medical record disclosures have been minimal, according to HCFA officials, and HCFA officials believe its administration of the Medicare program has not been hindered because all states permit release of information for health care treatment and payment. If a state law prohibited disclosure of information to HCFA that was critical for these purposes, and a federal statute required such disclosure, HCFA officials told us that the agency would rely on the Supremacy Clause of the U.S. Constitution and its express statutory authority.[5]

HCFA officials told us that if information is not critical to HCFA operations, HCFA's policy is to respect and abide by state laws that provide greater health records protection than would otherwise be required by federal law or regulation. For example, when California and Washington notified HCFA that laws in their states did not authorize the disclosure of diagnostic information related to the human immunodeficiency virus (HIV), acquired immunodeficiency syndrome (AIDS) and sexually transmitted diseases (STD), HCFA changed the system used to collect and analyze certain nursing home information by allowing the states to withhold diagnostic information collected about HIV/AIDS and STDs for their nursing home patients.[6] HCFA told us that 15 states have exercised this option by blanking out identifiable codes for HIV/AIDs or STDs before submitting the requisite information to HCFA. According to HCFA officials, the deletion of diagnostic information collected about HIV/AIDS and STDs for nursing home patients generally has not affected its operations. However, HCFA officials told us that the agency will require diagnostic information as it refines its new prospective payment system for skilled nursing facilities as well as its other payment systems and may, therefore, need to change its policy of allowing states to withhold information.

[5]U.S. Const. Art. VI, cl. 2. The Supreme Court has construed the Supremacy Clause of the U.S. Constitution to hold that federal law preempts state law where, for example: (1) the state law directly conflicts with federal law, (2) the federal legislative scheme leaves no room for state regulation, or (3) the state statute frustrates or conflicts with the purposes of the federal law.

[6]The information is used by HCFA to track changes in health and functional status of nursing home residents. The information system is known as the National Minimum Data Set (Resident Assessment Instrument) repository.

Restricting HCFA from receiving uniform health information across the country could adversely affect internal operations such as rate-setting and monitoring for quality assurance. It could also affect the ability of analysts in HCFA, other federal agencies, and nongovernmental organizations to conduct policy analysis and health services research because of the difficulty in complying with varying state laws. If the same data elements and health information were not available from all states, HCFA's ability to conduct research and analysis to improve Medicare policies might be compromised.

Conclusions and Recommendations

In its role as administrator and overseer of the nation's Medicare program, HCFA must collect and maintain personally identifiable information on millions of beneficiaries to effectively operate and manage the program. As a steward of confidential information, HCFA must balance its need to effectively manage the Medicare program with the privacy concerns of its beneficiaries. HCFA must protect beneficiaries' health information from inappropriate or inadvertent disclosures.

We found that HCFA's policies and practices are generally consistent with Privacy Act protections. However, we also found that the agency needs to do a better job implementing and enforcing certain protections. As the OIG has reported, HCFA continues to have vulnerabilities in its information management systems. In addition, HCFA has not consistently monitored its claims administration contractors' safeguards for protecting confidential information. We recognize that HCFA, consistent with priorities set forth by OMB, has focused its resources on ensuring that the agency and its contractors are compliant with year 2000 computer requirements. Nonetheless, we believe that reducing the vulnerabilities in its information systems and increasing its monitoring of contractors are important concerns that HCFA must address in the coming year.

HCFA also needs to better implement other aspects of its confidentiality policies and practices. The agency does not always fully and clearly inform beneficiaries that their information may be disclosed. It also lacks the ability to readily provide beneficiaries with an accounting of disclosures. In addition, HCFA does not have a formal system for monitoring the confidentiality protections of organizations to which it discloses personally identifiable information. As a result, HCFA is unable to systematically reduce the likelihood of inappropriate use of the data or identify instances of such misuse.

Although few complaints about Privacy Act violations have been made to date, we believe that the weaknesses we and others have identified potentially compromise the confidentiality of health information on Medicare beneficiaries. However, HCFA has begun some important initiatives that appear promising and could improve its protection of Medicare beneficiary health information. These include the creation of a new beneficiary confidentiality board and actions taken in response to OMB guidance for agencies to reevaluate the circumstances under which they disclose information.

Our report makes recommendations to the HCFA Administrator to improve HCFA's protection of the confidentiality of personally identifiable information on Medicare beneficiaries. In summary, we recommend that HCFA correct the vulnerabilities identified in its information management systems by the OIG, systematically monitor contractors' safeguards for protecting confidential information; develop a system to routinely monitor other organizations that have received personally identifiable information on Medicare beneficiaries; ensure that all agency Privacy Act notifications contain the information required by the Act in a form that is clear and informative to beneficiaries, and implement a system that would permit HCFA to respond in a timely fashion to beneficiary inquiries about disclosure of their information outside HCFA as well as to provide information on Privacy Act activities to OMB and others.

Mr. Chairman, this concludes my prepared statement. I would be happy to answer any questions you or the Subcommittee members may have.

GAO Contacts and Acknowledgments

For future contacts regarding this testimony, please call Leslie G. Aronovitz at (312) 220-7600 or Bruce D. Layton at (202) 512-6837. Key contributors to this testimony include Nancy Donovan, Bonnie Brown, Nila Garces-Osorio, Barry Bedrick, and Julian Klazkin.

Related GAO Products

Medicare: Improvements Needed to Enhance Protection of Confidential Health Information (GAO/HEHS-99-140, July 20, 1999).

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999).

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, Apr. 27, 1999).

Financial Audit: 1998 Financial Report of the United States Government (GAO/AIMD-99-130, Mar. 31, 1999).

Auditing the Nation's Finances: Fiscal Year 1998 Results Highlight Major Issues Needing Resolution (GAO/T-AIMD-99-131, Mar. 31, 1999).

Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Is Limited (GAO/HEHS-99-55, Feb. 24, 1999).

Year 2000 Computing Crisis: Readiness Improving, but Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-50, Jan. 20, 1999).

Major Management Challenges and Program Risks: Department of Health and Human Services (GAO/OGC-99-7, Jan. 1999).

Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, Sept. 28, 1998).

Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, Sept. 23, 1998).

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. 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

or visit:

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

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or 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.

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

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