United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, July 24, 2007

VETERANS AFFAIRS

Lack of Accountability and Control Weaknesses over IT Equipment at Selected VA Locations

Statement of McCoy Williams,
Director, Financial Management and Assurance

July 24, 2007

VETERANS AFFAIRS

Lack of Accountability and Control Weaknesses over IT Equipment at Selected VA Locations

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-1100T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

Why GAO Did This Study

In July 2004, GAO reported that the six Department of Veterans Affairs (VA) medical centers it audited lacked a reliable property control database and had problems with implementation of VA inventory policies and procedures. Fewer than half the items GAO selected for testing could be located. Most of the missing items were information technology (IT) equipment. In light of these concerns and recent thefts of laptops and data breaches at VA, this testimony focuses on (1) the risk of theft, loss, or misappropriation of IT equipment at selected locations; (2) whether selected locations have adequate procedures in place to assure accountability and physical security of IT equipment in the excess property disposal process; and (3) what actions VA management has taken to address identified IT inventory control weaknesses. GAO statistically tested inventory controls at four case study locations.

What GAO Recommends

GAO's companion report (GAO-07-505), released with this testimony, includes12 recommendations to improve VA-wide policies and procedures with respect to controls over IT equipment, including recordkeeping requirements, physical inventories, user-level accountability, and physical security. VA agreed with GAO's findings, noted significant actions under way, and concurred on the 12 recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-1100T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact McCoy Williams at (202) 512-9095 or williamsm1@gao.gov.

What GAO Found

A weak overall control environment for VA IT equipment at the four locations GAO audited poses a significant security vulnerability to the nation's veterans with regard to sensitive data maintained on this equipment. GAO's *Standards for Internal Control in the Federal Government* requires agencies to establish physical controls to safeguard vulnerable assets, such as IT equipment, which might be vulnerable to risk of loss, and federal records management law requires federal agencies to record essential transactions. However, GAO found that current VA property management policy does not provide guidance for creating records of inventory transactions as changes occur. GAO also found that policies requiring annual inventories of sensitive items, such as IT equipment; adequate physical security; and immediate reporting of lost and missing items have not been enforced. GAO's statistical tests of physical inventory controls at four VA locations identified a total of 123 missing IT equipment items, including 53 computers that could have stored sensitive data. The lack of user-level accountability and inaccurate records on status, location, and item descriptions make it difficult to determine the extent to which actual theft, loss, or misappropriation may have occurred without detection. The table below summarizes the results of GAO's statistical tests at each location.

Current IT Inventory Control Failures at Four Test Locations

Control failures	Washington, D.C.	Indianapolis	San Diego	VA HQ offices
Missing items	28%	6%	10%	11%
Incorrect user organization	80%	69%	70%	11%
Incorrect location	57%	23%	53%	44%
Recordkeeping errors	5%	0%	5%	3%

Source: GAO analysis.

Note: Each of these estimates has a margin of error, based on a two-sided, 95 percent confidence interval, of +/- 10 percent or less.

GAO also found that the four VA locations reported over 2,400 missing IT equipment items, valued at about $6.4 million, identified during physical inventories performed during fiscal years 2005 and 2006. Missing items were often not reported for several months and, in some cases, several years. It is very difficult to investigate these losses because information on specific events and circumstances at the time of the losses is not known. GAO's limited tests of computer hard drives in the excess property disposal process found hard drives at two of the four case study locations that contained personal information, including veterans' names and Social Security numbers. GAO's tests did not find any remaining data after sanitization procedures were performed. However, weaknesses in physical security at IT storage locations and delays in completing the data sanitization process heighten the risk of data breach. Although VA management has taken some actions to improve controls over IT equipment, including strengthening policies and procedures, improving the overall control environment for sensitive IT equipment will require a renewed focus, oversight, and continued commitment throughout the organization.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss our recent audit of controls over information technology (IT) equipment at the Department of Veterans Affairs (VA). In light of reported weaknesses in VA inventory controls and reported thefts of laptop computers and data breaches, the adequacy of such controls has been an ongoing concern. Today, I will summarize the results of our recent work, the details of which are included in our audit report, which the Subcommittee is releasing today.[1] This audit followed a July 2004 report[2] in which we identified weak practices and lax implementation of controls over equipment at the six VA medical centers we audited. As a result, personnel at the VA medical centers located fewer than half of the 100 items we selected for testing at each of five medical centers and 62 of 100 items at the sixth medical center. Most of the items that could not be located were computer equipment.

For today's testimony, I will provide the highlights of our current findings related to

- the risk of theft, loss, or misappropriation[3] of IT equipment[4] at selected VA locations;
- whether selected VA locations have adequate procedures in place to assure physical security and accountability over IT equipment in the excess property disposal process;[5] and
- what actions VA management has taken to address identified IT equipment inventory control weaknesses.

[1]GAO, *Veterans Affairs: Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation*, GAO-07-505 (Washington, D.C.: July 16, 2007).

[2] GAO, *VA Medical Centers: Internal Control over Selected Operating Functions Needs Improvement*, GAO-04-755 (Washington, D.C.: July 21, 2004).

[3] As used in this testimony, theft and misappropriation both refer to the unlawful taking or stealing of personal property, with misappropriation occurring when the wrongdoer is an employee or other authorized user.

[4] For the purpose of our test work, we defined IT equipment as any equipment capable of processing or storing data, regardless of how VA classifies it. Therefore, medical devices that would typically not be classified as IT equipment, but may capture, process, or store patient data, were considered IT equipment for this audit.

[5] As used in this testimony, the term excess property refers to property that a federal agency leases or owns that is not required to meet either the agency's needs or any other federal agency's needs.

My statement is based on our report on VA IT inventory controls, which you are releasing today.[6] As part of our audit, we statistically tested IT equipment inventory at selected case study locations. In addition, our investigator inspected physical security at IT equipment storage sites. We performed our audit procedures in accordance with generally accepted government auditing standards, and we performed our investigative procedures in accordance with quality standards for investigators as set forth by the President's Council on Integrity and Efficiency.

Summary

Our statistical tests of IT equipment inventory controls at our four VA case study locations identified a total of 123 missing IT equipment items, including 53 computers that could have stored sensitive data. Our estimates of the percentage of inventory control failures related to these missing items ranged from 6 percent at the Indianapolis medical center to 28 percent at the Washington, D.C., medical center.[7] In addition, we determined that VA property management policy does not establish accountability with individual users of IT equipment. Consequently, our control tests identified a pervasive lack of user-level accountability across the four case study locations and significant errors in recorded IT inventory information concerning user organization and location. As a result, we concluded that for the four case study locations we audited, essentially no one was accountable for IT equipment.

Our analysis of the results of physical inventories performed by the current four case study locations[8] identified over 2,400 missing IT equipment items, with a combined original acquisition value of about $6.4 million. In addition, the five other locations we previously audited had reported over 8,600 missing IT equipment items with a combined original acquisition value of over $13.2 million. Further, we found that missing IT items were often not reported for several months and, in some cases, several years, because most of the case study locations had not

[6] GAO-07-505.

[7] Each of these estimates has a margin of error, based on a two-sided, 95 percent confidence interval, of +/- 7 percent or less.

[8] The Washington, D.C., medical center was covered in both audits.

consistently performed physical inventories or completed Reports of Survey[9] promptly.

Our limited tests of computer hard drives in the excess property disposal process at the four case study locations found no data on those hard drives that were certified as sanitized.[10] However, file dates on the hard drives we tested indicated that some of them had been in the disposal process for several years without being sanitized, creating an unnecessary risk of compromising sensitive personal and medical information. We also found numerous unofficial IT equipment storage locations in VA headquarters area office buildings that did not meet VA physical security requirements. For example, at some VA headquarters locations, excess computer equipment was stored in open or unsecured areas.

Since our July 2004 report, VA management has taken some actions and has other actions under way to strengthen controls over IT equipment, including clarifying property management policies[11] and centralizing functional IT units under the new Chief Information Officer (CIO) organization. Even with these improvements, the department had not yet established and ensured consistent implementation of effective controls for accountability of IT equipment inventory, and IT inventory responsibilities are not well-defined. Until these shortcomings are addressed, VA will continue to face major challenges in safeguarding IT equipment and sensitive personal data on this equipment from loss, theft, and misappropriation. Our companion report released today includes 12 recommendations to VA to improve the overall control environment and strengthen key internal control activities and to increase attention to protecting IT equipment used in VA operations. VA generally agreed with our findings, noted significant actions under way, and concurred on the 12 recommendations.

[9] The Report of Survey system is the method used by VA to obtain an explanation of the circumstances surrounding loss, damage, or destruction of government property other than through normal wear and tear.

[10] VA information resource management (IRM) personnel and contractors follow National Institute of Standards and Technology (NIST) Special Publication 800-88 guidelines as well as more stringent Department of Defense (DOD) policy in DOD 5220.22-M, *National Industrial Security Program Operating Manual*, ch. 8, § 8-301, which requires performing three separate erasures for media sanitization.

[11] VA Handbook 7127/4 § 5302.3, "Inventory of Equipment in Use."

Inadequate IT Inventory Control and Accountability Pose Risk of Loss, Theft, and Misappropriation

Our tests of IT equipment inventory controls at four case study locations, including three VA medical centers and VA headquarters, identified a weak overall control environment and a pervasive lack of accountability for IT equipment items across the locations we tested. As summarized in table 1, our statistical tests of key IT inventory controls at our four case study locations found significant control failures. None of the case study locations had effective controls to safeguard IT equipment from loss, theft, and misappropriation.

Table 1: Current IT Equipment Inventory Control Failure Rates at Four Test Locations

Control failures	Washington, D.C., medical center	Indianapolis medical center	San Diego medical center	VA headquarters offices
Missing items in sample	28%	6%	10%	11%
Incorrect user organization	80%	69%	70%	11%
Incorrect user location	57%	23%	53%	44%
Recordkeeping errors	5%	0%	5%	3%

Source: GAO analysis.

Notes: Each of these estimates has a margin of error, based on a two-sided, 95 percent confidence interval, of +/- 10 percent or less. Because the four test locations did not record all IT equipment items in their inventory records, our estimated failure rates relate to current (recorded) inventory and not the population of all IT equipment at those locations.

Our statistical tests identified a total of 123 lost and missing IT equipment items across the four case locations, including 53 IT equipment items that could have stored sensitive personal information. Such information could include names and Social Security numbers protected under the Privacy Act of 1974[12] and personal health information accorded additional protections from unauthorized release under the Health Information Portability and Accountability Act of 1996 (HIPAA) and implementing regulations.[13] Although VA property management policy[14] establishes guidelines for holding employees and supervisors pecuniarily (financially) liable for loss, damage, or destruction because of negligence and misuse of government property, except for a few isolated instances, none of the case study locations assigned user-level accountability for IT equipment.

[12] Privacy Act of 1974, *codified*, *as amended*, at 5 U.S.C. § 552a.

[13] HIPAA, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033-34 (Aug. 21, 1996). The Secretary of Health and Human Services has prescribed standards for safeguarding medical information in the HIPAA Medical Privacy Rule. *See* 45 C.F.R. pt. 164.

[14] VA Handbook 7125, *Materiel Management General Procedures*, § 5003 (Oct. 11, 2005).

Instead, these locations relied on information about user organization and user location, which was often incorrect and incomplete. Under this lax control environment, missing IT equipment items were often not reported for several months and, in some cases several years, until the problem was identified during a physical inventory.

Inventory Tests Identified Significant Numbers of Missing Items

Our statistical tests of IT equipment existence at the four case study locations identified a total of 123 missing IT equipment items. The 123 missing IT equipment items included 44 at the Washington, D.C., medical center; 9 at the Indianapolis medical center; 17 at the San Diego medical center; and 53 at VA headquarters. Our statistical tests of missing equipment found that none of the four test locations had effective controls.

Missing IT equipment items pose not only a financial risk but also a security risk associated with compromising sensitive personal data maintained on computer hard drives. The 123 missing IT equipment items included 53 that could have stored sensitive personal information, including 19 from the Washington, D.C., medical center; 3 from the Indianapolis medical center; 8 from the San Diego medical center; and 23 from VA headquarters. Because of a lack of user-level accountability and the failure to consistently update inventory records for inventory status and user location changes, VA officials at our test locations could not determine the user or type of data stored on this equipment and therefore the risk posed by the loss of these items.

Pervasive Lack of User-Level Accountability for IT Equipment at Case Study Locations

VA management has not enforced VA property management policy and has generally left implementation decisions up to local organizations, creating a nonstandard, high-risk environment. Although VA property management policy establishes guidelines for user-level accountability,[15] the three medical centers we tested assigned accountability for most IT equipment to their information resource management (IRM) or IT Services organizations, and VA headquarters organizations tracked IT equipment items through their IT inventory coordinators. However, because these personnel did not have possession (physical custody) of all IT equipment under their purview, they were not held accountable for IT equipment determined to be missing during physical inventories. Because of this

[15] VA Handbook 7125, *Materiel Management General Procedures*, § 5003.

weak overall control environment, we concluded that at the four case study locations essentially no one was accountable for IT equipment.

Absent user-level accountability, accurate information on the using organization and location of IT equipment is critical to maintaining effective asset visibility and control over IT equipment items. However, as table 1 shows, we identified high failure rates in our tests for correct user organization and location of IT equipment. Because property management system inventory records were inaccurate, it is not possible to determine the timing or events associated with lost IT equipment as a basis for holding individual employees accountable.

Although our *Standards for Internal Control in the Federal Government*[16] requires timely recording of transactions as part of an effective internal control structure and safeguarding of sensitive assets, we found that VA's property management policy[17] neither specified what transactions were to be recorded for various changes in inventory status nor provided criteria for timely recording. Further, IRM and IT Services personnel responsible for installation, removal, and disposal of IT equipment did not record or assure that transactions were recorded by property management officials when these events occurred.

Errors in IT Equipment Inventory Status and Item Description Information

We found errors related to the accuracy of other information in IT equipment inventory records, including equipment status (e.g., in use, turned-in, disposal), serial numbers, model numbers, and item descriptions. As shown in table 1, estimated overall error rates for recordkeeping were lower than the error rates for the other control attributes we tested. Even so, the errors we identified affect management decision making and create waste and inefficiency in operations. Many of these errors should have been detected and corrected during annual physical inventories.

[16] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[17] VA Handbook 7127/3, *Material Management Procedures*, pt. 1, § 5002-2.3, and VA Handbook 7127/4, *Material Management Procedures*, pt. 4, § 5302.3.

Physical Inventories by Case Study Locations Identified Thousands of Missing IT Equipment Items Valued at Millions of Dollars

To assess the effect of the lax control environment for IT equipment, we asked VA officials at the case study locations covered in both our current and previous audits to provide us with information on the results of their physical inventories performed after issuance of recommendations in our July 2004 report, including Reports of Survey information on identified losses of IT equipment. As of February 28, 2007, the four case study locations covered in our current audit reported over 2,400 missing IT equipment items with a combined original acquisition value of about $6.4 million as a result of inventories they performed during fiscal years 2005 and 2006. Based on information obtained through March 2, 2007, the five case study locations we previously audited had identified over 8,600 missing IT equipment items with a combined original acquisition value of over $13.2 million, $12.4 million of which was identified at the Los Angeles medical center. Because inventory records were not consistently updated as changes in user organization or location occurred and none of the locations we audited required accountability at the user level, it is not possible to determine whether the missing IT equipment items represent recordkeeping errors or the loss, theft, or misappropriation of IT equipment. Further, missing IT equipment items were often not reported for several months and, in some cases, several years. Although physical inventories should be performed over a finite period, at most of the case study locations, these inventories were not completed for several months or even several years while officials performed extensive searches in an attempt to locate missing items before preparing Reports of Survey to write them off. According to VA Police and security specialists,[18] it is very difficult to conduct an investigation after significant amounts of time have passed because the details of the incidents cannot be determined.

The timing and scope of the physical inventories performed by the case study locations varied. For example, the Indianapolis medical center had performed annual physical inventories in accordance with VA policy for several years. The Washington, D.C., medical center performed a wall-to-wall physical inventory in response to our July 2004 report. In this case, inventory results reflected several years of activity involving IT inventory records that had not been updated and lost and missing IT equipment items that had not previously been identified and reported. In addition, the

[18] VA medical centers and other facilities have a VA Police Service, which provides law enforcement and physical security services, including security inspections and criminal investigations. The VA headquarters building does not have a police service. VA headquarters law enforcement duties are the responsibility of the Federal Protective Service.

San Diego and Houston medical centers had not followed VA policy for including sensitive items, such as IT equipment valued at less than $5,000, in their physical inventories.

Physical Security Weaknesses Increase Risk of Loss, Theft, and Misappropriation of IT Equipment and Sensitive Data

Our investigator's inspection of physical security at officially designated IT warehouses and storerooms at our four case study locations that held new and used IT equipment found that most of these storage facilities met the requirements in VA Handbook 0730/1, *Security and Law Enforcement*. However, not all of the formally designated storage locations at two medical centers had required motion detection alarm systems and special door locks. We also found numerous instances of informal IT storage areas at VA headquarters that did not meet VA physical security requirements. In addition, although VA requires that hard drives of IT equipment and medical equipment be sanitized prior to disposal to prevent unauthorized release of sensitive personal and medical information, we found weaknesses in the disposal process that pose a risk of data breach related to sensitive personal information residing on hard drives in the property disposal process that have not yet been sanitized.

Weaknesses in Procedures for Controlling Excess Computer Hard Drives

VA requires that hard drives of excess computers be sanitized prior to reuse or disposal because they can store sensitive personal and medical information used in VA programs and activities, which could be compromised and used for unauthorized purposes. For example, our limited tests of excess computer hard drives in the disposal process that had not yet been sanitized found hundreds of unique names and Social Security numbers on VA headquarters computers and detailed medical histories with Social Security numbers on computer hard drives at the San Diego medical center. Our limited tests of hard drives that were identified as having been subjected to data sanitization procedures did not find data remaining on these hard drives. However, our limited tests identified some problems that could pose a risk of data breach with regard to sensitive personal and medical information on hard drives in the disposal process that had not yet been sanitized. For example, our IT security specialist noted excessive delays—up to 6 years—in performing data sanitization once the computer systems had been identified for disposal, posing an unnecessary risk of losing the sensitive personal and medical information contained on those systems.

Physical Security Weaknesses at IT Storage Locations Pose Risk of Data Breach

VA Handbook 0730/1, *Security and Law Enforcement*, prescribes physical security requirements for storage of new and used IT equipment, requiring storerooms to have walls to ceiling height, overhead barricades that prevent "up and over" access from adjacent rooms, motion intrusion detection alarm systems, and special key control, meaning room door lock keys and day lock combinations that are not master keyed for use by others. Most of the designated IT equipment storage facilities at the four case study locations met VA IT physical security requirements; however, we identified deficiencies related to lack of intrusion detection systems at the Washington, D.C., and San Diego medical centers and inadequate door locks at the Washington, D.C., medical center. In response to our findings, these facilities initiated actions to correct these weaknesses.

We also found numerous informal, undesignated IT equipment storage locations that did not meet VA physical security requirements. For example, at the VA headquarters building, our investigator found that the physical security specialist was unaware of the existence of IT equipment in some storerooms. Consequently, these storerooms had not been subjected to required physical security inspections. Further, during our statistical tests, we observed one IT equipment storeroom in the VA headquarters building IT Support Services area that had a separate wall, but no door. The wall opening into the storeroom had yellow tape labeled "CAUTION" above the doorway. The storeroom was within an IT work area that had dropped ceilings that could provide "up and over" access from adjacent rooms, and it did not meet VA's physical security requirements for motion intrusion detection and alarms and secure doors, locks, and special access keys. In another headquarters building, we observed excess IT equipment stacked in the corners of a large work area that had multiple doors and open access to numerous individuals. We also found that VA headquarters IT coordinators used storerooms and closets with office-type door locks and locked filing cabinets in open areas to store IT equipment that was not currently in use. The failure to provide adequate security leaves the information stored on these computers vulnerable to data breach.

Status of VA Actions to Improve IT Equipment Management

Mr. Chairman, although VA strengthened existing property management policy[19] in response to recommendations in our July 2004 report, issued several new policies to establish guidance and controls for IT security, and reorganized and centralized the IT function within the department under the CIO, additional actions are needed to establish effective control in this area. For example, pursuant to recommendations made in our July 2004 report, VA updated its property management policy to clarify that IT equipment valued at under $5,000 is to be included in annual inventories. However, as noted in this testimony and described in more detail in our companion report, VA had not taken action to assure that these items were, in fact, subjected to physical inventory. In addition, the new CIO organization has no formal responsibility for medical equipment that stores or processes patient data and does not address roles or necessary coordination between IRM and property management personnel with regard to inventory control of IT equipment. The Assistant Secretary for Information and Technology, who serves as the CIO, told us that the new CIO organization structure will include a unit that will have responsibility for IT equipment asset management once it becomes operational. However, this unit has not yet been funded or staffed. To assure accountability and safeguarding of sensitive IT equipment, effective implementation will be key to the success of VA IT policy and organizational changes.

Our companion report released today made 12 recommendations to VA to strengthen accountability of IT equipment and minimize the risk of theft, loss, misappropriation, and compromise of sensitive data. These included recommendations for revising policies related to recordkeeping requirements to document essential inventory events and transactions, ensuring that physical inventories are performed in accordance with VA policy, enforcing user-level accountability for IT equipment, and strengthening physical security of IT equipment storage locations. VA management agreed with our findings and concurred with all 12 recommendations. In VA's written comments provided to us, it noted actions planned or under way to address our recommendations.

Concluding Remarks

Poor accountability and a weak control environment have left the four VA case study organizations vulnerable to continuing theft, loss, and misappropriation of IT equipment and sensitive personal data. To provide

[19] VA Handbook 7127/4, *Materiel Management Procedures* (Oct. 11, 2005).

a framework for accountability and security of IT equipment, the Secretary of Veterans Affairs needs to establish clear, sufficiently detailed mandatory agencywide policies rather than leaving the details of how policies will be implemented to the discretion of local VA organizations. Keys to safeguarding IT equipment are effective internal controls for the creation and maintenance of essential transaction records; a disciplined framework for specific, individual user-level accountability, whereby employees are held accountable for property assigned to them, including appropriate disciplinary action for any lost equipment; and maintaining adequate physical security over IT equipment items. Although VA management has taken some actions to improve inventory controls, strengthening the overall control environment and establishing and implementing specific IT equipment controls will require a renewed focus, oversight, and continuing commitment throughout the organization. We appreciate VA's positive response to our current recommendations and planned actions to address them. If effectively implemented, these actions will go a long way to assuring that the weaknesses identified in our last two audits of VA IT equipment will be effectively resolved in the near future.

Mr. Chairman and Members of the Subcommittee, this concludes my statement. I would be pleased to answer any questions that you may have at this time.

Contacts and Acknowledgments

For further information about this testimony, please contact McCoy Williams at (202) 512-9095 or williamsm1@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Major contributors to this testimony include Gayle L. Fischer, Assistant Director; Andrew O'Connell, Assistant Director and Supervisory Special Agent; Abe Dymond, Assistant General Counsel; Monica Perez Anatalio; James D. Ashley; Francine DelVecchio; Lauren S. Fassler; Dennis Fauber; Jason Kelly; Steven M. Koons; Christopher D. Morehouse; Lori B. Tanaka; Chris J. Rodriguez; Special Agent Ramon J. Rodriguez; and Danietta S. Williams. In addition, technical expertise was provided by Keith A. Rhodes, Chief Technologist, and Harold Lewis, Assistant Director, Information Technology Security, Applied Research and Methods.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation and 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER