United States Government Accountability Office

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

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, March 25, 2014

# INFORMATION SECURITY

# VA Needs to Address Long-Standing Challenges

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

GAO Highlights

Highlights of GAO-14-469T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

## Why GAO Did This Study

The use of information technology is crucial to VA's ability to carry out its mission of ensuring that veterans receive medical care, benefits, social support, and memorials. However, without adequate security protections, VA's systems and information are vulnerable to exploitation by an array of cyber-based threats, potentially resulting in, among other things, the compromise of veterans' personal information. GAO has identified information security as a government-wide high-risk area since 1997. The number of information security incidents reported by VA has more than doubled over the last several years, further highlighting the importance of securing the department's systems and the information that resides on them.

GAO was asked to provide a statement discussing the challenges VA has experienced in effectively implementing information security, as well as to comment on a recently proposed bill aimed at improving the department's efforts to secure its systems and information. In preparing this statement GAO relied on previously published work as well as a review of recent VA inspector general and other reports related to the department's security program. GAO also analyzed the draft legislation in light of existing federal requirements and best practices for information security.

View GAO-14-469T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

March 25, 2014

# INFORMATION SECURITY

## VA Needs to Address Long-Standing Challenges

## What GAO Found

The Department of Veterans Affairs (VA) continues to face long-standing challenges in effectively implementing its information security program. Specifically, from fiscal year 2007 through 2013, VA has consistently had weaknesses in key information security control areas (see table).

**Control Weaknesses for Fiscal Years 2007-2013**

| Security control category | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|---|
| Access control | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Configuration management | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Segregation of duties | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Contingency planning | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Security management | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Source: GAO analysis based on VA and inspector general reports.

In addition, in fiscal year 2013, the department's independent auditor reported, for the 12th year in a row, that weaknesses in information system controls over financial systems constituted a material weakness. Further, the department's inspector general has identified development of an effective information security program and system security controls as a major management challenge for VA. These findings are consistent with challenges GAO has identified in VA's implementation of its security program going back to the late 1990s. More recently, GAO has reported and made recommendations on issues regarding the protection of personally identifiable information at federal agencies, including VA. These were related to developing and implementing policies and procedures for responding to data breaches, and implementing protections when engaging in computerized matching of data for the purposes of determining individuals' eligibility for federal benefits.

Draft legislation being considered by the Subcommittee addresses the governance of VA's information security program and security controls for the department's systems. It would require the Secretary of VA to improve transparency and coordination of the department's security program and ensure the security of its critical network infrastructure, computers and servers, operating systems, and web applications, as well as its core veterans health information system. Toward this end, the draft legislation prescribes specific security-related actions. Many of the actions and activities specified in the bill are sound information security practices and consistent with federal guidelines. If implemented on a risk-based basis, they could prompt VA to refocus its efforts on steps needed to improve the security of its systems and information. At the same time, the constantly changing nature of technology and business practices introduces the risk that control activities that are appropriate in the department's current environment may not be appropriate in the future. In light of this, emphasizing that actions should be taken on the basis of risk may provide the flexibility needed for security practices to evolve as changing circumstances warrant and help VA meet the security objectives in the draft legislation.

Chairman Coffman, Ranking Member Kirkpatrick, and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on information security at the Department of Veterans Affairs (VA). In 1997, we first designated information security as a government-wide high-risk issue and continued to do so in the most recent update to our high-risk series.[1] Effective information security is essential to protecting the availability, confidentiality, and integrity of the information residing on federal information systems. Moreover, as we have reported since the 1990s,[2] VA has faced challenges in safeguarding personal information.

My testimony today will discuss long-standing challenges VA has experienced in effectively implementing security controls over its systems and information, as well as comment on a draft bill being considered by the Subcommittee to improve information security at VA. In preparing this testimony, we relied on our previously published work in this area, as well as an analysis of recent VA Office of Inspector General (OIG) and VA reports related to the department's information security program and data from the U.S. Computer Emergency Readiness Team (U.S.CERT) related to reported information security incidents. We also analyzed the draft bill in light of existing federal requirements and best practices for information security. All the work supporting this testimony was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

## Background

VA's mission is to promote the health, welfare, and dignity of all veterans in recognition of their service to the nation by ensuring that they receive medical care, benefits, social support, and memorials. According to VA, its employees maintain the largest integrated health care system in the nation for approximately 6 million patients, provide compensation and benefits for about 4 million veterans and beneficiaries, and maintain about

[1] GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: Feb. 14, 2013).

[2] See the list of related GAO products at the end of this statement.

3 million gravesites at 164 properties. The use of information technology (IT) is crucial to the department's ability to provide these benefits and services, but without adequate protections, VA's systems and information are vulnerable to those with malicious intentions who wish to exploit the information.

## Federal Agencies Face an Array of Cyber-Based Threats

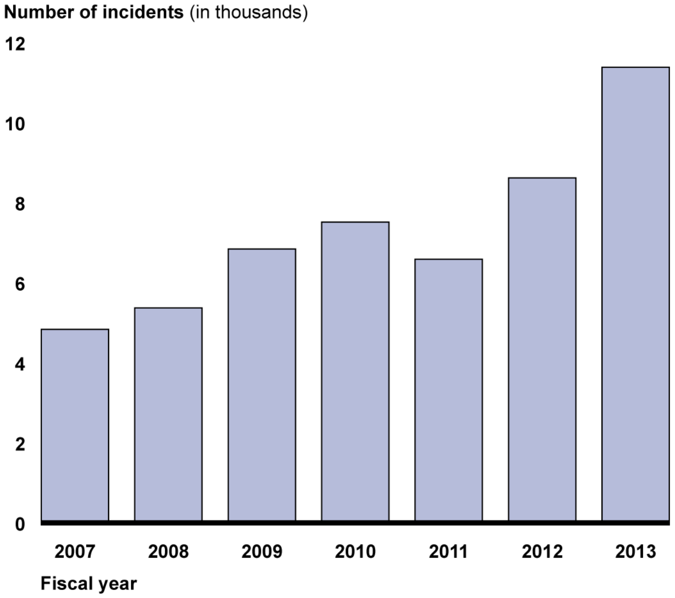
The evolving array of cyber-based threats can jeopardize the confidentiality, integrity, and availability of federal information systems and the information they contain. These threats can be unintentional or intentional. Unintentional threats can be caused by natural disasters; defective equipment; or the actions of careless, inattentive, or untrained employees that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources. These include disgruntled employees, criminal groups, hackers, and foreign nations engaged in espionage and information warfare. Such threat sources vary in terms of the types and capabilities of the actors, their willingness to act, and their motives.

These threat sources make use of various techniques to compromise information or adversely affect computers, software, networks, an organization's operation, an industry, or the Internet itself. Such techniques include, among others, denial-of-service attacks and malicious software codes or programs. The unique nature of cyber-based attacks can vastly enhance their reach and impact, resulting in the loss of sensitive information and damage to economic and national security, the loss of privacy, identity theft, and the compromise of proprietary information or intellectual property. The increasing number of incidents reported by federal agencies has further underscored the need to manage and bolster the security of the government's information systems.

## VA Has Reported an Increasing Number of Information Security Incidents

The number of incidents affecting VA's information, computer systems, and networks has generally risen over the last several years. Specifically, in fiscal year 2007, the department reported 4,834 information security incidents to US-CERT; in fiscal year 2013, it reported 11,382 incidents. These included incidents related to unauthorized access, denial-of-service attacks; installation of malicious code; improper usage of computing resources; and scans, probes, and attempted access, among others. Figure 1 shows the overall increase in the total number of incidents VA reported to US-CERT for fiscal year 2007 through 2013.

**Figure 1: VA Information Security Incidents Reported to US-CERT, Fiscal Years 2007-2013**



Source: US-CERT.

In addition, reports of incidents affecting VA's systems and information highlight the serious impact that inadequate information security can have on, among other things, the confidentiality, integrity, and availability of veterans' personal information. For example:

- According to a VA official, in January 2014 a software defect in VA's eBenefits system improperly allowed users to view the personal information of other veterans. According to this official, this defect potentially allowed almost 5,400 users to view data of over 1,300 veterans and/or their dependents.
- In May 2010, it was reported that VA officials had notified lawmakers of breaches involving the personal data of thousands of veterans, which had resulted from the theft of an unencrypted laptop computer from a VA contractor and a separate incident at a VA facility.[3]

[3] See http://www.federaltimes.com/article/20100514/CONGRESS01/5140301/.

## Federal Law and Policies Establish Information Security Responsibilities for Agencies

To help protect against threats to federal systems, the Federal Information Security Management Act of 2002 (FISMA)[4] sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The framework creates a cycle of risk management activities necessary for an effective security program. In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to agencies, the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and agency inspectors general.

Specifically, each agency is required to develop, document, and implement an agency-wide information security program and to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of its information security policies, procedures, practices, and compliance with requirements. For its part, OMB is required to develop and oversee the implementation of polices, principles, standards, and guidelines on information security in federal agencies. It is also responsible for reviewing, at least annually, and approving or disapproving agency information security programs. NIST's responsibilities include the development of security standards and guidance. Finally, inspectors general are required to evaluate annually the information security program and practices of their agency and submit the results to OMB.

Further, Congress enacted the Veterans Benefits, Health Care, and Information Technology Act of 2006[5] after a serious loss of data earlier that year revealed weaknesses in VA's handling of personal information. Under the act, VA's chief information officer is responsible for establishing, maintaining, and monitoring department-wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the department's information security program. It also reinforced the need for VA to establish and carry out the responsibilities outlined in FISMA, and included provisions to further

[4] FISMA was enacted as title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[5] Veterans Benefits, Health Care, and Information Technology Act of 2006, Pub. L. No. 109-461, 120 Stat. 3403, 3450 (Dec. 22, 2006). See also GAO, *Privacy: Lessons Learned about Data Breach Notification*, GAO-07-657 (Washington, D.C.: Apr. 30, 2007).

protect veterans and service members from the misuse of their sensitive personal information and to inform Congress regarding security incidents involving the loss of that information.

## VA Continues to Face Long-Standing Challenges in Effectively Implementing Its Information Security Program

Information security remains a long-standing challenge for the department. Specifically, VA has consistently had weaknesses in major information security control areas. For fiscal years 2007 through 2013, deficiencies were reported in each of the five major categories of information security controls as defined in our *Federal Information System Controls Audit Manual.*[6]

**Table 1: Control Weaknesses for Fiscal Years 2007 – 2013**

| Security control category | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|---|
| Access control | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Configuration management | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Segregation of duties | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Contingency planning | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Security management | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Source: GAO analysis based on VA and Inspector General reports.

*Access controls* ensure that only authorized individuals can read, alter, or delete data.

*Configuration management* controls provide assurance that only authorized software programs are implemented.

*Segregation of duties* reduces the risk that one individual can independently perform inappropriate actions without detection.

[6] GAO, *Federal Information System Controls Audit Manual (FISCAM),* GAO-09-232G (Washington, D.C.: February 2009).

*Contingency planning* includes continuity of operations, which provides for the prevention of significant disruptions of computer-dependent operations.

*Security management* includes an agency-wide information security program to provide the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

In fiscal year 2013, for the 12th year in a row, VA's independent auditor reported that inadequate information system controls over financial systems constituted a material weakness.[7] Specifically, the auditor noted that while VA had made improvements in some aspects of its security program, it continued to have control deficiencies in security management, access controls, configuration management, and contingency planning. In particular, the auditor identified significant technical weaknesses in databases, servers, and network devices that support transmitting financial and sensitive information between VA's medical centers, regional offices, and data centers. According to the auditor, this was the result of an inconsistent application of vendor patches that could jeopardize the data integrity and confidentiality of VA's financial and sensitive information.

In addition, the VA OIG reported in 2013 that development of an effective information security program and system security controls continued to be a major management challenge for the department. The OIG noted that VA had taken steps to, for example, establish a program for continuous monitoring and implement standardized security controls across the enterprise. However, the OIG continued to identify weaknesses in the department's security controls and noted that improvements were needed in key controls to prevent unauthorized access, alteration, or destruction of major applications and general support systems.

[7] See U.S. Department of Veterans Affairs, *2013 Performance and Accountability Report* (Washington, D.C.: Dec. 16, 2013). A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

These more recent findings are consistent with the challenges VA has historically faced in implementing an effective information security program. In a number of products issued beginning in 1998, we have identified wide-ranging, often recurring deficiencies in the department's information security controls.[8] These weaknesses existed, in part, because VA had not fully implemented key components of a comprehensive information security program. The persistence of similar weaknesses over 16 years later indicates the need for stronger, more focused management attention and action to ensure that VA fully implements a robust security program.

In addition, we have recently reported on issues regarding the protection of personally identifiable information (PII) at federal agencies, including VA. In December 2013, we issued a report on our review of agency practices in responding to data breaches involving PII.[9] Specifically, we determined the extent to which selected agencies had developed and implemented policies and procedures for responding to breaches involving PII.

Regarding VA, we found that the department had addressed relevant management and operational practices in its data breach response policies and procedures. In addition, it had implemented its policies and procedures by preparing breach reports and performing risk assessments for cases of data breach. However, VA had not documented the rationale for all its risk determinations, documented the number of individuals affected by breaches, consistently notified individuals affected by high-risk breaches, consistently offered credit monitoring to affected individuals, or consistently documented lessons learned from PII breaches. Accordingly, we recommended that VA take specific steps to address these weaknesses. VA agreed with some, but not all, of these recommendations. We maintained that all our recommendations were warranted.

In January 2014 we reported on selected agencies'—including VA's—compliance with amendments to the Privacy Act of 1974 that addressed

[8] See the related products page at the end of this statement for a list of relevant GAO products dealing with VA's information security.

[9] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,* GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

the computerized matching of personal information for purposes of determining eligibility for federal benefits programs.[10] Under these amendments, agencies are required to establish formal agreements with other agencies to share data for computer matching, conduct cost-benefit analyses of such agreements, and establish data integrity boards to review and report on agency computer matching activities.

Specifically regarding VA, we found that the department generally established computer matching agreements for its matching activities and conducted cost-benefit analyses of proposed matching programs. However, the completeness of these analyses varied in that they did not always include key costs and benefits needed to determine the value of a computer matching program. We noted that VA's guidance for developing cost-benefit guidance did not call for including key elements. We recommended that VA revise its guidance on cost-benefit analyses and ensure that its data integrity board review the analyses to make sure they include cost savings information. VA concurred and described steps it would take to implement our recommendations.

## Consideration of Proposed Legislation to Improve VA's Information Security

The Subcommittee is considering draft legislation that is intended to improve VA's information security. The draft bill addresses governance of the department's information security program and security controls for the department's information systems. It requires the Secretary of Veterans Affairs to improve the transparency and coordination of the information security program and to ensure the security of the department's critical network infrastructure, computers and servers, operating systems, and web applications, as well as its Veterans Health Information Systems and Technology Architecture system, from vulnerabilities that could affect the confidentiality of veterans' sensitive personal information. For each of these elements of VA's computing environment, the draft bill identifies specific security-related actions and activities that VA is required to perform.

Many of the actions and activities specified in the proposed legislation are sound information security practices and consistent with federal guidelines, if implemented on a risk-based basis. FISMA requires

[10] GAO, *Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation*, GAO-14-44 (Washington, D.C.: Jan. 13, 2014).

agencies to implement policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system. The provisions in the draft bill may prompt VA to refocus its efforts on actions that are necessary to improve the security over its information systems and information.

In a dynamic environment where innovations in technology and business practices supplant the status quo, control activities that are appropriate today may not be appropriate in the future. Emphasizing that specific security-related actions should be taken based on risk could help ensure that VA is better able to meet the objectives outlined in the draft bill. Doing this would allow for the natural evolution of security practices as circumstances warrant and may also prevent the department from focusing exclusively on performing the specified actions in the draft bill to the detriment of performing other essential security activities.

In summary, VA's history of long-standing challenges in implementing an effective information security program has continued, with the department exhibiting weaknesses in all major categories of security controls in fiscal year 2013. These challenges have been further highlighted by recent determinations that weaknesses in information security have contributed to a material weakness in VA's internal controls over financial reporting and continue to constitute a major management challenge for the department. While the draft legislation being considered by the Subcommittee may prod VA into taking needed corrective actions, emphasizing that these should be taken based on risk can provide the flexibility needed to respond to an ever-changing technology and business environment.

Chairman Coffman, Ranking Member Kirkpatrick, and Members of the Subcommittee, this concludes my statement today. I would be happy to answer any questions you may have.

## Contact and Acknowledgments

If you have any questions concerning this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov. Other individuals who made key contributions to this statement include Jeffrey L. Knott and Anjalique Lawrence (assistant directors), Jennifer R. Franks, Lee McCracken, and Tyler Mountjoy.

# Related GAO Products

*Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation.* GAO-14-44. Washington, D.C.: January 13, 2014.

*Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent.* GAO-14-34. Washington, D.C.: December 9, 2013.

*Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness.* GAO-13-776. Washington, D.C.: September 26, 2013.

*Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination.* GAO-12-8. November 29, 2011.

*Information Technology: Department of Veterans Affairs Faces Ongoing Management Challenges.* GAO-11-663T. Washington, D.C.: May 11, 2011.

*Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk.* GAO-11-43. Washington, D.C.: November 30, 2010.

*Information Security: Veterans Affairs Needs to Resolve Long-Standing Weaknesses.* GAO-10-727T. Washington, D.C.: May 19, 2010.

*Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing.* GAO-10-513. May 27, 2010.

*Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements.* GAO-10-202. Washington, D.C.: March 12, 2010.

*Veterans: Department of Veterans Affairs' Implementation of Information Security Education Assistance Program.* GAO-10-170R. Washington, D.C.: December 18, 2009.

*Department of Veterans Affairs: Improvements Needed in Corrective Action Plans to Remediate Financial Reporting Material Weaknesses.* GAO-10-65. Washington, D.C.: November 16, 2009.

*Information Security: Protecting Personally Identifiable Information.* GAO-08-343. Washington, D.C.: January 25, 2008.

*Information Security: Sustained Management Commitment and Oversight Are Vital to Resolving Long-Standing Weaknesses at the Department of Veterans Affairs.* GAO-07-1019. Washington, D.C.: September 7, 2007.

*Privacy: Lessons Learned about Data Breach Notification.* GAO-07-657. Washington, D.C.: April 30, 2007.

*Information Security: Veterans Affairs Needs to Address Long-Standing Weaknesses.* GAO-07-532T. February 28, 2007*.*

*Veterans Affairs: Leadership Needed to Address Information Security Weaknesses and Privacy Issues.* GAO-06-866T. Washington, D.C.: June 14, 2006.

*Veterans Affairs: The Critical Role of the Chief Information Officer Position in Effective Information Technology Management.* GAO-05-1017T. Washington, D.C.: September 14, 2005*.*

*Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements.* GAO-05-552. Washington, D.C.: July 15, 2005.

*Veterans Affairs: Sustained Management Attention Is Key to Achieving Information Technology Results.* GAO-02-703. Washington, D.C.: June 12, 2002.

*VA Information Technology: Progress Made, but Continued Management Attention Is Key to Achieving Results.* GAO-02-369T. Washington, D.C.: March 13, 2002.

*VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist.* GAO-01-550T. Washington, D.C.: April 4, 2001.

*VA Information Technology: Progress Continues Although Vulnerabilities Remain.* T-AIMD-00-321. Washington, D.C.: September 21, 2000.

*VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration.* AIMD-00-232. Washington, D.C.: September 8, 2000.

*Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies.* AIMD-00-295. Washington, D.C.: September 6, 2000.

*Information Technology: VA Actions Needed to Implement Critical Reforms.* AIMD-00-226. Washington, D.C.: August 16, 2000.

*Information Systems: The Status of Computer Security at the Department of Veterans Affairs.* AIMD-00-5. Washington, D.C.: October 4, 1999.

*VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls.* AIMD-99-161. Washington, D.C.: June 8, 1999.

*Major Management Challenges and Program Risks: Department of Veterans Affairs.* OCG-99-15. Washington, D.C.: January 1, 1999.

*Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure.* AIMD-98-175. Washington, D.C.: September 23, 1998.

## 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 website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

### Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

## Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

## Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.