United States Government Accountability Office

GAO

Report to the Commissioner of Internal Revenue

March 2011

INFORMATION SECURITY

IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data

GAO-11-308

March 2011

INFORMATION SECURITY

IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-308, a report to the Commissioner of Internal Revenue

Why GAO Did This Study

The Internal Revenue Service (IRS) has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. It relies extensively on computerized systems to support its financial and mission-related operations and on information security controls to protect financial and sensitive taxpayer information that resides on those systems.

As part of its audit of IRS's fiscal years 2010 and 2009 financial statements, GAO assessed whether controls over key financial and tax processing systems are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. To do this, GAO examined IRS information security policies, plans, and procedures; tested controls over key financial applications; and interviewed key agency officials at four sites.

What GAO Recommends

GAO recommends that IRS take eight actions to fully implement key components of its comprehensive information security program. In a separate report with limited distribution, GAO is recommending 32 specific actions for correcting newly identified control weaknesses. In commenting on a draft of this report, IRS agreed to develop a detailed corrective action plan to address each recommendation.

View GAO-11-308 or key components. For more information, contact Nancy R. Kingsbury at (202) 512-2700 or kingsburyn@gao.gov, or Gregory C. Wilshusen at (202)512-6244 or wilshuseng@gao.gov.

What GAO Found

Although IRS made progress in correcting previously reported information security weaknesses, control weaknesses over key financial and tax processing systems continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. Specifically, IRS did not consistently implement controls that were intended to prevent, limit, and detect unauthorized access to its financial systems and information. For example, the agency did not sufficiently (1) restrict users' access to databases to only the access needed to perform their jobs; (2) secure the system it uses to support and manage its computer access request, approval, and review processes; (3) update database software residing on servers that support its general ledger system; and (4) enable certain auditing features on databases supporting several key systems. In addition, 65 of 88—about 74 percent—of previously reported weaknesses remain unresolved or unmitigated.

An underlying reason for these weaknesses is that IRS has not yet fully implemented key components of its comprehensive information security program. Although IRS has processes in place intended to monitor and assess its internal controls, these processes were not always effective. For example, IRS's testing did not detect many of the vulnerabilities GAO identified during this audit and did not assess a key application in its current environment. Further, the agency had not effectively validated corrective actions reported to resolve previously identified weaknesses. Although IRS had a process in place for verifying whether each weakness had been corrected, this process was not always working as intended. For example, the agency reported that it had resolved 39 of the 88 previously identified weaknesses; however, 16 of the 39 weaknesses had not been mitigated.

IRS has various initiatives underway to bolster security over its networks and systems; however, until the agency corrects the identified weaknesses, its financial systems and information remain unnecessarily vulnerable to insider threats, including errors or mistakes and fraudulent or malevolent acts by insiders. As a result, financial and taxpayer information are at increased risk of unauthorized disclosure, modification, or destruction; financial data is at increased risk of errors that result in misstatement; and the agency's management decisions may be based on unreliable or inaccurate financial information. These weaknesses, considered collectively, are the basis for GAO's determination that IRS had a material weakness in internal control over financial reporting related to information security in fiscal year 2010.

Contents

Abbreviations

FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
TIGTA	Treasury Inspector General for Tax Administration

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 15, 2011

The Honorable Douglas H. Shulman
Commissioner of Internal Revenue

Dear Commissioner Shulman:

The Internal Revenue Service (IRS) has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. It relies extensively on computerized systems to support its financial and mission-related operations and on information security controls[1] to protect the confidentiality, integrity, and availability of the financial and sensitive taxpayer information that resides on those systems.

As part of our audit of IRS's fiscal years 2010 and 2009 financial statements,[2] we assessed the effectiveness of the agency's information security controls over its key financial and tax processing systems, information, and interconnected networks at four locations. These systems support the processing, storage, and transmission of financial and sensitive taxpayer information. In our report on IRS's fiscal years 2010 and 2009 financial statements, we reported that IRS could not rely on the internal controls[3] contained in its automated financial management system to provide reasonable assurance that (1) its financial statements, taken as a whole, were fairly stated; (2) the information IRS relied on to make decisions on a daily basis was accurate, complete, and timely; and (3) proprietary financial and taxpayer information was appropriately safeguarded. We concluded that the new information security weaknesses we identified in fiscal year 2010 and the unresolved weaknesses from prior

[1]Information security controls include logical and physical access controls, configuration management, segregation of duties, and continuity of operations. These controls are designed to ensure that access to data is appropriately restricted, physical access to sensitive computing resources and facilities is protected, only authorized changes to computer programs are made, incompatible duties are segregated among individuals, and back-up and recovery plans are adequate and tested to ensure the continuity of essential operations.

[2]GAO, *Financial Audit: IRS's Fiscal Years 2010 and 2009 Financial Statements*, GAO-11-142 (Washington, D.C.: Nov. 10, 2010).

[3]Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations, and management's system for measuring, reporting, and monitoring program performance.

audits, considered collectively, represent a material weakness[4] in internal control over financial reporting related to information security.

Our objective was to determine whether IRS's controls over key financial and tax processing systems are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. To do this, we examined IRS information security policies, plans, and procedures; tested controls over key financial applications; interviewed key agency officials; and reviewed our prior reports to identify previously reported weaknesses and assessed the effectiveness of corrective actions taken. We concentrated our evaluation on threats emanating from sources internal to IRS's computer networks.

We conducted this audit from May 2010 to March 2011 in accordance with U.S. generally accepted government auditing standards. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. For additional information about our objective, scope, and methodology, refer to appendix I.

Background

The use of information technology has created many benefits for agencies such as IRS in achieving their missions and providing information and services to the public, but extensive reliance on computerized information also creates challenges in securing that information from various threats. Information security is especially important for government agencies, where maintaining the public's trust is essential.

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The risk to these systems are well-founded for a number of reasons, including the increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. The Federal Bureau of Investigation has identified multiple sources of threats, including foreign entities engaged in intelligence gathering and information warfare,

[4]A material weakness is a deficiency, or a combination of deficiencies, in internal controls 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.

domestic criminals, hackers, virus writers, and disgruntled employees or contractors working within an organization. In addition, the U.S. Secret Service and the CERT® Coordination Center[5] studied insider threats in the government sector and stated in a January 2008 report[6] that "government sector insiders have the potential to pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases." Insider threats include errors or mistakes and fraudulent or malevolent acts by insiders.

Our previous reports, and those by federal inspectors general, describe persistent information security weaknesses that place federal agencies, including IRS, at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, we have designated information security as a governmentwide high-risk area since 1997, most recently in 2011.[7]

Information security is essential to creating and maintaining effective internal controls. The Federal Managers' Financial Integrity Act of 1982 requires us to issue standards for internal control in federal agencies.[8] The standards[9] provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance and management challenges and areas at greatest risk of fraud, waste, abuse, and mismanagement. The term internal control is synonymous with the term management control, which covers all aspects of an agency's operations (programmatic, financial, and compliance). The attitude and philosophy of management toward information systems can have a profound effect on internal control. Information system controls consist of those internal controls that are dependent on information systems

[5]The CERT® Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

[6]U.S. Secret Service and Computer Emergency Response Team, *Insider Threat Study: Illicit Cyber Activity in the Government Sector* (Washington, D.C., and Pittsburgh, Pa.: January 2008).

[7]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[8]See 31 U.S.C. § 3511.

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

processing and include general controls at the entitywide, system, and business process application levels (security management, access controls, configuration management, segregation of duties, and contingency planning); business process application controls (input, processing, output, master file, interface, and data management system controls); and user controls (controls performed by people interacting with information systems).

Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA)[10] in December 2002 to strengthen the security of information and systems within federal agencies. FISMA requires each agency to develop, document, and implement an agencywide information security program for the information and information systems that support the operations and assets of the agency, using a risk-based approach to information security management. Such a program includes assessing risk; developing and implementing cost-effective security plans, policies, and procedures; providing specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; and ensuring continuity of operations.

IRS Is the Tax Collector for the United States

IRS has demanding responsibilities in collecting taxes, processing tax returns, and enforcing federal tax laws, and relies extensively on computerized systems to support its financial and mission-related operations. In fiscal year 2010, IRS processed hundreds of millions of tax returns, collected about $2.3 trillion in federal tax payments, and paid about $467 billion in refunds to taxpayers. Further, the size and complexity of IRS add unique operational challenges. IRS employs over 100,000 people in its Washington, D.C., headquarters and over 700 offices in all 50 states and U.S. territories and in some U.S. embassies and consulates. To manage its data and information, the agency operates three enterprise computing centers located in Detroit, Michigan; Martinsburg, West Virginia; and Memphis, Tennessee. IRS also collects and maintains a significant amount of personal and financial information on each American taxpayer. Protecting the confidentiality of this sensitive information is paramount; otherwise, taxpayers could be exposed to loss

[10]FISMA was enacted as title III, E-Government Act of 2002, Pub L. No. 107-347, Dec. 17, 2002.

of privacy and to financial loss and damages resulting from identity theft or other financial crimes.

The Commissioner of Internal Revenue has overall responsibility for ensuring the confidentiality, integrity, and availability of the information and information systems that support the agency and its operations. FISMA requires the Chief Information Officer (CIO) or comparable official at federal agencies to be responsible for developing and maintaining an information security program. IRS has delegated this responsibility to the Associate Chief Information Officer for Cybersecurity, who heads the Office of Cybersecurity. The Office of Cybersecurity's mission is to protect taxpayer information and the IRS's electronic system, services, and data from internal and external cyber security-related threats by implementing security practices in planning, implementation, risk management, and operations. IRS develops and publishes its information security policies, guidelines, standards, and procedures in the *Internal Revenue Manual* and other documents in order for IRS divisions and offices to carry out their respective responsibilities in information security. In October 2010, the Treasury Inspector General for Tax Administration (TIGTA) stated that security, including computer security, was the top priority in its list of top 10 management challenges for IRS in fiscal year 2011.[11]

Significant Weaknesses Continue to Place Financial and Taxpayer Information at Risk

Although IRS has made progress in correcting information security weaknesses that we have reported previously, many weaknesses have not been corrected and we identified many new weaknesses during fiscal year 2010. Specifically, 65 out of 88 previously reported weaknesses[12]—about 74 percent—have not yet been corrected. In addition, we identified 37[13] new weaknesses. These weaknesses relate to access controls, configuration management, and segregation of duties. Weaknesses in these areas increase the likelihood of errors in financial data that result in misstatement and expose sensitive information and systems to unauthorized use, disclosure, modification, and loss. An underlying reason for these weaknesses—both old and new—is that IRS has not yet fully

[11]TIGTA, *Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2011* (Washington, D.C.: October 2010).

[12]In a separate report with limited distribution, we provide the status of each of the 88 previously reported weaknesses.

[13]This number includes 29 specific technical weaknesses and 8 weaknesses associated with IRS's comprehensive information security program.

implemented key components of a comprehensive information security program. These weaknesses continue to jeopardize the confidentiality, integrity, and availability of the financial and sensitive taxpayer information processed by IRS's systems and, considered collectively, are the basis of our determination that IRS had a material weakness in internal control over its financial reporting related to information security in fiscal year 2010.[14]

IRS Did Not Sufficiently Control Access to Information Resources

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Access controls include those related to user identification and authentication, authorization, cryptography, audit and monitoring, and physical security. However, IRS did not fully implement effective controls in these areas. Without adequate access controls, unauthorized individuals may be able to login, access sensitive information, and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized individuals may be able to intentionally or unintentionally add, modify, or delete data to which they should not have been given access.

Controls Were Not Consistently Implemented for Identifying and Authenticating Users

A computer system needs to be able to identify and authenticate each user so that activities on the system can be linked and traced to a specific individual. An organization does this by assigning a unique user account to each user, and in so doing, the system is able to distinguish one user from another—a process called identification. The system also needs to establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. The combination of identification and authentication—such as user account/password combinations—provides the basis for establishing individual accountability and for controlling access to the system. The *Internal Revenue Manual* requires the use of a strong password for authentication (defined as a minimum of eight characters, containing at least one numeric or special character, and a mixture of at least one uppercase and one lower case letter). Furthermore, the *Internal Revenue Manual* states that database account passwords are

[14]GAO-11-142.

not to be reused within 10 password changes[15] and that the password grace time for a database—the number of days an individual has to change his or her password after it expires—should be set to 10.

IRS properly configured password complexity on its servers used to manage access to network resources. In addition, IRS made progress in correcting a previously identified weakness by restricting remote login access. However, IRS did not consistently implement strong authentication controls on certain systems, as required by the *Internal Revenue Manual*. For example:

- Databases that support IRS administrative accounting and procurement systems had a certain password control set to "null." This password control verifies certain password settings, such as password complexity and minimum password length, to ensure the user's password complies with IRS policy. By configuring this control to "null," no password verifications are performed.
- Seventeen of 90 network devices[16] we reviewed had a password length of 6 characters.
- Databases that support the IRS's administrative accounting and procurement systems contained several password resource values that were not set to the settings required by IRS policy. For example, the password reuse and password grace time values were set to "unlimited."

As a result of these weaknesses, increased risk exists that an individual with malicious intentions could gain inappropriate access to these sensitive IRS applications and data, and potentially use the access to attempt compromises of other IRS systems.

Users Have More System Access than Needed to Perform Their Jobs

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying an individual access rights is the concept of "least privilege." Least privilege, which is a basic principle for securing computer resources and information, means that a user is granted only those access rights and permissions needed to perform official duties. To restrict legitimate users'

[15]As noted later in this report, IRS policy regarding this password control is inconsistent.

[16]Network devices include routers, switches, and firewalls.

access to only those programs and files needed to do their work, organizations establish access rights and permissions to users. These "user rights" are allowable actions that can be assigned to one user or to a group of users. File and directory permissions are rules that regulate which users can access a particular file or directory and the extent of that access. To avoid unintentionally authorizing a user access to sensitive files and directories, an organization should give careful consideration to its assignment of rights and permissions. IRS policy states that access control measures based on least privilege and that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information should be implemented. Additionally, the *Internal Revenue Manual* requires that the guest account be disabled to prevent any user from being authenticated as a guest.

Although IRS had taken steps to control access to systems, it continued to permit excessive access. For example, IRS had corrected a previously identified weakness by limiting access to certain key financial documents used for input into the administrative accounting system. However, it continued to permit excessive access to several systems by granting rights and permissions that gave users more access than they needed to perform their assigned functions. For example, IRS granted excessive privileges to a database account on the online system used to support and manage its computer access request, approval, and review process. In addition, the agency allowed some individuals to manually enter commands that would permit them to bypass the application programs intended to be used to access the data. Also, all database users had unnecessary execute permissions on several sensitive database packages[17] that allowed them to manipulate data and gain access to sensitive files and directories on IRS's access authorization, administrative accounting, electronic tax payment, and procurement systems. Furthermore, while IRS made progress in correcting a previously identified weakness by disabling the guest account on some SQL servers, IRS had not disabled the SQL server guest account on its real property management system, increasing the risk that unauthorized users could use this account to gain system access. These excessive access privileges can provide opportunities for individuals to circumvent security controls.

[17]According to Oracle, a package is an encapsulated collection of related program objects stored together in the database. Program objects are procedures, functions, variables, constants, cursors, and exceptions.

Sensitive Data Is Sent across the IRS Network Unencrypted

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption, which is used to transform plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. According to IRS policy, the use of insecure protocols should be restricted because its widespread use can allow passwords and other sensitive data to be transmitted across its internal network unencrypted.

Although IRS discontinued the use of unencrypted protocols on the servers supporting the procurement system, its network devices were configured to use protocols that allowed unencrypted transmission of sensitive data. For example, 37 of the 90 network devices we reviewed and a server supporting the IRS's tax payment system used unencrypted protocols to transmit sensitive information. In addition, IRS had not corrected previously identified weaknesses, such as weak encryption controls over user login to its administrative accounting system and transmission of unencrypted mainframe administrator login information across its network. By not encrypting sensitive data, IRS is at increased risk that an unauthorized individual could view and then use the data to gain unwarranted access to its system and/or sensitive information.

IRS Did Not Consistently Audit and Monitor Security-Relevant Activity on Certain Systems

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail—a log of system activity—that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security-relevant events. The *Internal Revenue Manual* states that IRS should enable and configure audit logging on all systems to aid in the detection of security violations, performance problems, and flaws in applications. Additionally, IRS policy states that security controls in information systems shall be monitored on an ongoing basis.

IRS is currently utilizing a commercial off-the-shelf audit trail solution allowing the agency to review audit log reports and analyze audit data. In addition, IRS has established the Enterprise Security Audit Trails Project Management Office, which is responsible for managing all enterprise audit

initiatives and identifying and overseeing deployment and transition of various audit trail solutions. Despite these steps forward, IRS did not enable certain auditing features on three systems we reviewed. For example, IRS did not enable security event auditing[18] or system privilege auditing[19] features on databases that support its access authorization, administrative accounting, and procurement systems. In addition, IRS had not corrected a previously identified weakness in which certain servers were not configured to ensure sufficient audit trails. As a result, IRS's ability to establish individual accountability, monitor compliance with security policies, and investigate security violations was limited.

Physical Access Controls Were Not Consistently Implemented

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms in which they are housed and periodically reviewing access granted, in order to ensure that access continues to be appropriate. At IRS, physical access control measures, such as physical access cards that are used to permit or deny access to certain areas of a facility, are vital to safeguarding its facilities, computing resources, and information from internal and external threats. The *Internal Revenue Manual* requires access controls to protect employees and contractors, information systems, and the facilities in which they are located. The policy also requires that entry to restricted areas should be limited to only those who need it to perform their job duties. It also requires department managers of restricted areas to review, validate, sign, and date the authorized access list for restricted areas on a monthly basis and then forward the list to the physical security office for review of employee access.

Although IRS had implemented numerous physical security controls, certain controls were not working as intended, and the agency had not consistently applied the policy in others. IRS has a dedicated guard force at each computing center visitor entrance. These guards screen every visitor that enters these facilities. The agency had also corrected a previously identified weakness by consistently reviewing the images displayed on x-ray machines while screening employees, visitors, and

[18]Security event auditing is used to log authentication events.

[19]System privilege auditing logs the use of powerful system privileges that enable corresponding actions. Privilege auditing can be set to log a selected user or every user in the database.

contractors entering restricted areas. However, visitor physical access cards to restricted areas at one computing center provided unauthorized access to other restricted areas within the center—a weakness previously reported in 2010. In addition, IRS had not consistently applied its processes for reviewing access to restricted areas within its computing centers. For example, effective procedures were not in place at two of the three computing centers to ensure that individuals with an ongoing need to access restricted areas within the center were reviewed regularly in order to assess whether the access was warranted to perform their job. Although one computing center regularly reviewed the visitor access list, it did not review the list of individuals who had ongoing access. The other center only reviewed access based on the number of times in a given week the individual entered certain areas within the center, rather than based on the individual's need to perform job duties. Further, at the third data center, IRS was unable to provide evidence that the physical security office had addressed a prior recommendation to remove employee access to restricted areas when a manager indicated access was no longer needed.

Because employees and visitors may have unnecessary access to restricted areas, IRS has reduced assurance that its computing resources and sensitive information are adequately protected from unauthorized access.

Weaknesses in Other Information Security Controls Increase Risk

In addition to access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an organization's information. These controls include policies, procedures, and techniques for securely configuring information systems, and segregating incompatible duties. However, IRS has weaknesses in these areas, thus increasing its risk of unauthorized use, disclosure, modification, or loss of information and information systems.

Outdated and Unsupported Software Exposes IRS to Known Vulnerabilities

Configuration management involves, among other things, (1) verifying the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) obtaining reasonable assurance that systems are configured and operating securely and as intended. Patch management, a component of configuration management, is an important element in mitigating the risks associated with software vulnerabilities. When a software vulnerability is discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. Without the patch, an attacker can exploit a software vulnerability to read, modify, or delete sensitive information; disrupt

operations; or launch attacks against systems at another organization. Outdated and unsupported software is more vulnerable to an attack and exploitation because vendors no longer provide updates, including security updates. Accordingly, the *Internal Revenue Manual* states that IRS will manage systems to reduce vulnerabilities by promptly installing patches. In addition, the manual states that system administrators will ensure the operating system version is a version for which the vendor still offers standardized technical support.

Although IRS made progress in updating certain systems, it did not always apply critical patches to its databases that support two financial applications. For example, the agency made major upgrades to key servers supporting the administrative accounting system; however, databases supporting this and another administrative accounting application had not been updated with the latest critical patches. In addition, patches had not been applied since 2006 for at least four other database installations on servers supporting the agency's general ledger system for tax-related activities. IRS had also not corrected previously identified weaknesses related to outdated and unsupported software on domain name servers. As a result, the agency has limited assurance that its systems are protected from known vulnerabilities.

Incompatible Duties Were Not Appropriately Segregated on Certain Financial Management Systems

Segregation of duties refers to the policies, procedures, and organizational structures that help ensure that no single individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often, organizations achieve segregation of duties by dividing responsibilities among two or more individuals or organizational groups. This diminishes the likelihood that errors and wrongful acts will go undetected, because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. The *Internal Revenue Manual* requires that IRS divide and separate duties and responsibilities of incompatible functions among different individuals so that no individual shall have all of the necessary authority and system access to disrupt or corrupt a critical security process. Furthermore, the manual specifies that the primary security role of any database administrator is to administer and maintain database repositories for proper use by authorized individuals and that database administrators shall not have system administrator access rights.

IRS did not always appropriately segregate certain duties. Specifically, on its general ledger system for tax-related activities, IRS granted certain database administration privileges to at least 25 database users with no database administration duties. These privileges allowed them to grant other users access to tables within the database, including the ability to add, change, or delete important accounting data. In addition, IRS had not corrected a previously identified weakness related to permitting an individual the ability to execute the roles and responsibilities of both a database and system administrator for the procurement system. By not properly segregating incompatible duties in these financial management systems, IRS reduces the effectiveness of its internal controls over financial management and increases the likelihood of errors and misstatements. Additionally, these weaknesses increase the potential for unauthorized use or disclosure of sensitive information or disruption of systems.

IRS Has Not Fully Implemented Key Components of Its Information Security Program

An underlying reason for the information security weaknesses in IRS's financial and tax processing systems is that it has not yet fully implemented key components of its comprehensive information security program. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems;
- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency

depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;

- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security policies, procedures, or practices; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

IRS has made progress in developing and documenting elements of its information security program. To bolster security over its networks and systems and to address its information security weaknesses, IRS has developed various initiatives. For example, IRS has created a detailed roadmap to guide its efforts in targeting critical weaknesses. The agency is in the process of implementing this comprehensive plan to mitigate numerous information security weaknesses, such as those associated with access controls, audit trails, contingency planning, and training. According to the plan, the last of these weaknesses is scheduled to be resolved in the first quarter of fiscal year 2014. In addition, IRS has developed metrics to measure success in complying with guides, policies, and standards in the areas of inventory management, configuration management, access authorizations, auditing, and change management. As long as these efforts remain flexible to address changing technology and evolving threats, include our findings and those of TIGTA in measuring success, and are fully and effectively implemented, they should improve the agency's overall information security posture.

Although the agency has a framework in place for its comprehensive information security program, as demonstrated below, key components of IRS's program have not yet been fully implemented.

Although IRS Had Documented Risk Assessments, One Had Not Been Updated and Another Was Not Comprehensive

According to the National Institute of Standards and Technology (NIST), risk is determined by identifying potential threats to the organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data. Identifying and assessing information security risks are essential to determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that the policies and controls operate as intended. Consistent with NIST guidance,

IRS requires its risk assessment process to detail the residual risk[20] assessed, as well as potential threats, and to recommend corrective actions for reducing or eliminating the vulnerabilities identified. IRS policy also requires system risk assessments to be updated a minimum of every 3 years or whenever there is a significant change to the system, the facilities where the system resides, or other conditions that may affect the security or status of system accreditation.

Although IRS had implemented a risk assessment process, which includes, among other things, threat and vulnerability identification, impact analysis, risk determination, and recommended corrective actions, certain risks may not have been identified. For the six systems that we reviewed, five of the risk assessments were up-to-date, documented, and formally approved by IRS management. However, IRS's general ledger system for tax-related activities was moved from one mainframe environment to another at a different facility; yet, the risk assessment had not been updated. Further, IRS's risk assessment of the mainframe environment supporting its general ledger for tax-related activities and tax processing applications was not comprehensive. Specifically, the assessment did not consider all potential threats and vulnerabilities for portions of the system; IRS considered the test and development environment of the system as out of scope although these portions could affect the system's security. As a result, potential risks to this system may not be fully known and associated controls may not be in place.

Policies and Procedures Were in Place, but Some Were Inconsistent and Others Lacked Specificity

Another key element of an effective information security program is to develop, document, and implement risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. If properly developed and implemented, policies and procedures should help reduce the risk associated with unauthorized access or disruption of services. In addition, technical security standards can provide consistent implementation guidance for each computing environment. Developing, documenting, and implementing security policies and standards are the important primary mechanisms by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls. In addition, agencies need to take the actions necessary to effectively implement or execute these procedures and controls. Otherwise, agency

[20]Residual risk is the risk remaining after the implementation of new or enhanced controls.

systems and information will not receive the protection that the security policies and controls should provide.

IRS had generally developed, documented, and approved information security policies and procedures, and had corrected a previously identified weakness by enhancing its policies and procedures related to password age and configuration settings to comply with federal guidance. However, some policies were inconsistent and some were lacking specifics about administering, managing, and monitoring certain controls. For example, the agency's overall policy on password management requires that systems be configured such that passwords cannot be reused within 24 password changes; another policy specified 3 in one section and 10 in another. Inconsistent policies can lead to less stringent implementation of controls, such as those for password management. In addition, specific policy and procedures for a key access control were lacking. Although IRS relies on system-managed storage[21] as a key access control to prevent unauthorized access between logical partitions[22] that have different mission support functions and different security requirements, the agency did not document in its policy or related procedures how this control environment should be administered, managed, and monitored. As a result, IRS does not have processes in place to verify that system-managed storage controls are implemented, administered, and monitored in a manner that provides necessary access controls. Further, in an August 2010 report,[23] TIGTA reported that IRS had not documented all IT security roles and responsibilities in the *Internal Revenue Manual* and had not developed day-to-day IT security procedures and guidelines. Without having fully documented, approved, and implemented policies and procedures, IRS cannot ensure that its information security requirements are applied consistently across the agency.

[21]According to IBM, system-managed storage allows the operating system to take over many storage management tasks that had previously been performed manually.

[22]According to IBM, logical partitioning provides users the ability to divide a single server into several independent systems. Each partition is capable of running one or more applications in an independent environment with its own set of operational attributes.

[23]TIGTA, *More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness*, 2010-20-084 (Washington, D.C.: Aug. 26, 2010).

Security Plans Were Documented, but One Plan Did Not Describe Controls in the Current Environment

An objective of system security planning is to improve the protection of information technology resources. A system security plan provides an overview of the system's security requirements and describes the controls that are in place or planned to meet those requirements. OMB Circular A-130 requires that agencies develop system security plans for major applications and general support systems, and that these plans address policies and procedures for providing management, operational, and technical controls. Furthermore, IRS policy requires that security plans describing the security controls in place or planned for its information systems be developed, documented, implemented, reviewed annually, and updated a minimum of every 3 years or whenever there is a significant change to the system.

Although IRS documented its management, operational, and technical controls in system security plans for the six systems we reviewed, one plan did not reflect the current operating environment. IRS used OMB Circular A-130 as guidance to develop system security plans for the respective systems. In addition, IRS documented the review of its system security plans through certification and accreditation memos, which provide IRS with the authorization to operate systems. These memos were formally approved by key officials. Further, all the plans reviewed were within the 3-year time frame. However, one application's system security plan did not describe controls in place in the current environment. IRS had moved this application from one mainframe to another, but the plan still reflected controls from the previous environment. Without a specific and accurate security plan for this key financial system, IRS cannot ensure that appropriate controls are in place to protect the critical information this system stores.

Security Awareness and Specialized Training Was Provided to All Employees Reviewed

Individuals can be one of the weakest links in securing systems and networks. Therefore, a very important component of an information security program is providing sufficient training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks. IRS policy requires that personnel performing information technology security duties meet minimum continuing professional education hours in accordance with their roles. Individuals performing security roles are required by IRS to have 12, 8, or 4 hours of specialized training per year, depending on their specific role.

IRS had processes in place for providing employees with security awareness and specialized training. For the employees with specific security-related roles and the newly-hired employees that we reviewed, all

met the required minimum security awareness and specialized training hours.

Tests and Evaluations of Policies, Procedures, and Controls Were Not Always Effective

Another key element of an information security program is to test and evaluate policies, procedures, and controls to determine whether they are effective and operating as intended. This type of oversight is a fundamental element because it demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results improve the security program. FISMA requires that the frequency of tests and evaluations be based on risks and occur no less than annually. The *Internal Revenue Manual* also requires periodic testing and evaluation of the effectiveness of information security policies and procedures.

Although IRS has processes in place intended to monitor, test, and evaluate its security policies and procedures, these processes were not always effective. For example, IRS did not:

- Detect many of the readily identifiable vulnerabilities we are reporting. We previously recommended that IRS expand the scope for testing and evaluating controls to ensure more comprehensive testing.
- Perform comprehensive testing within the past year for one of its key network components that it considered to be a high-risk system.
- Test application security over its general ledger system for tax-related activities in its current production environment. This general ledger system was moved from one mainframe environment to another at a different facility; yet, the test and evaluation had not been updated to reflect the current operating environment. We tested access controls in the current environment and identified weaknesses in the general ledger system's controls that compromised segregation of duties and jeopardized the integrity of the application's data.
- Comprehensively test security controls over the mainframe environment supporting its general ledger for tax-related activities and tax processing applications. For example, the test was limited to a portion of the operating environment and, therefore, did not test all of the relevant controls.

In addition, in an August 2010 report,[24] TIGTA reported that IRS did not properly conduct compliance assessments to test the implementation of day-to-day IT procedures. Because of the lack of comprehensive testing, IRS may not be fully aware of vulnerabilities that could adversely affect critical applications and data.

Remedial Action Plans Were Complete, but Corrective Actions Were Not Fully Validated

A remedial action plan is a key component of an agency's information security program as described in FISMA. Such a plan assists agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses that are found in information systems. In its annual FISMA guidance to agencies, OMB requires agency remedial action plans, also known as plans of action and milestones, to include the resources necessary to correct identified weaknesses. According to the *Internal Revenue Manual*, the agency should document weaknesses found during security assessments, as well as planned, implemented, and evaluated remedial actions to correct any deficiencies. IRS policy further requires that IRS track the resolution status of all weaknesses and verify that each weakness is corrected.

IRS had a process in place for evaluating and tracking remedial actions. The agency developed remedial action plans for the systems that we reviewed and implemented a remedial action process to address deficiencies in its information security policies, procedures, and practices. These plans documented weaknesses and included planned actions that were tracked by IRS. In addition, during fiscal year 2010, IRS made progress toward correcting previously reported information security weaknesses, correcting or mitigating 23 of the 88 previously identified weaknesses that were unresolved at the end of our prior audit.[25] However, at the time of our review, 65 of 88—about 74 percent—of the previously reported weaknesses remained unresolved or unmitigated. According to IRS officials, the agency is continuing actions toward correcting or mitigating previously reported weaknesses.

However, the agency's process for verifying whether an action had corrected or mitigated the weakness was not working as intended. The

[24]TIGTA, 2010-20-084.

[25]GAO, *Information Security: IRS Needs to Continue to Address Significant Weaknesses*, GAO-10-355 (Washington, D.C.: Mar. 19, 2010) and *Information Security: Significant Weaknesses at IRS Continue to Jeopardize Financial and Taxpayer Data*, GAO-10-300SU (Washington, D.C.: Mar. 19, 2010).

agency informed us that it had corrected 39 of the 88 previously reported weaknesses, but we determined that IRS had not fully implemented the remedial actions for 16 of the 39 weaknesses that it considered corrected. We previously recommended that IRS implement a revised verification process that ensures remedial actions are fully implemented. Until the agency takes additional steps to implement a more effective verification process, it will have limited assurance that weaknesses are being properly mitigated or corrected and that controls are operating effectively.

IRS Documented Contingency Plans for Major Systems and Made Efforts to Mitigate Previous Weaknesses

Continuity of operations planning, which includes contingency planning, is critical to protecting sensitive information. To ensure that mission-critical operations continue, organizations should be able to detect, mitigate, and recover from service disruptions while preserving access to vital information. Organizations should prepare plans that are clearly documented, communicated to staff who could be affected, and updated to reflect current operations. In addition, testing contingency plans is essential in determining whether the plans will function as intended in an emergency situation. FISMA requires that plans and procedures be in place to ensure continuity of operations for agency information systems. IRS policy states that individuals with responsibility for disaster recovery should be provided with copies of or access to agency disaster recovery plans.

IRS had appropriately documented and communicated the four contingency plans we reviewed. In addition, IRS had resolved prior weaknesses by updating disaster recovery and business resumption plans to include UNIX and Windows mission-critical systems and ensuring the availability of a disaster recovery keystroke manual for its administrative accounting system.

Conclusions

Although IRS continues to make progress in correcting or mitigating previously reported weaknesses, implementing controls over key financial systems, and developing and documenting a framework for its comprehensive information security program, information security weaknesses—both old and new—continue to jeopardize the confidentiality, integrity, and availability of IRS's systems. An underlying reason for the information security weaknesses in IRS's financial and tax processing systems is that it has not yet fully implemented key components of its comprehensive information security program. The financial and taxpayer information on IRS systems will remain particularly vulnerable to insider threats until the agency (1) addresses newly identified and previously reported weaknesses pertaining to identification

and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, and segregation of duties; and (2) fully implements key components of a comprehensive information security program that ensures risk assessments are conducted in the current operating environment; policies and procedures are appropriately specific and effectively implemented; security plans are written to reflect the current operating environment; processes intended to test, monitor, and evaluate internal controls are appropriately detecting vulnerabilities; comprehensive testing is conducted on key networks on an at least annual basis; and tests and evaluations are conducted in the current operating environment.

Until IRS takes these further steps, financial and taxpayer information are at increased risk of unauthorized disclosure, modification, or destruction; financial data is at increased risk of errors that result in misstatement; and the agency's management decisions may be based on unreliable or inaccurate financial information. These weaknesses, considered collectively, were the basis of our determination that IRS had a material weakness in internal control over financial reporting related to information security in fiscal year 2010.

Recommendations for Executive Action

In addition to implementing our previous recommendations, we are recommending that the Commissioner of Internal Revenue take the following eight actions to fully implement key components of the IRS comprehensive information security program:

- Update risk assessments whenever there is a significant change to the system, the facilities where the system resides, or other conditions that may affect the security or status of system accreditation.
- Update the risk assessment for the mainframe environment supporting the general ledger for tax-related activities and tax processing applications to include all portions of the environment that could affect security.
- Update policies and procedures pertaining to password controls to ensure they are consistent.
- Document and implement policy and procedures for how systems-managed storage as an access control mechanism should be administered, managed, and monitored.

- Update the application security plan to describe controls in place in its current mainframe operating environment.
- Perform comprehensive testing of the key network component considered to be a high-risk system, at least annually.
- Test the application security for the general ledger system for tax-related activities in its current operating environment.
- Perform comprehensive testing of security controls over the mainframe environment to include all portions of the operating environment.

We are also making 32 detailed recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct specific information security weaknesses related to identification and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, and segregation of duties identified during this audit.

Agency Comments

In providing written comments (reprinted in app. II) on a draft of this report, the Commissioner of Internal Revenue stated that the security and privacy of taxpayer and financial information is of the utmost importance to the agency and that he appreciated that the draft report recognized the progress IRS has made in improving its information security program and that numerous initiatives are underway. He also noted that IRS is committed to securing its computer environment and will continually evaluate processes, promote user awareness, and apply innovative ideas to increase compliance. The Commissioner stated that IRS is steadily progressing toward eliminating the material weakness in information security by establishing enterprise repeatable processes, which are overseen by an internal team that performs self-inspections, identifies and mitigates risk, and provides executive governance over corrective actions. Further, he stated that IRS will provide a detailed corrective action plan addressing each of our recommendations.

This report contains recommendations to you. As you know, 31 U.S.C. § 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform not later than 60 days from the date of the report and to the House and Senate Committees on Appropriations

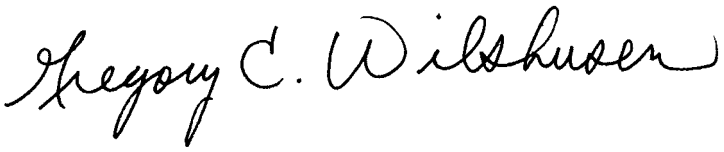
with the agency's first request for appropriations made more than 60 days after the date of this report. Because agency personnel serve as the primary source of information on the status of recommendations, we request that the agency also provide us with a copy of the agency's statement of action to serve as preliminary information on the status of open recommendations.

We are sending copies of this report to interested congressional committees, the Secretary of the Treasury, and the Treasury Inspector General for Tax Administration. The report also is available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact Nancy R. Kingsbury at (202) 512-2700 or Gregory C. Wilshusen at (202) 512-6244. We can also be reached by e-mail at kingsburyn@gao.gov and wilshuseng@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Sincerely yours,

Nancy R. Kingsbury
Managing Director, Applied Research and Methods



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objective, Scope, and Methodology

The objective of our review was to determine whether controls over key financial and tax processing systems were effective in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer information at the Internal Revenue Service (IRS). To do this, we examined IRS information security policies, plans, and procedures; tested controls over key financial applications; and interviewed key agency officials in order to (1) assess the effectiveness of corrective actions taken by IRS to address weaknesses we previously reported[1] and (2) determine whether any additional weaknesses existed. This work was performed in connection with our audit of IRS's fiscal year 2010 and 2009 financial statements for the purpose of supporting our opinion on internal control over the preparation of those statements.

To determine whether controls over key financial and tax processing systems were effective, we considered the results of our evaluation of IRS's actions to mitigate previously reported weaknesses, and performed new audit work at the three enterprise computing centers located in Detroit, Michigan; Martinsburg, West Virginia; and Memphis, Tennessee, as well as an IRS facility in New Carrollton, Maryland. We concentrated our evaluation on threats emanating from sources internal to IRS's computer networks. Considering systems that directly or indirectly support the processing of material transactions that are reflected in the agency's financial statements, we focused on eight critical applications/systems as well as the general support systems.

Our evaluation was based on our *Federal Information System Controls Audit Manual*,[2] which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; National Institute of Standards and Technology guidance; and IRS policies and procedures. We evaluated controls by

- reviewing the complexity and expiration of password settings to determine if password management had been enforced;

[1]We examined corrective actions for weaknesses IRS reported as having been corrected as of April 30, 2010.

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

- analyzing users' system access to determine whether they had been granted more permissions than necessary to perform their assigned functions;
- reviewing configuration files for servers and network devices to determine if encryption was being used for transmitting data;
- assessing configuration settings to evaluate settings used to audit security-relevant events and discussing and observing monitoring efforts with IRS officials;
- observing and analyzing physical access controls to determine if computer facilities and resources had been protected;
- inspecting key servers to determine whether critical patches had been installed or software was up-to-date; and
- examining user access and responsibilities to determine whether incompatible functions had been segregated among different individuals.

Using the requirements in the Federal Information Security Management Act that establish elements for an effective agencywide information security program, we reviewed and evaluated IRS's implementation of its security program by

- analyzing IRS's risk assessments for six IRS financial and tax processing systems that are key to supporting the agency's financial statements, to determine whether risks and threats had been documented;
- comparing IRS's policies, procedures, practices, and standards to actions taken by IRS personnel to determine whether sufficient guidance had been provided to personnel responsible for securing information and information systems;
- analyzing security plans for six systems to determine if management, operational, and technical controls had been documented and if security plans had been updated;
- verifying whether new employees had received system security orientation within the first 10 working days;
- verifying whether employees with security-related responsibilities had received specialized training within the year;

- analyzing test plans and test results for six IRS systems to determine whether management, operational, and technical controls had been tested at least annually;
- reviewing IRS's system remedial action plans to determine if they were complete;
- reviewing IRS's actions to correct weaknesses to determine if they had effectively mitigated or resolved the vulnerability or control deficiency;
- reviewing system backup and recovery procedures to determine if they had adequately provided for recovery and reconstitution to the system's original state after a disruption or failure; and
- examining contingency plans for six IRS systems to determine whether those plans had been tested or updated.

In addition, we discussed with management officials and key security representatives, such as those from IRS's Computer Security Incident Response Center, Office of Cybersecurity, as well as the three computing centers, whether information security controls were in place, adequately designed, and operating effectively.

Appendix II: Comments from the Internal Revenue Service

COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

March 1, 2011

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report, *Information Security: IRS Needs to Enhance Internal Control Over Financial Reporting and Taxpayer Data* (GAO-11-308). We appreciate that your draft report recognizes the progress that the Internal Revenue Service has made to improve our information security program and that numerous initiatives are underway.

The security and privacy of all taxpayer and financial information is of utmost importance to us, and the integrity of our financial systems continues to be sound. We are committed to securing our computer environment as we continually evaluate processes, promote user awareness, and apply innovative ideas to increase compliance.

The IRS has established enterprise repeatable processes which are overseen by an internal team that performs self-inspections, identifies and mitigates risks, and provides executive governance over the corrective actions to this material weakness. The combination of all of these actions makes us confident that we are steadily progressing toward eliminating this issue as a material weakness.

We appreciate your continued support and guidance as we work to improve our security posture and look forward to working with you to develop appropriate measures. We will provide the detailed corrective action plan addressing each of the recommendations with our response to the final report.

If you have any questions or would like to discuss our response in further detail, please contact Terence V. Milholland, Chief Technology Officer, at (202) 622-6800.

Sincerely,

Douglas H. Shulman

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nancy R. Kingsbury (202) 512-2700 or kingsburyn@gao.gov
Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individuals named above, David Hayes (assistant director), Jeffrey Knott (assistant director), Angela Bell, Mark Canter, Sharhonda Deloach, Nancy Glover, Nicole Jarvis, George Kovachick, Sylvia Shanks, Eugene Stevens, Michael Stevens, and Daniel Swartz made key contributions to this report.

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to 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 Web site, 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.

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

Ralph Dawn, Managing Director, dawnr@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