

March 2007

INFORMATION
SECURITY

Further Efforts
Needed to Address
Significant
Weaknesses at the
Internal Revenue
Service





Highlights of [GAO-07-364](#), a report to the Commissioner of Internal Revenue

Why GAO Did This Study

In fiscal year 2006, the Internal Revenue Service (IRS) collected about \$2.5 trillion in tax payments and paid about \$277 billion in refunds. Because IRS relies extensively on computerized systems, effective information security controls are essential to ensuring that financial and taxpayer information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of its audit of IRS's fiscal years 2006 and 2005 financial statements, GAO assessed (1) IRS's actions to correct previously reported information security weaknesses and (2) whether controls were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. To do this, GAO examined IRS information security policies and procedures, guidance, security plans, reports, and other documents; tested controls over five critical applications at three IRS sites; and interviewed key security representatives and management officials.

What GAO Recommends

GAO is recommending that the IRS Commissioner take several actions to fully implement an agencywide information security program. In commenting on a draft of this report, IRS agreed to address all recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-364.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Greg Wilshusen at (202) 512-6244 or WilshusenG@gao.gov or Keith A. Rhodes at (202) 512-6412 or Rhodesk@gao.gov.

INFORMATION SECURITY

Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service

What GAO Found

IRS has made limited progress toward correcting or mitigating previously reported information security weaknesses at two data processing sites, but 66 percent of the weaknesses that GAO had previously identified still existed. Specifically, IRS has corrected or mitigated 25 of the 73 information security weaknesses that GAO reported as unresolved at the time of our last review. For example, IRS has improved password controls on its servers and enhanced audit and monitoring efforts for mainframe and Windows user activity, but it continues to (1) use inadequate account lockout settings for Windows servers and (2) inadequately verify employees' identities against official IRS photo identification.

Significant weaknesses in access controls and other information security controls continue to threaten the confidentiality, integrity, and availability of IRS's financial and tax processing systems and information. For example, IRS has not implemented effective access controls related to user identification and authentication, authorization, cryptography, audit and monitoring, physical security, and other information security controls. These weaknesses could impair IRS's ability to perform vital functions and increase the risk of unauthorized disclosure, modification, or destruction of financial and sensitive taxpayer information. Accordingly, GAO has reported a material weakness in IRS's internal controls over its financial and tax processing systems.

A primary reason for the new and old weaknesses is that IRS has not yet fully implemented its information security program. IRS has taken a number of steps to develop, document, and implement an information security program. However, the agency has not yet fully or consistently implemented critical elements of its program. Until IRS fully implements an agencywide information security program that includes risk assessments, enhanced policies and procedures, security plans, training, adequate tests and evaluations, and a continuity of operations process for all major systems, the financial and sensitive taxpayer information on its systems will remain vulnerable.

Contents

Letter		1
	Results in Brief	2
	Background	3
	Objectives, Scope, and Methodology	5
	IRS Made Limited Progress in Correcting Previously Reported Weaknesses	7
	Significant Weaknesses Continue to Place Financial and Taxpayer Information at Risk	8
	Conclusions	22
	Recommendations for Executive Action	22
	Agency Comments	23
Appendix I	Comments from the Commissioner of Internal Revenue	26
Appendix II	GAO Contacts and Staff Acknowledgments	29

Abbreviations

CIO	Chief Information Officer
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
MA&SS	Mission Assurance and Security Services
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TIGTA	Treasury Inspector General for Tax Administration

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



United States Government Accountability Office
Washington, DC 20548

March 30, 2007

The Honorable Mark W. Everson
Commissioner of Internal Revenue

Dear Commissioner Everson:

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. Effective information system controls are essential to ensuring that financial and taxpayer information are adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. These controls also affect the confidentiality, integrity, and availability of financial and sensitive taxpayer information.

As part of our audit of IRS's fiscal years 2006 and 2005 financial statements, we assessed the effectiveness of the service's information security controls¹ over key financial systems, information, and interconnected networks at three locations. These systems support the processing, storage, and transmission of financial and sensitive taxpayer information. In our report on IRS's fiscal years 2006 and 2005 financial statements,² we reported that the new information security deficiencies we identified in fiscal year 2006 and the unresolved deficiencies from prior audits represent a material weakness³ in internal controls over financial and tax processing systems.

¹Information security controls include electronic access controls, software change controls, physical security, segregation of duties, and continuity of operations. These controls are designed to ensure that access to data is appropriately restricted, that only authorized changes to computer programs are made, that physical access to sensitive computing resources and facilities is protected, that computer security duties are segregated, and that back-up and recovery plans are adequate to ensure the continuity of essential operations.

²GAO, *Financial Audit: IRS's Fiscal Years 2006 and 2005 Financial Statements*, [GAO-07-136](#) (Washington, D.C.: Nov. 9, 2006).

³A material weakness is a reportable condition that precludes the entity's internal controls from providing reasonable assurance that material misstatements in the financial statements would be prevented or detected on a timely basis.

We assessed (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses at two data processing sites and (2) whether controls over key financial and tax processing systems are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information.

This report provides a general summary of the vulnerabilities identified and our recommendations to help strengthen and improve IRS's information security program. We are also issuing a separate report for limited distribution that contains sensitive information. It describes in more detail the information security weaknesses that we identified and our specific recommendations for correcting them.

We performed our review in accordance with generally accepted government auditing standards, from June 2006 through November 2006.

Results in Brief

IRS has made limited progress toward correcting previously reported information security weaknesses at two data processing sites. It has corrected or mitigated 25 of the 73 information security weaknesses that we reported as unresolved at the time of our last review at those sites. Actions have been taken to address weaknesses related to access controls and configuration management, among other things. For example, IRS has implemented controls used to authorize access to Windows systems, network devices,⁴ databases, and mainframe systems; improved password controls on its servers; enhanced audit and monitoring efforts for mainframe and Windows user activity; conducted a facility risk assessment at a critical data processing site; and improved change controls over one of its mainframe systems. Nevertheless, 66 percent, or 48 of the 73 previously identified information security weaknesses remain unresolved.

Significant weaknesses in access controls and other information security controls continue to threaten the confidentiality, integrity, and availability of IRS's financial and tax processing systems and information. IRS has not

⁴Organizations secure their networks, in part, by installing and configuring network devices that permit authorized network service requests, deny unauthorized requests, and limit the services that are available on the network. Devices used to secure networks include (1) firewalls that prevent unauthorized access to the network, (2) routers that filter and forward data along the network, (3) switches that forward information among segments of a network, and (4) servers that host applications and data.

consistently implemented effective access controls to prevent, limit, or detect unauthorized access to computing resources from within its internal network. These access controls include those related to user identification and authentication, authorization, cryptography, audit and monitoring, and physical security. In addition, IRS faces risks to its financial and sensitive taxpayer information due to weaknesses in configuration management, segregation of duties, media destruction and disposal, and personnel security controls. A key reason for the information security weaknesses in IRS's financial and tax processing systems is that it has not yet fully implemented its agencywide information security program to ensure that controls are effectively established and maintained. As a result, weaknesses in information security controls over its key financial and tax processing systems could impair IRS's ability to perform vital functions and could increase the risk of unauthorized disclosure, modification, or destruction of financial and sensitive taxpayer information.

We are making recommendations to the Commissioner of Internal Revenue to take several actions to fully implement a comprehensive agencywide information security program. We also are making recommendations to the commissioner in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses related to user identification and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, media destruction and disposal, and personnel security.

In providing written comments on a draft of this report, the Commissioner of Internal Revenue recognized that continued diligence of IRS's security and privacy responsibilities is required. He further stated that IRS would continue to remedy all recommendations to completion to ensure that operations of its applications and systems adhere to security requirements.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Without proper safeguards, systems are unprotected from individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit

fraud, disrupt operations, or launch attacks against other computer systems and networks. These concerns are well founded for a number of reasons, including the dramatic 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.

Our previous reports, and those by the Treasury Inspector General for Tax Administration (TIGTA), describe persistent information security weaknesses that place federal agencies, including IRS, at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002⁵ 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 to provide information security for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management. Such a program includes developing and implementing security plans, policies, and procedures; testing and evaluating the effectiveness of controls; assessing risk; providing specialized training; planning, implementing, evaluating, and documenting remedial action to address information security deficiencies; and ensuring continuity of operations. We have designated information security as a governmentwide high-risk area since 1997⁶—a designation that remains in force today.⁷

IRS has demanding responsibilities 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. In fiscal year 2006, IRS collected about \$2.5 trillion in tax payments, processed hundreds of millions of tax and information returns, and paid about \$277 billion in refunds to taxpayers. IRS is a large and complex organization, adding unique mission operational challenges for management. It employs tens of thousands of people in 10 service center

⁵FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (Dec. 17, 2002).

⁶GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997).

⁷GAO, *High-Risk Series: An Update*, [GAO-07-310](#) (Washington, D.C.: January 2007).

campuses, 3 computing centers, and numerous other field offices throughout the United States.

IRS also collects and maintains a significant amount of personal and financial information on each American taxpayer. The confidentiality of this sensitive information must be protected; otherwise, taxpayers could be exposed to loss 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, availability, and integrity of the information and information systems that support the agency and its operations. FISMA states that the Chief Information Officer (CIO) is responsible for developing and maintaining an information security program. Within IRS, this responsibility is delegated to the Chief of Mission Assurance and Security Services (MA&SS). The Chief of MA&SS is responsible for developing policies and procedures regarding information technology security; establishing a security awareness and training program; conducting security audits; coordinating the implementation of logical access controls into IRS systems and applications; providing physical and personnel security; and, among other things, monitoring IRS security activities. To help accomplish these goals, MA&SS has developed and published information security policies, guidelines, standards, and procedures in the *Internal Revenue Manual*, the *Law Enforcement Manual*, and other documents. The Modernization and Information Technology Services organization, led by the CIO, is responsible for developing security controls for systems and applications; conducting annual tests of systems; implementing, testing, and validating the effectiveness of remedial actions; ensuring that continuity of operations requirements are addressed for all applications and systems it owns; and mitigating technical vulnerabilities and validating the mitigation strategy.

Objectives, Scope, and Methodology

The objectives of our review were to determine (1) the status of IRS's actions to correct or mitigate previously reported weaknesses at two data processing sites and (2) whether controls over key financial and tax processing systems located at three sites were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. This review was completed to support the annual financial statement audit, by assessing the effectiveness of information system controls for the purposes of supporting our opinion on internal controls over the preparation of the financial statements.

We concentrated our evaluation primarily on threats emanating from sources internal to IRS's computer networks. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; (2) FISMA, which establishes key elements that are required for an effective agencywide information security program; and (3) previous reports from TIGTA and GAO. Specifically, we evaluated information security controls that are intended to

- prevent, limit, and detect electronic access to computer resources (information, programs, and systems), thereby protecting these resources against unauthorized disclosure, modification, and use;
- provide physical protection of computer facilities and resources from espionage, sabotage, damage, and theft;
- prevent the exploitation of security vulnerabilities;
- prevent the introduction of unauthorized changes to application or system software;
- ensure that work responsibilities for computer functions are segregated so that one individual does not perform or control all key aspects of computer-related operations and, thereby, have the ability to conduct unauthorized actions or gain unauthorized access to assets or records without detection;
- provide confidentiality of used media; and
- limit the disruption to a system due to the intentional or unintentional actions of individuals.

In addition, we evaluated IRS's agencywide information security program. We identified and reviewed pertinent IRS information security policies and procedures, guidance, security plans, relevant reports, and other documents. We also tested the effectiveness of information security controls at three IRS sites. We focused on five critical applications that directly or indirectly support the processing of material transactions that are reflected in the agency's financial statement. These applications are used for procurement, asset management, and tax administration, which are located at the sites. We also discussed with key security representatives and management officials whether information security controls were in place, adequately designed, and operating effectively.

IRS Made Limited Progress in Correcting Previously Reported Weaknesses

IRS has made limited progress toward correcting previously reported information security weaknesses at two data processing sites. Specifically, it has corrected or mitigated 25 of the 73 weaknesses that we reported as unresolved at the time of our last review. IRS corrected weaknesses related to access controls and configuration management, among others. For example, it has

- made progress in implementing controls used to authorize access to Windows systems, network devices, databases, and mainframe systems by, among other things, removing administrative privileges from Windows users who did not need them to perform job duties; securely configuring the protocol used for managing network performance; improving control over data sharing among mainframe users; and restricting a certain access privilege to mainframe users who did not need it to perform their job duties;
- improved password controls on its servers by installing a password filter on Windows systems requiring users to create passwords in accordance with IRS policy, discontinuing the use of stored passwords in clear text for automatic logon files and structured query language scripts, and requiring password complexity and stronger password expiration policies on Windows systems;
- enhanced audit and monitoring efforts for mainframe and Windows user activity;
- conducted a facility risk assessment at a critical data processing site; and
- improved change controls over one of IRS's mainframe systems.

In addition, IRS has made progress in enhancing its information security program. For example, IRS has trained its staff to restore operations in the event of an emergency at an off-site location, assessed risks for the systems we reviewed, certified and accredited the systems we reviewed, enhanced information security awareness and training by providing training to employees and contractors, and established an ongoing process of testing and evaluating its systems to ensure compliance with policies and procedures.

Although IRS has made progress in correcting many of the previously identified security weaknesses, 48 weaknesses (66 percent) remain unresolved. For example, IRS continued to, among other things,

- use inadequate account lockout settings for Windows servers,

-
- improperly restrict file permissions on UNIX systems,
 - routinely permit unencrypted protocols for remote logon capability to servers,
 - insufficiently monitor system activities and configure certain servers to ensure adequate audit trails,
 - inadequately verify employees' identities against official IRS photo identification,
 - use an ineffective patch management program, and
 - use disaster recovery plans that did not include disaster recovery procedures for certain mission-critical systems.

Significant Weaknesses Continue to Place Financial and Taxpayer Information at Risk

Significant weaknesses in access controls and other information security controls continue to threaten the confidentiality, integrity, and availability of IRS's financial and tax processing systems and information. A primary reason for these weaknesses is that IRS has not yet fully implemented its information security program. As a result, IRS's ability to perform vital functions could be impaired and the risk of unauthorized disclosure, modification, or destruction of financial and sensitive taxpayer information is increased.

Access Controls Were Inadequate

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. Inadequate access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service. Access controls include those related to user identification and authentication, authorization, cryptography, audit and monitoring, and physical security. IRS did not ensure that it consistently implemented effective access controls in each of these areas, as the following sections in this report demonstrate.

User Identification and Authentication

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals.

When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system also must 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. According to IRS policy, user accounts will be associated with only one individual or process and should automatically lockout after three consecutive failed logon attempts. If user accounts are not associated with an individual (e.g., group user accounts), they must be controlled, audited, and managed. In addition, IRS policy requires strong enforcement of passwords for authentication to IRS systems. For example, passwords are to expire and are not to be shared by users.

IRS did not adequately control the identification and authentication of users to ensure that only authorized individuals were granted access to its systems. For example, administrators at one site shared logon accounts and passwords when accessing a database production server for the procurement system.⁸ By allowing users to share accounts and passwords, individual accountability for authorized system activity as well as unauthorized system activity could be lost. In addition, at the same site, IRS did not enforce strong password management on the same database production server. Accounts did not lock out users after failed logon attempts and passwords did not expire. As a result, the database was susceptible to a brute force password attack that could result in unauthorized access. Furthermore, at another site, IRS stored user IDs and passwords in mainframe files that could be read by every mainframe user. As a result, increased risk exists that an intruder or unauthorized user could read and use these IDs and passwords to log on to the computer systems and masquerade as an authorized user.

Authorization

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 access rights is the concept of “least privilege.” Least privilege is a basic principle for securing computer resources and information. This principle means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users’ access to only those programs and files that they need to do their work, organizations establish access rights and permissions. “User rights” are

⁸This system processed about \$3.9 billion in fiscal year 2006.

allowable actions that can be assigned to users or to groups 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 users access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions. IRS policy requires that all production systems be securely configured to specifically limit access privileges to only those individuals who need them to perform their official duties.

IRS permitted excessive access to key financial systems by granting rights and permissions that gave users more access than they needed to perform their official duties. For example, at one site, excessive read access was allowed to production system libraries that contained mainframe configuration information. In addition, this site did not maintain documentation of approved access privileges allowed to each system resource by each user group. Without such documentation, IRS limits its ability to monitor and verify user access privileges. Furthermore, IRS did not appropriately restrict the use of anonymous e-mails on the two mainframe systems we reviewed. These servers allowed anonymous e-mails from one of our analysts masquerading as a legitimate sender and could expose IRS employees to malicious activity, including phishing.⁹ At another site, IRS granted all users excessive privileges to sensitive files on its production database server for the procurement system. Additionally, the procurement system was vulnerable to a well-known exploit whereby database commands could be inserted into the application through a user input screen that was available to everyone on the agency's network. Administrative privileges also were granted to the procurement system's database application user ID at this location. This user ID allowed extensive administrative privileges that were inappropriate for this type of account. Excessive or unauthorized access privileges provide opportunities for individuals to circumvent security controls.

Cryptography

Cryptography¹⁰ underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic

⁹Phishing is the act of tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

¹⁰Cryptography is used to secure transactions by providing ways to ensure data confidentiality, data integrity, authentication of the message's originator, electronic certification of data, and nonrepudiation (proof of the integrity and origin of data that can be verified by a third party).

element of cryptography is encryption. Encryption can be used to provide basic data confidentiality and integrity, by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. IRS policy requires the use of encryption for transferring sensitive but unclassified information between IRS facilities. The National Security Agency also recommends disabling protocols that do not encrypt information transmitted across the network, such as user ID and password combinations.

IRS did not consistently apply encryption to protect sensitive data traversing its network. For example, at one site, IRS was using an unencrypted protocol to manage network devices on a local server. In addition, the procurement application and the UNIX servers we reviewed at another site were using unencrypted protocols. Therefore, all information, including user ID and password information, was being sent across the network in clear text. These weaknesses could allow an attacker to view information and use that knowledge to gain access to financial and system data being transmitted over the network.

Audit and Monitoring

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, or logs 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* requires that auditable events be captured and audit logs be used to review what occurred after an event, for periodic reviews, and for real-time analysis. In addition, the manual requires that audit logs be maintained and archived in a way that allows for efficient and effective retrieval, viewing, and analysis, and that the logs be protected from corruption, alteration, or deletion.

IRS did not consistently audit and monitor security-relevant system activity on its applications. According to IRS officials, IRS did not capture auditable events for its procurement application as a result of system performance issues. Therefore, no audit reports were being reviewed by managers for this application. In addition, IRS was unable to effectively monitor activity for its administrative financial system because the volume

of the information in the log made it difficult for IRS officials to systematically analyze targeted activities and security-relevant events or archive logs. As a result, unauthorized access could go undetected, and the agency's ability to trace or recreate events in the event of a system modification or disruption could be diminished.

Physical Security

Physical access controls are used to mitigate the risks to systems, buildings, and supporting infrastructure related to their physical environment and to control the entry and exit of personnel in buildings as well as data centers containing agency resources. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, and locks. Without these protections, IRS computing facilities and resources could be exposed to espionage, sabotage, damage, and theft. IRS policy states that only authorized personnel should have access to IRS buildings and structures.

Although IRS has implemented physical security controls over its information technology resources, certain weaknesses reduce the effectiveness of these controls. For example:

- IRS did not physically protect a server containing source code for its procurement application. The server was not located in a secured computer room; instead, it was located in a cubicle.
- IRS did not consistently manage the use of proximity cards, which are used to gain access to secured IRS facilities. For example, one of the sites we visited could not account for active proximity cards for at least 11 separated employees. At that same site, at least 12 employees and contractors were given proximity cards that allowed them access to a computer room, although these individuals did not need this access to perform their official duties.
- IRS did not always effectively secure certain restricted areas. For example, it implemented motion detectors at one site to release the locks on doors that lead from areas that are accessible by the general public directly into IRS-controlled areas. The motion detector's field of view was set wider than necessary, so that an unauthorized individual would simply have to wait for an authorized individual to pass by the motion detector on the IRS-controlled side of the door to gain unauthorized access to the IRS facility.

As a result, IRS is at increased risk of unauthorized access to financial information and inadvertent or deliberate disruption of procurement services.

Other Information System Controls Were Not Sufficient

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, segregating incompatible duties, sufficiently disposing of media, and implementing personnel security. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of IRS's information and information systems.

Configuration Management

The purpose of configuration management is to establish and maintain the integrity of an organization's work products. By implementing configuration management, organizations can better ensure that only authorized applications and programs are placed into operation through establishing and maintaining baseline configurations and monitoring changes to these configurations. According to IRS policy, changes to baseline configurations should be monitored and controlled. Patch management, a component of configuration management, is an important factor in mitigating software vulnerability risks. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involves considerably less time and effort than responding after an exploit has occurred. Up-to-date patch installation can help diminish vulnerabilities associated with flaws in software code. Attackers often exploit these flaws to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations' systems. According to the National Institute of Standards and Technology (NIST), tracking patches allows organizations to identify which patches are installed on a system and provides confirmation that the appropriate patches have been applied. IRS's patch management policy also requires that patches be implemented in a timely manner, and that critical patches are applied within 72 hours to minimize vulnerabilities.

IRS did not properly implement configuration management procedures. For example, IRS did not record successful changes to baseline configurations on one of its mainframe systems, which supports its general ledger for tax administration activities. Without adequately logging system configuration changes, IRS cannot adequately ensure they are properly monitored and controlled. In addition, IRS did not effectively

track or install patches in a timely manner. For example, one IRS location did not have a tracking process in place to ensure that up-to-date patches have been applied on UNIX servers. Furthermore, installation of critical patches through the configuration management process for Windows systems was not timely. For example, critical Windows patches released in July 2006 had not yet been applied at the time of our review in August 2006. As a result, increased risk exists that the integrity of IRS systems could be compromised.

Segregation of Duties

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.

IRS did not always properly segregate incompatible duties. For example, IRS established test accounts on a production server for its procurement system. Test accounts are used by system developers and are not typically found on production servers. Allowing test accounts on production servers creates the potential for individuals to perform incompatible functions, such as system development and production support. Granting this type of access to individuals who do not require it to perform their official duties increases the risk that sensitive information or programs could be improperly modified, disclosed, or deleted.

Media Destruction and Disposal

Media destruction and disposal is a key to ensuring confidentiality of information. Media can include magnetic tapes, optical disks (such as compact disks), and hard drives. Organizations safeguard used media to ensure that the information it contains is appropriately controlled. Improperly disposed media can lead to the inappropriate or inadvertent disclosure of an agency's sensitive information or the personally identifiable information of its employees and customers. This potential

vulnerability can be mitigated by properly sanitizing the media. According to IRS policy, all media should be sanitized prior to disposal in such a manner that sensitive information on that media cannot be recovered by ordinary means. The policy further requires that IRS maintain records certifying that sanitation was performed.

IRS did not have an appropriate process for disposing of information stored on optical disk. According to agency officials at one of the sites we visited, discarded optical disks were left unattended in a hallway bin awaiting destruction by the cleaning staff. These disks had not been sanitized, and IRS staff were unaware if the unattended disks contained sensitive information. Furthermore, the cleaning staff did not maintain records certifying that the media were destroyed. As a result, IRS could not ensure the confidentiality of potentially sensitive information stored on optical disks marked for destruction.

Personnel Security

The greatest harm or disruption to a system comes from the actions, both intentional and unintentional, of individuals. These intentional and unintentional actions can be reduced through the implementation of personnel security controls. According to NIST, personnel security controls help organizations ensure that individuals occupying positions of responsibility (including third-party service providers) are trustworthy and meet established security criteria for those positions. Organizations should also ensure that information and information systems are protected during and after personnel actions, such as terminations and transfers. Organizations can decrease the risk of harm or disruption of systems by implementing personnel security controls associated with personnel screening and termination. Personnel screening controls should be implemented when an individual requires access to facilities, information, and information systems before access is authorized. Organizations should also implement controls for when employment is terminated, including ceasing information system access and ensuring the return of organizational information system-related property (e.g., ID cards or building passes).

According to the *Internal Revenue Manual*, contractor employees must complete a background investigation to be granted on-site, staff-like access to IRS facilities. However, if a background investigation has not been completed, individuals may not have access to IRS sensitive areas unless they are escorted by an IRS employee. The manual further states that managers are responsible for identifying separated employees in order to recover IRS assets, such as ID media. Separated employees' accounts are to be deactivated within 1 week of an individual's departure

on friendly terms and immediately upon an individual's departure on unfriendly terms.

IRS did not always ensure the effective implementation of its personnel security controls. For example, at two sites, IRS granted contractors¹¹ who did not have a completed background investigation unescorted physical access to sensitive areas. In addition, at all three sites we reviewed, IRS did not appropriately remove application access for separated personnel. For example, 19 individuals who had separated from IRS for periods ranging from 3 weeks to 14 months still maintained access to applications during our review this year. These practices increase the risk that individuals might gain unauthorized access to IRS resources.

Agencywide Information Security Program Was Not Yet Fully Implemented

A key reason for the information security weaknesses in IRS's financial and tax processing systems is that it has not yet fully implemented its agencywide information security program to ensure that controls are effectively established and maintained. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes

- periodic assessments of the risk and the 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 risks, (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;
- at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices relating to management,

¹¹This year's background investigation review only consisted of contractors.

operational, and technical controls of every major information system that is identified in the agency's inventories;

- 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.

Although IRS continued to make important progress in developing and documenting a framework for its information security program, key components of the program had not been fully or consistently implemented.

Risk Assessments

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 these policies and controls operate as intended. The Office of Management and Budget (OMB) *Circular A-130*, appendix III, prescribes that risk be reassessed when significant changes are made to computerized systems—or at least every 3 years. Consistent with NIST guidance, IRS requires its risk assessment process to detail the residual risk assessed and potential threats, and to recommend corrective actions for reducing or eliminating the vulnerabilities identified.

Although IRS had implemented a risk assessment process, it did not always effectively evaluate potential risks for the systems we reviewed. IRS has reassessed the risk level for each of its 264 systems and categorized them on the basis of risk. Furthermore, the five risk assessments that we reviewed were current, documented residual risk assessed and potential threats, and recommended corrective actions for reducing or eliminating the vulnerabilities they identified. However, IRS did not identify many of the vulnerabilities in this report and did not assess the risks associated with them. As a result, potential risks to these systems may be unknown.

Policies and Procedures

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 implemented, policies and procedures should help reduce the risk that could come from unauthorized access or

disruption of services. Technical security standards provide consistent implementation guidance for each computing environment. Developing, documenting, and implementing security policies is important because they are the 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 systems and information will not receive the protection that the security policies and controls should provide.

Although IRS has developed and documented information security policies, standards, and guidelines that generally provide appropriate guidance to personnel responsible for securing information and information systems, it did not always provide needed guidance on how to guard against significant mainframe security weaknesses. For example, IRS policy lacked guidance on how to correctly configure certain mainframe IDs used by the operating system and certain powerful mainframe programs used to control processing. As a result, IRS has reduced assurance that its systems and the information they contain are sufficiently protected.

Security Plans

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.

IRS had developed system security plans for four of the five systems we reviewed. The plans addressed policies and procedures for providing management, operational, and technical controls. However, IRS had not developed a system security plan for the system that supports its general ledger for tax administration activities. As a result, IRS cannot ensure that appropriate controls are in place to protect this key financial system and critical information.

Specialized Training

People are one of the weakest links in attempts to secure systems and networks. Therefore, an important component of an information security program is providing required training so that users understand system security risks and their own role in implementing related policies and

controls to mitigate those risks. IRS policy mandates that personnel with significant security responsibilities be provided with specialized training.¹² In addition, IRS policy requires that personnel performing information technology security duties meet minimum continuing professional education levels in accordance with their roles. Specifically, personnel performing technical security roles are required to have 24 hours of specialized training per year, personnel performing nontechnical roles are required to have 16 hours of specialized training per year, and personnel performing executive security roles should have 6 hours of specialized training per year. IRS policy also requires that effective tracking and reporting mechanisms be in place to monitor specialized training.

Although IRS has made significant progress in providing security personnel with job-related training and established a methodology for identifying employees with significant security responsibilities, in fiscal year 2006, at least 95 individuals with significant security responsibilities did not have the minimum number of hours of specialized training required by IRS policy. Of those 95 individuals, 18 had not completed any training for the last reporting year. In addition, IRS was not able to determine whether all of its employees had met minimum continuing professional education requirements. For example, IRS monitored employee training through its Enterprise Learning Management System, but the system could not differentiate between employees who are required to have only 6 hours of training and employees who are required to have more. Furthermore, IRS did not track all security-related training courses taken by its employees. These conditions increase the risk that employees and contractors may not be aware of their security responsibilities.

Tests and Evaluations of Control Effectiveness

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

¹²In its fiscal year 2006 FISMA submission, IRS reported that it has 2,476 employees with significant security responsibilities.

frequency of tests and evaluations be based on risks and occur no less than annually. IRS policy also requires periodic testing and evaluation of the effectiveness of information security policies and procedures.

IRS tested and evaluated information security controls for each of the systems we reviewed. However, these evaluations did not address many of the vulnerabilities we have identified in this report. For example, IRS's test and evaluation plan for its procurement system did not include tests for password expiration, insecure protocols, or the removal of employees' system access after separation from the agency. As a result, IRS has limited assurance that it has appropriately implemented controls, and it will be less able to identify needed controls.

Remedial Actions

A remedial action plan is a key component 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. According to IRS policy, the agency should document weaknesses found during security assessments as well as document any planned, implemented, and evaluated remedial actions to correct any deficiencies. The policy further requires that IRS track the status of resolution of all weaknesses and verify that each weakness is corrected.

IRS has developed and implemented a remedial action process to address deficiencies in its information security policies, procedures, and practices, however, this remedial action process was not working as intended. For example, the verification process used to determine whether remedial actions were implemented was not always effective. Of the 73 previously reported weaknesses, IRS had indicated that it had corrected or mitigated 57 of them. However, of those 57 weaknesses, 33 still existed at the time of our review. In addition, IRS had identified weaknesses but did not document them in a remedial action plan. For example, we reviewed system self-assessments for five systems and identified at least 8 weaknesses not documented in a remedial action plan. These weaknesses pertained to system audit trails, approval and distribution of continuity of operations plans, and documenting emergency procedures. TIGTA also reported that IRS was not tracking all weaknesses found during security assessments in 2006. As a result, increased risk exists that known vulnerabilities will not be mitigated.

IRS did not proactively ensure that weaknesses found at one of its facilities or on one of its systems were considered and, if necessary, corrected at other facilities or on similar systems. Many of the issues identified in this report were previously reported at other locations and on

similar systems. Yet, IRS had not applied those recommendations to the facilities and systems we reviewed this year. For example, we have been identifying weaknesses with encryption at IRS since 1998.¹³ However, IRS was not using encryption to protect information traversing its network. In addition, in 2002 we recommended that IRS promptly remove system access for separated employees and verify that system access has been removed. Nevertheless, IRS did not promptly remove system access for separated employees.

Recognizing the need for a servicewide solution, IRS developed a plan in October 2006 to address many of the recurring weaknesses. This plan includes remedial actions to address various weaknesses such as access authorization, audit and monitoring, configuration management, and testing of technical controls. According to IRS, the plan should be fully implemented by fiscal year 2012. However, until IRS fully implements its plan to address recurring weaknesses, it may not be able to adequately protect its information and information systems from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

Continuity of Operations

Continuity of operations planning is a critical component of information protection. To ensure that mission-critical operations continue, it is necessary to be able to detect, mitigate, and recover from service disruptions while preserving access to vital information. The elements of robust continuity of operations planning include, among others, identifying preventative controls (e.g., environmental controls); developing recovery strategies, including alternative processing locations; and performing disaster recovery exercises to test the effectiveness of continuity of operations plans. According to NIST, systems need to have a reasonably well-controlled operating environment, and failures in environmental controls such as air-conditioning systems may cause a service interruption and may damage hardware. IRS policy mandates that an alternate processing site be identified, and that agreements be in place when the primary processing capabilities are unavailable. The policy further requires that each application's recovery plan be tested on a yearly basis.

¹³GAO, *IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk*, [GAO/AIMD-99-38](#) (Washington, D.C.: Dec. 14, 1998); and *Information Security: Continued Progress Needed to Strengthen Controls at the Internal Revenue Service*, [GAO-06-328](#) (Washington, D.C.: Mar. 23, 2006).

IRS did not have adequate environmental controls at one of the sites we visited. For example, the air-conditioning system for the computer room that houses the procurement system could not adequately cool down the systems in the room and was supplemented by a portable fan. In addition, the fire extinguishers for the same room had not had an up-to-date inspection. Without providing adequate environmental controls, IRS is at increased risk that critical system hardware may be damaged.

Also, IRS had established alternate processing sites for four of the five applications we reviewed. However, it did not have an alternate processing site for its procurement system, and it had not tested the application's recovery plan. As a result, unforeseen events could significantly impair IRS's ability to fulfill its mission.

Conclusions

IRS has made important progress in correcting or mitigating previously reported weaknesses, implementing controls over key financial and tax processing systems, and developing and documenting a solid framework for its agencywide information security program. However, information security weaknesses—both old and new—continue to impair the agency's ability to ensure the confidentiality, integrity, and availability of financial and sensitive taxpayer information. These deficiencies represent a material weakness in IRS's internal controls over its financial and tax processing systems. A key reason for these weaknesses is that the agency has not yet fully implemented critical elements of its agencywide information security program. Until IRS (1) fully implements a comprehensive agencywide information security program that includes risk assessments, enhanced policies and procedures, security plans, training, adequate tests and evaluations, and a continuity of operations process for all major systems and (2) begins to address weaknesses across the service, its facilities, computing resources, and the financial and sensitive taxpayer information on its systems will remain vulnerable.

Recommendations for Executive Action

To help establish effective information security over key financial and tax processing systems, financial and sensitive taxpayer information, and interconnected networks, we recommend that you take the following 10 actions to implement an agencywide information security program:

- update the risk assessments for the five systems reviewed to include the vulnerabilities identified in this report;

-
- update policies and procedures to include guidance on configuring mainframe ID's used by the operating system and certain powerful mainframe programs used to control processing;
 - develop a system security plan for the system that supports the general ledger for tax administration activities;
 - enhance the Enterprise Learning Management System to include all security-related training courses taken by IRS employees and contractors and to differentiate required training hours for all employees;
 - update test and evaluation procedures to include tests for vulnerabilities identified in this report, such as password expiration, insecure protocols, and removal of system access after separation from the agency;
 - implement a revised remedial action verification process that ensures actions are fully implemented;
 - document weaknesses identified during security assessments in a remedial action plan;
 - provide adequate environmental controls for the computer room that houses the procurement system, such as a sufficient air-conditioning system and up-to-date fire extinguishers;
 - establish an alternate processing site for the procurement application; and
 - test the procurement system recovery plan.

We are also making 50 detailed recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses related to user identification and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, media destruction and disposal, and personnel security.

Agency Comments

In providing written comments (reprinted in app. I) on a draft of this report, the Commissioner of Internal Revenue stated that IRS understands that information security controls are essential for ensuring information is adequately protected from inadvertent or deliberate misuse, disruption, or destruction. He also noted that IRS has taken several steps to create a strong agencywide information security program as required by FISMA. The commissioner recognized that continued diligence of IRS's security

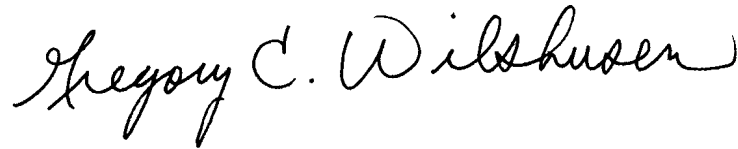
and privacy responsibilities is required, and he further stated that IRS will continue to remedy all recommendations to completion to ensure that operations of its applications and systems adhere to security requirements.

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, GAO requests that the agency also provide it with a copy of your 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 and the Secretary of the Treasury. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you have any questions regarding this report, please contact Gregory Wilshusen at (202) 512-6244 or Keith Rhodes at (202) 512-6412. We can also be reached by e-mail at wilshuseng@gao.gov and rhodesk@gao.gov. Contact points for our Offices 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 II.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues



Keith A. Rhodes,
Chief Technologist

Appendix I: Comments from the Commissioner of Internal Revenue



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

March 16, 2007

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

Dear Mr. Wilshusen:

I am writing to provide the Internal Revenue Service's (IRS's) comments on the Government Accountability Office (GAO) draft report, *Information Security: Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service (GAO-07-364)*.

Thank you for recognizing the progress IRS has made in taking actions to implement more effective information security controls over key financial and tax processing systems. The report indicates that the IRS has corrected or mitigated several of the specific technical weaknesses that GAO reported as unresolved at the time of your last review. We understand that effective information security controls are essential for ensuring information is adequately protected from inadvertent or deliberate misuse, disruption, or destruction.

The IRS has taken significant steps to create a strong, agency-wide information technology security program as required by the Federal Information Security Management Act (FISMA). This was noted in the recent Treasury Inspector General for Tax Administration assessment of IRS's progress toward that goal. We established the Mission Assurance and Security Services organization to bring focus to all security disciplines. Over the last year, we have made progress in addressing computer security deficiencies throughout the IRS by focusing attention in key areas:

- We began an aggressive initiative to complete the full suite of security certification and accreditation activities for all IRS computer applications and systems to bring them into compliance with recently issued National Institute of Standards and Technology (NIST) security guidance.
- We implemented NIST recommendations for the protection of sensitive information on laptops and removable media and established a comprehensive set of data protection initiatives to further safeguard our sensitive agency information. In conjunction with these initiatives, policies have been updated and issued; multi-layered encryption technology has been deployed; and extensive user training has been provided to our personnel.

2

- We established an Access Controls Project Team charged with documenting the appropriate authorization and access to all IRS systems and applications. We are currently implementing an automated process that will systematically control the proper authorization for gaining access; thus, minimizing our risk of unauthorized disclosure of sensitive information and disruption of service. In addition, system access privileges are regularly audited using tools that we have in place, and all security violations are captured and aggressively pursued.
- We strengthened our IT security program by ensuring that our personnel have specialized, role-based training to improve the secure operations of all computing environments.
- We continued our commitment of ensuring that all contractors and employees with access to our systems, data, or facilities have had an appropriate investigation commensurate with the level of risk of the positions they encumber prior to providing access.
- We developed a Physical Security Design Guide and standard operating procedures to improve the security and control of assets and to enhance the protections of IRS facilities. By adhering to our corrective action monitoring plan, the IRS is addressing physical security vulnerabilities at an enterprise level and monitoring for completion.
- We implemented protections to ensure that our computer and network infrastructure systems are resistant to external attacks—thus far, there have been no successful penetrations into any IRS systems by unauthorized users.

As mandated by FISMA, all IRS senior officials are actively engaged in fulfilling their security responsibilities for the business systems and applications in their areas of responsibility. The Chief Information Officer and Chief, Mission Assurance and Security Services are collaborating with executives throughout the IRS to ensure security policies, standards, and procedures are followed across the enterprise.

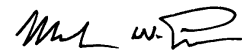
The IRS takes its security and privacy responsibilities very seriously. While we have made significant progress, we recognize that continued diligence is required. The report indicates ten recommendations for executive action. We will provide a detailed corrective action plan addressing each of the recommendations with our response to the final report. We will continue to remedy all recommendations to completion to ensure the operations of IRS applications and systems adhere to security requirements.

**Appendix I: Comments from the
Commissioner of Internal Revenue**

3

I appreciate your continued support and the valuable assistance and guidance from your staff. If you have any questions, or you would like to discuss this response in more detail, please contact Richard Spires, Chief Information Officer, at (202) 622-6800 or Daniel Galik, Chief Mission Assurance and Security Services at (202) 622-8910.

Sincerely,



Mark W. Everson

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244
Keith A. Rhodes, (202) 512-6412

Staff Acknowledgments

In addition to the persons named above, Don Adams, Bruce Cain, Mark Canter, Nicole Carpenter, Jason Carroll, West Coile, Denise Fitzpatrick, Edward Glagola Jr., David Hayes, Kevin Jacobi, Jeffrey Knott (Assistant Director), George Kovachick, Joanne Landesman, Leena Mathew, Kevin Metcalfe, Amos Tevelow, and Chris Warweg 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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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