United States Government Accountability Office

GAO

Report to the Commissioner of Internal Revenue

March 2006

INFORMATION SECURITY

Continued Progress Needed to Strengthen Controls at the Internal Revenue Service

GAO-06-328

March 2006

INFORMATION SECURITY

Continued Progress Needed to Strengthen Controls at the Internal Revenue Service

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-328, 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. Effective information security controls are essential for ensuring that information is adequately protected from inadvertent or deliberate misuse, disruption, or destruction.

As part of its audit of IRS's fiscal year 2005 financial statements, GAO assessed (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses at two sites and (2) whether controls over key financial and tax processing systems located at the facilities are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer data.

What GAO Recommends

GAO recommends that the IRS Commissioner take several actions to fully implement an information security program. In commenting on a draft of this report, IRS concurred with our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-328.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

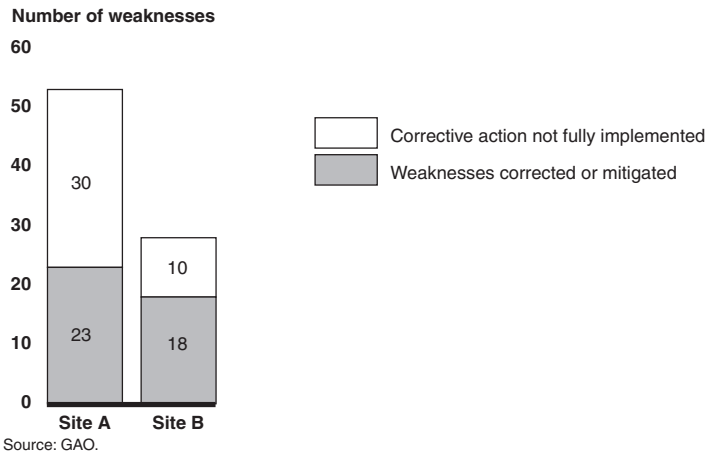
What GAO Found

IRS has made progress in correcting or mitigating previously reported information security weaknesses and in implementing controls over key financial and tax processing systems that are located at two of its critical data processing sites. It has corrected or mitigated 41 of the 81 specific technical weaknesses that we reported as unresolved at the time of our last review at those selected sites.

Although IRS has made progress, controls over its key financial and tax processing systems located at two sites were ineffective. In addition to the 40 previously reported weaknesses for which IRS has not completed actions, GAO identified new information security control weaknesses that threaten the confidentiality, integrity, and availability of IRS's financial information systems and the information they process. For example, IRS has not implemented effective electronic access controls related to network management, user accounts and passwords, user rights and file permissions, and logging and monitoring of security-related events. In addition, it has not effectively implemented other information security controls to physically secure computer resources, and to prevent exploitation of vulnerabilities and unauthorized changes to system software. Collectively, these weaknesses increase the risk that sensitive financial and taxpayer data will be inadequately protected against disclosure, modification, or loss, possibly without detection, and place IRS operations at risk of disruption.

A key reason for IRS's weaknesses in information security controls is that it has not yet fully implemented an information security program to ensure that effective controls are established and maintained. Until IRS fully implements a comprehensive agencywide information security program, its facilities and computing resources and the information that is processed, stored, and transmitted on its systems will remain vulnerable.

Status of Previously Reported Weaknesses at Selected Sites



Source: GAO.

Contents

Abbreviations

CIO	chief information officer
FISMA	Federal Information Security Management Act of 2002
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
TIGTA	Treasury Inspector General for Tax Administration

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

March 23, 2006

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 information is 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 taxpayer information.

As part of our audit of the IRS's fiscal year 2005 financial statements,[1] we assessed the effectiveness of its information security controls[2] over key financial systems, data, and interconnected networks at two of IRS's critical data processing sites that support the processing, storage, and transmission of sensitive financial and taxpayer data.

This report describes (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses at the 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 data.

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

[1]GAO, *Financial Audit: IRS's Fiscal Years 2005 and 2004 Financial Statements*, GAO-06-137 (Washington, D.C.: Nov. 10, 2005).

[2]Information security controls include electronic access controls, software change control, 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.

the information security weaknesses that we identified and our specific recommendations for correcting them.

Results in Brief

IRS has made progress in implementing more effective information security controls over key financial and tax processing systems that are located at two critical data processing sites, and has corrected or mitigated 41 of the 81 specific technical weaknesses that we reported as unresolved at the time of our last review at those selected sites. Actions have been taken to address weaknesses related to electronic access, physical access, and software change controls, among others. For example, IRS has implemented controls to protect mainframe system files that contain embedded user accounts and passwords.

Nevertheless, significant control weaknesses continue to threaten the confidentiality, integrity, and availability of key financial and tax processing systems and information. In addition to the remaining 40 previously reported specific technical weaknesses, for which IRS had not completed actions at the time of our review, other newly identified information security control weaknesses exist. IRS has not implemented effective electronic controls to prevent, limit, or detect unauthorized access to computing resources from its internal network. For example, IRS was not adequately managing its network, user accounts and passwords, and user privileges, and it was not adequately logging and monitoring security-relevant events. In addition, IRS faces risks to its key financial and tax-processing systems due to weaknesses in physical security, patch management, and system change controls. As a result, sensitive data and computing resources are at increased risk of unauthorized use, modification, loss, and disclosure, possibly without detection.

A key reason for the information security weaknesses in IRS's financial and tax processing systems was that the agency had not yet fully implemented its information security program. IRS has developed the framework for an effective information security program, with written policies and procedures that designate responsibility for implementation throughout the agency, and risk assessments that identify potential threats and recommended actions for reducing vulnerabilities. It has also established an incident handling program with defined procedures for detecting, responding to, and reporting security incidents. However, it has not fully implemented other key elements. For example, it has not (1) consistently implemented its policies and procedures, (2) completed system security plans, (3) trained employees with significant security responsibilities,

(4) adequately tested and evaluated systems to ensure compliance with policies and procedures, (5) completed remedial action plans, and (6) installed key hardware and equipment at its disaster recovery site. Until IRS fully implements a comprehensive agencywide information security program, its facilities, computing resources, and the information that is processed, stored, and transmitted on its systems will remain vulnerable.

We are making recommendations to the Commissioner of Internal Revenue to take several actions to fully implement a comprehensive agencywide information security program.

In providing written comments on a draft of this report, the Commissioner of Internal Revenue acknowledged that IRS needs to continue to implement a comprehensive agencywide security program, and agreed to implement the five recommendations in this report. He said that efforts are under way to remedy weaknesses and will continue until all recommendations have been addressed.

Background

Information security is an important consideration for any organization that depends on information systems and computer networks to carry out its mission or business. The same speed and accessibility that create the enormous benefits of the computer age can, if not properly controlled, allow individuals and groups with malicious intent to intrude into inadequately protected systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer networks and systems.

Protecting computer systems that support critical operations and infrastructures is important due to the concern about attacks from individuals and groups, including terrorists. These concerns are well founded for a number of reasons, including the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the warnings of new and more destructive attacks to come.

Computer-supported federal operations are likewise at risk. Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of critical federal operations, including those at IRS, at risk of disruption, fraud, and inappropriate disclosure. We have designated information security as a

governmentwide high-risk area since 1997[3]—a designation that remains today.[4]

In December 2002, Congress enacted the Federal Information Security Management Act of 2002 (FISMA) to strengthen security of information and systems within federal agencies.[5] 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.

In its role as the nation's tax collector, IRS has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. In fiscal year 2005, IRS collected about $2.3 trillion in tax payments, processed hundreds of millions of tax and information returns, and paid about $267 billion in refunds to taxpayers. IRS is a large and complex organization, with a unique mission that adds operational challenges for management. It employs tens of thousands of people in 10 service center campuses, three computing centers, and numerous other field offices throughout the United States. Because of the nature of its mission, IRS also collects and maintains a significant amount of personal and financial data 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 information and information systems supporting the agency and its operations. The Chief of Mission Assurance and Security Services is responsible for developing policies and procedures regarding information technology security; providing assurance services to improve physical, data, and personnel security; conducting independent testing; and ensuring security is integrated into its modernization activities. To help accomplish these goals, IRS has developed and published information security policies, guidelines,

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

[4]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

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

standards, and procedures in the *Internal Revenue Manual*, *Law Enforcement Manual*, and other documents.

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 sites and (2) whether controls over key financial and tax processing systems located at the sites are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer data. We concentrated our evaluation primarily on threats emanating from internal sources on 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 data; (2) FISMA, which sets key elements that are required for an effective information security program; and (3) previous reports from the Treasury Inspector General for Tax Administration (TIGTA).

Specifically, we evaluated information security controls that are intended to

- prevent, limit, and detect electronic access to computer resources (data, 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 vulnerabilities;
- prevent the introduction of unauthorized changes to application or system software; and
- 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 by another individual performing assigned responsibilities.

In addition, we evaluated IRS's information security program. Such a program includes assessing risk; developing and implementing policies,

procedures, and security plans; providing security awareness and training; testing and evaluating control effectiveness; planning, implementing, evaluating, and documenting remedial action to address information security deficiencies; detecting, reporting, and responding to security incidents; and ensuring continuity of operations.

To evaluate IRS's information security controls and program, we identified and reviewed pertinent IRS information security policies and procedures, guidance, security plans, relevant reports, and other documents, and we tested the effectiveness of these controls at two of IRS's critical data processing sites. Specifically, our tests focused on three critical applications, as well as three general support systems[6] located at the two sites. We also discussed with key security representatives and management officials whether information security controls were in place, adequately designed, and operating effectively.

We performed our review at the two previously mentioned IRS sites in accordance with generally accepted government auditing standards from June through November 2005. We discussed the results of our review with IRS officials.

IRS Has Made Progress in Correcting Previously Reported Weaknesses

IRS has made progress toward implementing more effective information security controls over key financial and tax processing systems that are located at two critical data processing sites, and has corrected or mitigated 41 of the 81 specific technical weaknesses that we reported as unresolved at the time of our last reviews at the selected sites.[7] Actions have been taken to address weaknesses related to electronic access, physical access, and software change controls, among others. For example, IRS has

- implemented controls to protect mainframe system files that contain embedded user accounts and passwords;

[6]A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications.

[7]The results of these reviews were reported in fiscal years 2003, 2004, and 2005 in reports for limited distribution due to the sensitive information they contained.

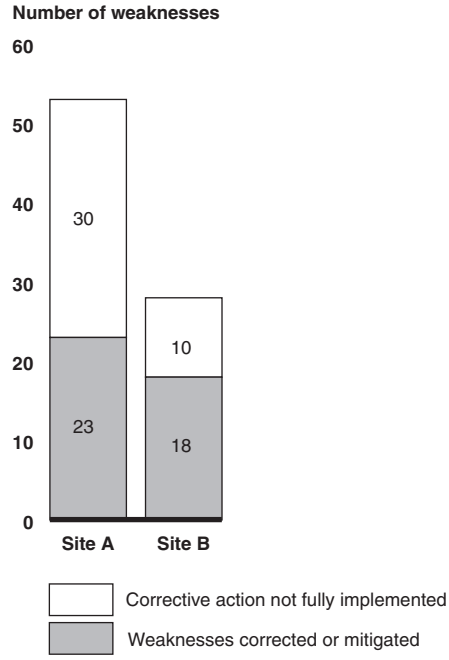
- improved the security of authentication data for network devices, such as routers and switches;
- securely configured certain vulnerable network services to help prevent unauthorized access;
- implemented procedures for periodically reviewing employee access to sensitive areas; and
- ensured that its software change control process includes the submission of documented test plans.

Additionally, IRS addressed critical mainframe weaknesses. In 2005, we reported[8] that IRS had not implemented effective electronic access controls over its mainframe computing environment to logically separate its taxpayer data from the Financial Crimes Enforcement Network's Bank Secrecy Act data, which include information related to financial crimes, terrorist financing, money laundering, and other illicit activities. These two types of data have different security requirements, and, accordingly, we made specific recommendations to correct these access control weaknesses. Since our last report, IRS has taken action to mitigate these weaknesses.

Although IRS has taken steps to strengthen its information security controls, it had not completed actions to correct or mitigate the remaining 40 previously reported technical weaknesses as illustrated in figure 1.

[8]GAO, *Information Security: Internal Revenue Service Needs to Remedy Serious Weaknesses over Taxpayer and Bank Secrecy Act Data*, GAO-05-482 (Washington, D.C.: Apr. 15, 2005).

Figure 1: Status of Previously Reported Weaknesses at Selected IRS Sites



Source: GAO.

These weaknesses include routinely permitting unencrypted protocols for remote log-on capability; not taking sufficient measures to prevent attackers from accessing information, copying sensitive files, and introducing malicious code via CD-ROM drives; inadequately restricting access to certain accounts with powerful rights over the system's operating system; and configuring servers without ensuring sufficient audit trails. Failure to resolve these issues will leave sensitive IRS computing resources and data vulnerable to unauthorized access, manipulation, and destruction.

In addition, last year we made three recommendations related to improving IRS's information security program. These recommendations included ensuring that established security policies and procedures are consistently followed and implemented, ensuring that employees with significant information security responsibilities are provided with the sufficient training and understand their role in implementing security-related policies and controls, and implementing an ongoing process of testing and evaluating systems to ensure compliance with established policies and

procedures. IRS agreed to implement these recommendations and is in the process of doing so.

Significant Weaknesses Place Financial and Taxpayer Data at Risk

Although IRS has made progress in implementing information security for its financial and tax processing systems and information by addressing many of its previously identified security weaknesses, significant weaknesses in electronic access and other information security controls continue to threaten the confidentiality, integrity, and availability of those systems and information. A primary reason for these weaknesses is that IRS has not yet fully implemented its information security program. As a result, weaknesses in controls over its key financial and tax processing systems could impair IRS's ability to perform vital functions and increase the risk of unauthorized disclosure, modification, or destruction of taxpayer data.

Electronic 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, and information. Electronic access controls include those related to network management, user accounts and passwords, user rights and file permissions, and logging and monitoring of security-relevant events. Inadequate controls over electronic processes diminish the reliability of computerized information, and they increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and of disruption of service.

IRS's electronic access controls were inadequate. Serious weaknesses existed in network management, user accounts and passwords, user rights and file permissions, and logging and monitoring of security-relevant events.

Network Management

Networks are collections of interconnected computer systems and devices that allow individuals to share resources, such as computer programs and information. Because sensitive programs and information are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations 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. Network services consist of protocols for transmitting data between network devices. Insecurely configured network services and devices can make a system vulnerable to internal or external threats, such as denial-of-service attacks.[9] Because networks often include both external and internal access points for electronic information assets, failure to secure these assets increases the risk of unauthorized modification of sensitive information and systems, or disruption of service.

IRS did not consistently configure network services and devices securely to prevent unauthorized access to and ensure the integrity of computer systems operating on its networks. For example, it did not sufficiently prevent the use of vulnerable remote services on servers. In addition, IRS's network management traffic was not segregated from normal user traffic, and IRS continued to rely on unencrypted protocols for remote management of certain devices. As a result, the agency is at increased risk of system compromise, such as unauthorized access to and manipulation of sensitive system data, disruption of services, and denial of service.

According to IRS officials, the agency took actions to mitigate the network traffic management weakness subsequent to our site visits.

User Accounts and Passwords

A computer system must be able to identify and differentiate among 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 distinguishes one user from another—a process called identification. The system must also establish the validity of a user's claimed identity though some means of authentication, such as a password, that is known only to its owner. 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. Accordingly, agencies (1) establish password parameters, such as number of characters, type of characters, and the frequency with which users should change their passwords, in order to strengthen the effectiveness of

[9]A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

passwords for authenticating the identity of users; (2) require encryption for passwords to prevent their disclosure to unauthorized individuals; and (3) implement procedures to control the use of user accounts. IRS policy identifies and prescribes minimum requirements for creating and managing passwords, such as minimum password length.

IRS did not adequately control user accounts and passwords to ensure that only authorized individuals were granted access to its systems. Although IRS has a policy in place addressing password expiration and complexity, it has not always implemented these requirements. For example, the agency did not always implement the use of complex passwords on its Windows servers. It also set the password expiration on a Windows server to a value inconsistent with its policy, and did not adequately control the storage of passwords on its systems. For example, instead of using encryption, IRS stored clear text passwords in readable form at one of the sites. Further, it had not implemented procedures to control user accounts by not adequately limiting the number of superuser accounts for over half of the UNIX servers reviewed. These practices increase the risk that individuals might gain unauthorized access to critical resources without attribution.

User Rights and File Permissions

The concept of "least privilege" is a basic underlying principle for securing computer systems and data. It 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 allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that are associated with a particular file or directory and regulate which users can access them and the extent of that access. To avoid unintentionally giving users unnecessary access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions. IRS policy states that users should only be given the minimum level of permissions needed to perform job duties.

IRS permitted excessive access to key financial systems, granting rights and permissions that allowed more access than users needed to perform their jobs. For example, IRS granted administrators of certain Windows servers a user right that could allow them to add false entries into the security log. In addition, it granted all users on one Windows server "read" access to a certain registry setting that would allow users to remotely read sensitive system settings. Further, IRS granted mainframe users privileges that were not needed to perform assigned job duties. For example, all

mainframe users were granted a powerful privilege that would allow users to read, execute, modify, delete, or create new datasets without restriction. Inappropriate access to sensitive files and directories provides opportunities for individuals to circumvent security controls to deliberately or inadvertently read, modify, or delete critical or sensitive information.

Logging and Monitoring of Security-Relevant Events

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. IRS policy states that audit logs must be generated for use in monitoring security-related events on all multiuser systems, and that these logs must be periodically reviewed. Further, National Institute of Standards and Technology (NIST) guidance states that organizations should deploy centralized logging servers and configure devices to send duplicates of their log entries to the centralized servers.

IRS was not adequately logging and monitoring security-relevant events. For example, two Windows servers at one site were not configured to log successful and failed attempts to access directory services. In addition, neither of the sites visited had implemented centralized logging and monitoring of logs for any of the UNIX servers reviewed. Further, at one site, although IRS was logging system developer activity[10] in the production environment, they were not monitoring the logs. As a result, the agency is at increased risk that unauthorized or inappropriate system activity may not be detected.

[10]One site was temporarily authorizing system developers' access to the production environment on the basis of a business need. Such access is not recommended by best practices; a mitigating control is to log and monitor developers' activities.

Other Information System Controls Were Not Sufficient

In addition to electronic access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an organization's data. These controls include policies, procedures, and control techniques to physically secure computer resources, prevent exploitation of vulnerabilities, and prevent unauthorized changes to system software. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of IRS's information systems and information.

Physical Security

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted, in order to ensure that access continues to be appropriate. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, and locks. The agency has developed and documented policies that identify minimum physical protection measures for facilities used to process, transmit, or store sensitive but unclassified information in support of critical operations and missions. For example, one such IRS policy requires that a facility risk assessment should be performed at least once every 5 years. Inadequate physical security could lead to loss of life and property, disruption of functions and services, and unauthorized disclosure of documents and information.

Although IRS has implemented physical security controls, certain weaknesses reduce the effectiveness of these controls in protecting and controlling physical access to assets at the two sites we reviewed. For example, guards at one site did not always examine IRS-issued photo identification to verify employees' identities as they entered the facility. Failure to check IRS-issued photo identification increases the risk that unauthorized individuals could gain entrance to the facility. However, following our notification of this issue, agency officials took immediate action during our visit to ensure that the security guards always verified each employee's identity against official IRS photo identification.

In addition, IRS has not fully implemented a procedure for periodically reviewing employee access to sensitive areas. Although steps have been taken to implement such a procedure, access to sensitive areas was not being limited to individuals with an ongoing need for that access. Site

officials acknowledged this problem and stated that efforts are under way to correct it.

Further, although IRS policy requires that a facility risk assessment be performed at least once every 5 years, one site's most recent facility risk assessment was conducted about 5 years ago, and agency officials confirmed that an updated assessment was not planned or under way. The lack of a current facility risk assessment hinders IRS's ability to determine the effectiveness and appropriateness of existing safeguards and security guidelines.

Patch Management

Patch management is a critical process that can help alleviate many of the challenges of securing computing systems.[11] As vulnerabilities in a system are discovered, attackers may attempt to exploit them, possibly causing significant damage. Malicious acts can range from defacing Web sites to taking control of entire systems and thereby being able to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations' systems. After a vulnerability is validated, the software vendor may develop and test a patch or workaround. Incident response groups and software vendors issue information updates on the vulnerability and the availability of patches. IRS's patch management policy assigns organizational responsibilities for the patch management process—including the application of countermeasures to mitigate system vulnerabilities if patch testing fails—and requires that patches be kept up to date or that officials otherwise apply for a waiver.

IRS did not consistently install software patches in a timely manner. For example, IRS's installation of critical or high-priority patches through the configuration management process for Windows systems was not timely. Further, several patches—some that had been issued in 2001—had not been applied to certain UNIX servers that we reviewed in 2005. Because IRS had not yet installed the latest patches, servers used for processing financial information and taxpayer data were vulnerable to denial-of-service attacks and to execution of arbitrary code that will allow administrative privileges.

System Change Controls

It is important to ensure that only authorized and fully tested systems are placed in operation. To ensure that changes to systems are necessary, work

[11]For example, see GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO-04-706 (Washington, D.C.: June 2, 2004).

as intended, and do not result in the loss of data or program integrity, such changes should be documented, authorized, tested, and independently reviewed. In addition, according to IRS policy, a security goal of configuration management is to know what changes occur and how they will affect system security.

IRS did not consistently document changes to critical mainframe system files. Changes to key file directories—which could contain program files that can override security controls—were not always logged. Without proper documentation of changes to critical system files, IRS is unable to effectively detect unusual or unauthorized modifications to its systems. This increases the risk that undocumented changes could be made, jeopardizing the security of sensitive information and increasing the likelihood of disruptions to system operations.

Information Security Program Is Not Yet Fully Implemented

A key reason for the information security weaknesses in IRS's financial and tax processing systems was that although the agency has developed and documented policies and procedures, it has not yet fully implemented its information security program to help ensure that effective controls were established and maintained.

FISMA[12] requires agencies to develop, document, and implement an information security program that 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;

[12]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, including those operated or maintained by contractors or others on behalf of the agency, using a risk-based approach to information security management.

- plans for providing adequate information security for networks, facilities, and systems;

- security awareness training to inform personnel—including contractors and other users of information systems—of information security risks and of their responsibilities in complying with agency policies and procedures;

- at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices relating to management, operational, and technical controls of every major information system that is identified in the agencies' inventories;

- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in their information security policies, procedures, or practices;

- procedures for detecting, reporting, and responding to security incidents; and

- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

IRS has made important progress in developing a framework for its information security program. IRS's policy on information technology security requires each of these FISMA elements, and the agency has initiatives under way in each of these areas. Specifically, IRS has established

- a methodology for its general support system certification and accreditation process, including guidance on conducting risk assessments and security test and evaluations, and developing security plans;

- the office of Mission Assurance and Security Services for developing policies and procedures regarding information technology security;

- a policy describing requirements for its security awareness and training program;

- a working group to develop and execute an approach to managing the remedial action tracking and implementation process;

- the Computer Security Incident Response Center for detecting and responding to intrusions and misuse; and
- business resumption plans that address continuity of operations for certain systems.

However, we identified instances in which the information security program had not been fully or consistently implemented for IRS's information systems. In discussions during our review, agency officials recognized that more work is needed to continue to improve their information security program.

Risk Assessments

Identifying and assessing information security risks are essential steps in 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. 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, potential threats, and recommended corrective actions for reducing or eliminating the vulnerabilities identified.

IRS generally identified and assessed information security risks. The six risk assessments that we reviewed were current and documented residual risk assessed, potential threats, and recommended corrective actions for reducing or eliminating the vulnerabilities identified.

Policies and Procedures

Another key element of an effective information security program is to develop 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 implementing guidance for each computing environment. Establishing and documenting security policies is important because they are the primary mechanism 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 should be provided by the security policies and controls.

IRS has developed information security policies, standards, and guidelines that generally provide appropriate guidance to personnel responsible for securing IRS information systems and data. Yet, we noted instances where policies and procedures were inconsistent with federal guidance, incomplete, and not consistently implemented. For example, IRS's policies and procedures did not always include minimum security requirements as outlined in NIST or National Security Agency (NSA) guidance. To illustrate, password standards, such as password age and password history, set in IRS policies are less stringent than those strongly encouraged by NIST guidance, and specific requirements for certain systems, such as use of superuser accounts and configuration of registry keys, do not meet the guidance issued by NSA. In addition, IRS's methodology for the certification and accreditation of their general support systems is incomplete, with several key sections of it missing information or left completely blank. Further, we continue to report that IRS has not consistently implemented policies and procedures contained in the *Law Enforcement Manual* and *Internal Revenue Manual* pertaining to network management, user accounts and passwords, user rights and file permissions, and other information system controls. Without effectively updating these policies to establish appropriate minimum security requirements, ensuring that policies and procedures are complete, and implementing them, IRS has less assurance that their systems and information are sufficiently protected.

Security Plans

The 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 and implement system security plans for major applications and for general support systems, and that these plans address policies and procedures for providing management, operational, and technical controls. Further, NIST guidelines state that when nonmajor applications are bundled with a general support system, the security requirements for each of the nonmajor applications should be included in the general support system's security plan. IRS policy requires that security plans be developed and provides guidance on developing security plans. According to both IRS and NIST guidance, plans should include elements such as security controls currently in place or planned,

the individual responsible for the security of the system, a description of the system and its interconnected environment, and rules of behavior.

The six security plans we reviewed generally included elements such as security controls currently in place or planned, the individual responsible for the security of the system, a description of the system and its interconnected environment, and rules of behavior. However, we identified instances where plans were incomplete. Of the three security plans for general support systems with nonmajor applications that we reviewed, none addressed specific controls for the nonmajor applications nor assigned specific accountability for those controls. TIGTA identified similar issues,[13] and noted that business unit owners of nonmajor applications may rely too heavily on the general support system controls to protect sensitive data. Without complete security plans, IRS cannot ensure that appropriate controls are in place to protect its systems and critical information.

Security Awareness and Training

Another important element of an information security program involves promoting awareness and providing required training so that users understand the system security risks and their role in implementing related policies and controls to mitigate those risks. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees who use computer resources in their day-to-day operations be made aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality, integrity, and availability. FISMA mandates that all federal employees and contractors who use agency information systems be provided with information security awareness training. Further, FISMA requires agency chief information officers (CIO) to ensure that personnel with significant information security responsibilities get specialized training. OMB and NIST also require agencies to implement system-specific security training.

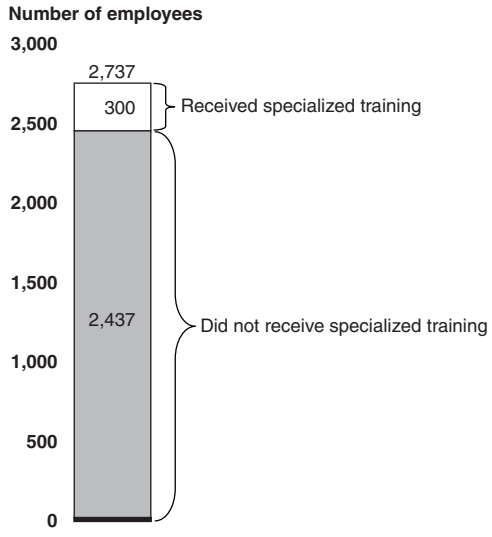
IRS has developed and implemented several methods for notifying employees and contractors of their security-related roles and responsibilities. These methods include specifying security roles and responsibilities in various policy manuals available to employees and contractors, providing security awareness training during new hire

[13]Treasury Inspector General for Tax Administration, *Federal Information Security Management Act Report for Fiscal Year 2005* (Washington, D.C.: Oct. 7, 2005).

orientations, distributing security awareness bulletins and brochures, and creating information security poster boards. As reported by TIGTA in its 2005 FISMA report, security awareness training was provided to all IRS employees and contractors.

Despite the agency's efforts in providing security awareness training, it did not always provide specialized training to individuals with significant information security responsibilities. In its fiscal year 2005 FISMA submission, IRS reported it has 2,737 employees with significant information technology security responsibilities, yet only 300 (11 percent) of those employees received specialized training (see fig. 2).

Figure 2: Status of Specialized Training for IRS Employees with Significant Security Responsibilities



Source: IRS.

IRS did not always provide specialized training for its contractor personnel with information security responsibilities. For example, it did not provide Computer Security Incident Response Center contractors with specialized training. IRS has taken some key steps to address this area, including establishing a working group to improve its training program. Without sufficiently trained security personnel, security lapses are more likely to occur and could contribute to further information security weaknesses.

Tests and Evaluations of Control Effectiveness

Another key element of an information security program is the testing and evaluation of systems to ensure that they are in compliance with security policies and that those policies and controls are both appropriate and effective. 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. Analyzing the results of security reviews provides security specialists and business managers with a means of identifying new problem areas, reassessing the appropriateness of existing controls, and identifying the need for new controls. FISMA requires that the frequency of tests and evaluations be based on risks, but occur no less than annually. Furthermore, IRS policy requires periodic testing and evaluation of the effectiveness of information security policies and procedures.

Although IRS had conducted system tests and evaluations for the three systems we reviewed, its tests did not identify key security vulnerabilities. For example:

- At one of the IRS sites we visited, one system's security test and evaluation report did not identify any vulnerabilities. However, during our review, we identified several vulnerabilities, including unpatched software.

- At the same site, IRS did not detect control deficiencies during its test and evaluation of the mainframe. For example, IRS was not using standardized naming conventions for its datasets and was not logging changes to software on the mainframe. These weaknesses could have been detected and corrected using the results of effective security tests and evaluations.

In addition, in its 2005 FISMA report, TIGTA reported that security tests and evaluations for major applications did not comply with NIST standards. Tests did not include all system components, such as encryption, telecommunication links, and user account management. Without appropriate tests and evaluations, IRS cannot be assured that employees and contractors are complying with established policies or that policies and controls are appropriate and working as intended.

Remedial Actions

Remedial action plans are a key component described in FISMA. They assist agencies in identifying, assessing, prioritizing, and monitoring the progress in correcting security weaknesses that are found in information systems. According to OMB *Circular A-123*, agencies should take timely and effective action to correct deficiencies that they have identified through a variety of information sources. To accomplish this, remedial action plans should be developed for each deficiency, and progress should be tracked for each. IRS policy also requires a process for ensuring remedial action to address any significant deficiencies.

According to TIGTA, IRS has made noteworthy progress in the area of tracking remedial actions. In its 2005 FISMA report, TIGTA reported that it was able to verify that IRS's remedial action plans included weaknesses from various reviews and were tailored to specific applications.

Although IRS had developed remedial plans to address information security weaknesses identified through previous reviews, the plans we reviewed were incomplete. All four remedial plans were missing certain key elements. For example, none of the four plans specified the funds required to correct identified weaknesses. In addition, three of the plans did not identify scheduled completion dates for correcting or mitigating identified weaknesses. Further, the fourth plan was outdated because it included scheduled completion dates that had already passed. For example, weaknesses that were still considered "open" in June 2005 had scheduled completion dates of April 2005. IRS officials explained that the remedial plans were a "work in progress," since the documents were not due to be submitted to OMB until September 2005. However, OMB requires at least quarterly updates of agency remedial plans; therefore, the plan should have been updated during the time of our review. Without complete and current remedial action plans, the agency may not be able to prioritize and monitor progress in correcting security weaknesses.

Incident Handling

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they promptly take steps to detect and respond to them before significant damage can be done. In addition, accounting for and analyzing security problems and incidents are effective ways for organizations to gain a better understanding of threats to their information and of the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be eliminated so that they will not be exploited again. Problem and incident reports can provide valuable input for risk assessments, can help

in prioritizing security improvement efforts, and can be used to illustrate risks and related trends for senior management.

IRS has implemented an incident handling program and established the Computer Security Incident Response Center in 2001. The center's mission is to detect, react, and respond to computer security incidents targeting the IRS enterprise information infrastructure. It provides assistance and guidance in both cyber and physical incident response and uses a centralized approach to incident handling across IRS. The agency has also defined procedures for detecting, responding to, and reporting computer and network security incidents, and has created several detailed incident detection and response procedures outlining the roles and responsibilities of center personnel and event analysis. In 2005, TIGTA reported[14] that the center was effective at preventing, detecting, and responding to computer security incidents, but it recommended further improvements in reporting and documenting remedial actions related to incidents.

Continuity of Operations

Continuity of operations controls, which includes disaster recovery planning, should be designed to ensure that when unexpected events occur, key operations continue without interruption or are promptly resumed, and that critical and sensitive data are protected. These controls include environmental controls and procedures designed to protect information resources and minimize the risk of unplanned interruptions, along with a plan to recover critical operations should interruptions occur. If continuity of operations controls are inadequate, even a relatively minor interruption could result in significant adverse nationwide impact on IRS operations. IRS requires that continuity of operations, or business resumption, plans be included as part of its certification and accreditation process.

Shortcomings in IRS's ability to recover from disruptions due to unexpected events continue to exist. In 2004, we reported that non-IRS staff at an IRS site were not trained to restore operations in the event IRS staff were not available. In addition, in 2005, we reported that the disaster recovery plans we reviewed at an IRS site did not include disaster recovery procedures for its UNIX and Windows systems. Also, the site's business resumption plans did not include UNIX and Windows systems. Although IRS has various initiatives under way to improve continuity of operations, these and other shortcomings still exist. Specifically, IRS has not procured

[14]TIGTA, *The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made*, 2005-20-143 (September 2005).

and installed UNIX-based hardware and equipment for processing applications and data at its disaster recovery hot-site—an alternate processing location that can be used in case of an emergency. Further, in 2005, the agency reported that they had tested contingency plans for only 36 percent of its systems. Until the agency completes actions to address these weaknesses, it is at risk of not being able to appropriately recover in a timely manner from certain service disruptions.

Conclusions

IRS has made progress in correcting or mitigating previously reported weaknesses and in implementing controls over key financial and tax processing systems. However, information security weaknesses—both old and new—continue to impair its ability to ensure the confidentiality, integrity, and availability of financial and other sensitive data. A key reason for these weaknesses is that IRS has not yet fully implemented critical elements of its information security program, although it has developed a solid framework. Until IRS fully implements a comprehensive agencywide information security program that includes enhanced policies, procedures, plans, training, and continuity of operations, its facilities and computing resources and the information that is processed, stored, and transmitted on its systems will remain vulnerable.

Recommendations for Executive Action

To help establish effective information security over key financial systems, data, and interconnected networks, we recommend that you take the following five actions to implement an information security program:

- enhance policies and procedures related to password age and configuration settings to comply with federal guidelines;
- review system security plans to ensure that they appropriately address nonmajor applications;
- ensure contractors with significant information security responsibilities are provided with sufficient specialized training;
- ensure that remedial action plans are complete and up to date; and
- continue to enhance continuity of operations capabilities by
    - training non-IRS staff to restore operations,

- updating disaster recovery plans to include disaster recovery procedures for UNIX and Windows systems,
- updating business resumption plans to include UNIX and Windows systems, and
- installing UNIX-based hardware and equipment for processing applications and data at IRS's disaster recovery hot-site.

We are also making recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses we identified that are related to network management, user accounts and passwords, user rights and file permissions, audit and monitoring of security-related events, physical security, and patch management at the two sites we visited.

Agency Comments

In providing written comments (reprinted in app. I) on a draft of this report, the Commissioner of Internal Revenue acknowledged that IRS needs to continue to implement a comprehensive agencywide security program, and agreed to implement the five recommendations in this report. He said that efforts are under way to remedy weaknesses and will continue until all recommendations have been addressed.

The Commissioner also said that IRS is taking an agencywide approach to address the root cause of the weaknesses we identified. He also stated that many weaknesses have been corrected and additional controls have been implemented. Further, he said that IRS is continuing its aggressive initiative to complete required security activities at each of the computing centers. These activities include the development of security plans, security documentation, and security testing.

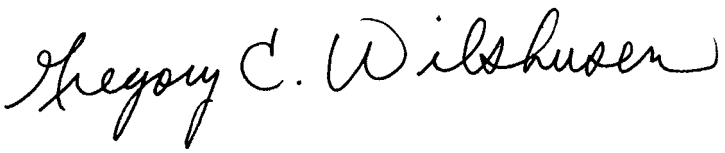
This report contains recommendations to you. As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Government Reform 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

Comments from the Commissioner of Internal Revenue

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

COMMISSIONER

February 27, 2006

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

Dear Mr. Wilshusen:

I am writing to provide the Internal Revenue Service's comments on the draft Government Accountability Office (GAO) report, *Information Security: Continued Progress Needed to Strengthen Controls at the Internal Revenue Service (GAO-06-328)*.

We agree the IRS needs to continue to implement a comprehensive agency-wide information security program, and we agree to implement the five recommendations contained in the report. Efforts to remedy these weaknesses are currently underway and will continue until all recommendations have been addressed. We will provide you with a detailed corrective action plan in the near future.

Thank you for recognizing the IRS has made progress in implementing more effective information security controls over key financial and tax processing systems. The report indicates the IRS has corrected or mitigated 41 of the 81 specific technical weaknesses GAO reported as unresolved at the time of your last review. Because the IRS's solution extends beyond the specific findings and addresses the root cause of the weaknesses at an enterprise-wide level, a majority of the weaknesses remain open. However, as a result of this agency-wide approach and other initiatives we have underway, the IRS now has stronger controls to protect taxpayer data.

As discussed in Treasury's response to the previous GAO report, *Information Security: Internal Revenue Service Needs to Remedy Serious Weaknesses Over Taxpayer and Bank Secrecy Act Data (GAO-05-482)* dated April 2005, all senior officials at the IRS share the responsibility for information technology security. In response to that report, the Chief Information Officer and the Chief of Mission Assurance and Security Services are collaborating with executives throughout the IRS to ensure security policies, standards, and procedures are being followed enterprise-wide.

The IRS continues to make progress in addressing computer security deficiencies throughout the Service. Many weaknesses have been corrected and additional controls have been implemented. The IRS has continued the extremely aggressive initiative it

began in 2004 to complete the full suite of required security activities at each of its computing centers and campuses and to support security certification and accreditation. This is being accomplished using the latest processes and guidance specified by the National Institute for Standards and Technology and in accordance with the requirements of the Federal Information Security Management Act. The security activities include the development of security plans, security documentation, and security testing.

We are aware that effective information security controls are essential for ensuring information is adequately protected from inadvertent or deliberate misuse, disruption, or destruction. The IRS takes security and privacy responsibilities very seriously.

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 W. Todd Grams, Chief Information Officer, at (202) 622-6800, or Daniel Galik, Chief of Mission Assurance and Security Services, at (202) 622-8910.

Sincerely,

Mark W. Everson

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, Edward Alexander Jr., Gerald Barnes, Bruce Cain, Mark Canter, Nicole Carpenter, Jason Carroll, Lon Chin, Kirk Daubenspeck, Neil Doherty, Patrick Dugan, Denise Fitzpatrick, Edward Glagola Jr., Nancy Glover, David Hayes, Franklin Jackson, Myong Suk Kim, Jeffrey Knott, Mary Marshall, Leena Mathew, Kevin Metcalfe, Duc Ngo, Tracy Pierson, Henry Sutanto, 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