United States Government Accountability Office

GAO

Report to the Commissioner of Internal Revenue

March 2010

INFORMATION SECURITY

IRS Needs to Continue to Address Significant Weaknesses

GAO-10-355

G A O
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-10-355, a report to the Commissioner of Internal Revenue

Why GAO Did This Study

The Internal Revenue Service (IRS) relies extensively on computerized systems to carry out its demanding responsibilities to collect taxes, process tax returns, and enforce the nation's tax laws. Effective information security controls are essential to protect financial and taxpayer information from inadvertent or deliberate misuse, improper disclosure, or destruction.

As part of its audit of IRS's fiscal years 2009 and 2008 financial statements, GAO assessed (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses 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. To do this, GAO examined IRS information security policies, plans, and procedures; tested controls over key financial applications; and interviewed key agency officials at six sites.

What GAO Recommends

GAO is recommending that IRS take four actions towards fully implementing its agencywide information security program. In a separate report with limited distribution, GAO recommends 23 specific actions for IRS to take in correcting newly identified control weaknesses. In commenting on a draft of this report, IRS agreed to develop a detailed corrective action plan addressing each of the recommendations.

View GAO-10-355 or key components.
For more information, contact Nancy Kingsbury at (202) 512-2700 or kingsburyn@gao.gov or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

March 2010

INFORMATION SECURITY

IRS Needs to Continue to Address Significant Weaknesses

What GAO Found

IRS has continued to make progress during fiscal year 2009 in correcting previously reported information security weaknesses that GAO reported as unresolved at the conclusion of its fiscal year 2008 audit. Specifically, IRS has corrected or mitigated 28 of the 89 weaknesses and deficiencies—21 of 74 previously identified information security control weaknesses and 7 of 15 previously identified program deficiencies. For example, it has

- changed vendor-supplied user accounts and passwords;
- avoided storing clear-text passwords in scripts;
- enhanced its policies and procedures for configuring mainframe operations; and
- established an alternate processing site for its procurement system.

While IRS has corrected 28 control weaknesses and program deficiencies, 61 of them—or about 69 percent—remain unresolved or unmitigated. For example, IRS continued to install patches in an untimely manner and used passwords that were not complex. In addition, IRS did not always verify that remedial actions were implemented or effectively mitigated the security weaknesses. According to IRS officials, they continued to address uncorrected weaknesses and, subsequent to GAO's site visits, had completed additional corrective actions on some of them.

Despite these actions, newly identified and the unresolved information security control weaknesses in key financial and tax processing systems continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. IRS did not consistently implement controls that were intended to prevent, limit, and detect unauthorized access to its systems and information. For example, IRS did not always (1) enforce strong password management for properly identifying and authenticating users; (2) authorize user access to permit only the access needed to perform job functions; (3) log and monitor security events on a key system; and (4) physically protect its computer resources. A key reason for these weaknesses is that IRS has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. Although IRS has made important progress in developing and documenting its information security program, it did not, among other things, review risk assessments at least annually for certain systems or ensure contractors receive awareness training. Until these control weaknesses and program deficiencies are corrected, the agency remains unnecessarily vulnerable to insider threats related to the unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as the disruption of system operations and services. The new and unresolved weaknesses and deficiencies are the basis for GAO's determination that IRS had a material weakness in internal controls over financial reporting related to information security in fiscal year 2009.

Contents

Abbreviations

CSIRC	Computer Security Incident Response Center
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 19, 2010

The Honorable Douglas Shulman
Commissioner of Internal Revenue

Dear Commissioner Shulman:

The Internal Revenue Service (IRS) has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. It relies extensively on computerized systems to support its financial and mission-related operations. Effective information system controls are essential for protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer information and ensuring that information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of our audit of IRS's fiscal years 2009 and 2008 financial statements,[1] we assessed the effectiveness of the agency's information security controls[2] over key financial and tax processing systems, information, and interconnected networks at six locations. These systems support the processing, storage, and transmission of financial and sensitive taxpayer information. In our report on IRS's fiscal years 2009 and 2008 financial statements, we reported that the new information security deficiencies we identified in fiscal year 2009 and the unresolved deficiencies from prior audits represent a material weakness[3] in internal controls over financial reporting related to information security.

[1] GAO, *Financial Audit: IRS's Fiscal Years 2009 and 2008 Financial Statements*, GAO-10-176 (Washington, D.C.: Nov. 10, 2009).

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

[3] A material weakness is a deficiency, or a combination of deficiencies, in internal controls such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

We assessed (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses 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. To do this, we examined IRS information security policies, plans, and procedures; tested controls over key financial applications; and interviewed key agency officials. We concentrated our evaluation primarily on threats emanating from sources internal to IRS's computer networks. We conducted this performance audit from April 2009 to March 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. For additional information about our objectives, scope, and methodology, refer to appendix I.

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 maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have revolutionized the way our government, our nation, and much of the world communicates and conducts business. Although this expansion has created many benefits for agencies such as IRS in achieving their missions and providing information to the public, it also exposes federal networks and systems to various threats.

Without proper safeguards, computer systems are vulnerable to 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. The risk to these systems 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. The Federal Bureau of Investigation has identified multiple sources of threats, including foreign nation states engaged in intelligence gathering and information warfare, domestic criminals, hackers, virus writers, and disgruntled employees or contractors working within an organization. In addition, the U.S. Secret Service and the CERT® Coordination Center[4] studied insider threats in the government sector and stated in a January 2008 report that "government sector insiders have the potential to pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases."

Our previous reports, and those by federal inspectors general, describe persistent information security weaknesses that place federal agencies, including IRS, at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, we have designated information security as a governmentwide high-risk area since 1997, most recently in 2009.[5]

Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002[6] to strengthen the security of information and systems within federal agencies. FISMA requires each agency to develop, document, and implement an agencywide information security program for the information and information systems that support the operations and assets of the agency, using a risk-based approach to information security management. Such a program includes assessing risk; developing and implementing cost-effective security plans, policies, and procedures; providing specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; and ensuring continuity of operations.

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

[5] GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

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

IRS Has Demanding Responsibilities as the United States' Tax Collector

IRS has demanding responsibilities in collecting taxes, processing tax returns, and enforcing the federal tax laws, and relies extensively on computerized systems to support its financial and mission-related operations. In fiscal years 2009 and 2008, IRS collected about $2.3 trillion and $2.7 trillion, respectively, in tax payments, processed hundreds of millions of tax and information returns, and paid about $438 billion and $426 billion, respectively, in refunds to taxpayers. Further, the size and complexity of IRS add unique operational challenges. The agency employs tens of thousands of people in its Washington, D.C. headquarters, 10 service center campuses, 3 enterprise computing centers, as well as 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. Protecting the confidentiality of this sensitive information is paramount; 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, integrity and availability of the information and information systems that support the agency and its operations. FISMA requires the Chief Information Officer or comparable official at federal agencies to be responsible for developing and maintaining an information security program. IRS has delegated this responsibility to the Associate Chief Information Officer for Cybersecurity, who heads the Office of Cybersecurity. This group is responsible for ensuring IRS's compliance with federal laws, policies and guidelines governing measures to assure the confidentiality, integrity, and availability of IRS electronic systems, services and data. It manages IRS's information security program, including activities associated with identifying, mitigating, and monitoring cybersecurity threats; determining strategy and priorities; and monitoring security program implementation. Within the Office of Cybersecurity, the Computer Security Incident Response Center (CSIRC) is tasked with preventing, detecting, and responding to computer security incidents targeting IRS's information technology enterprise. IRS develops and publishes its information security policies, guidelines, standards and procedures in the *Internal Revenue Manual* and other documents in order for IRS divisions and offices to carry out their respective responsibilities in information security.

IRS Has Made Progress in Correcting Previously Reported Weaknesses

During fiscal year 2009, IRS has made progress toward correcting previously reported information security control weaknesses and information security program deficiencies at its three computing centers, another facility, and enterprisewide. IRS had corrected or mitigated 28 of the 89 previously identified weaknesses and deficiencies that were unresolved at the end of our prior audit. This includes 21 of 74 control weaknesses and 7 of 15 program deficiencies. To illustrate, IRS corrected weaknesses related to user identification and authentication and physical access, among others. For example, it has

- changed vendor-supplied user accounts and passwords,
- avoided storing clear-text passwords in scripts,
- deactivated proximity cards for separated employees in a timely manner, and
- ensured that security guards follow established procedures and screen packages and briefcases for prohibited items.

In addition, IRS has improved aspects of its information security program. For example, IRS has enhanced its policies and procedures for configuring mainframe operations and established an alternate processing site for its procurement system.

IRS has also continued to take other actions to improve information security. The agency is in the process of implementing a comprehensive plan to address numerous information security weaknesses, such as those associated with network and system access, audit trails, system software configuration, and contingency planning. According to the plan, the last of these weaknesses is scheduled to be resolved in the first quarter of fiscal year 2014. Further, for fiscal year 2010, IRS has targeted initiatives to improve information security controls in areas such as identity and access management, auditing and monitoring, and disaster recovery. These efforts, if fully and effectively implemented, are positive steps towards improving the agency's overall information security posture.

Nonetheless, of the previously identified security weaknesses and program deficiencies reported as unresolved at the completion of our prior year's audit, 61 of them—or about 69 percent—remain unresolved or unmitigated. For example, IRS continues to

- use passwords that are not complex,
- ineffectively remove application accounts in a timely manner for separated employees,
- allow personnel excessive file and directory permissions,
- allow the unencrypted transmission of user and administrator login information,
- install patches in an untimely manner,
- ineffectively verify that remedial actions are complete, and
- not always annually review risk assessments.

As a result, IRS is at increased risk of unauthorized disclosure, modification, or destruction of financial and taxpayer information.

Weaknesses Placed Financial and Taxpayer Information at Risk

Although IRS has continued to make progress toward correcting previously reported information security weaknesses at its three computing centers, another facility, and enterprisewide, many deficiencies remain. These deficiencies, and new weaknesses identified during this year's audit, relate to access controls, configuration management, and segregation of duties. A key reason for these weaknesses is that IRS has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. These weaknesses—both old and new—continue to jeopardize the confidentiality, integrity, and availability of IRS's systems and were the basis of our determination that IRS had a material weakness in internal controls over financial reporting related to information security in fiscal year 2009.[7]

IRS Did Not Fully Implement Access Controls

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.

[7] GAO-10-176.

Inadequate access controls potentially 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. However, IRS did not fully implement effective controls in these areas.

Weaknesses Exist in Controls for 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. 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. According to the *Internal Revenue Manual*, maximum password age should be 60 days for administrator accounts and strong passwords for authentication to IRS systems should be enforced. In addition, the *Internal Revenue Manual* states that passwords should be protected from unauthorized disclosure and modification when stored and transmitted.

IRS did not always enforce strong identification and authentication controls. For example, administrator passwords for two servers located at one center were not set to comply with IRS's password age policy. In both instances the administrator password age was set to 118 days, which exceeded IRS's requirement by 58 days. Consequently, an increased risk exists that compromised administrator passwords will be used by unauthorized individuals for a longer period of time to gain unauthorized access to server resources. In addition, IRS employees continued to use weak passwords for UNIX systems at two centers and stored clear text passwords in computer program scripts at another center. Further, IRS did not sufficiently protect passwords during transmission. For example, IRS implemented weak authentication protocols[8] for network logons. Ten servers, including domain controllers, located at five sites, were

[8] An authentication protocol is a message exchange process that verifies possession of a token for remote authentication. Some authentication protocols also provide encryption to protect a message exchange so that the data transferred is cryptographically protected.

configured to accept an authentication protocol that was vulnerable to widely published attacks for obtaining user passwords. As a result, increased risk exists that malicious individuals could capture user passwords and use them to gain unauthorized access to IRS systems.

Users Have More System Access Than Needed to Perform Their Jobs

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying 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 they need to perform their official duties. To restrict legitimate users’ access to only those programs and files 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 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’s manual states that the configuration and use of system utilities are based on least privilege and are limited to those individuals that require them to perform their assigned functions.

IRS permitted excessive access to systems and files by granting rights and permissions that gave users more access than they needed to perform their assigned functions. For example, about 120 IRS employees had access to key documents, including cost data for input to its administrative accounting system and a critical process-control spreadsheet used in IRS’s cost allocation process. However, fewer than 10 employees needed this access to perform their jobs. The large number of employees with access to these documents increases the chances that they may intentionally or unintentionally corrupt the data in these documents, which could result in incorrect input and data processing, thus jeopardizing the accuracy of the cost allocation output and, ultimately the information presented in IRS’s annual financial statements. In addition, accounts on three servers supporting the accounting system and used for data transfer at two centers, were given remote login access, which was not needed for these types of accounts and reduces IRS’s ability to control access to the servers. Further, IRS had not corrected previously reported weaknesses related to not restricting users’ ability to bypass application controls for its procurement system and allowing excessive access to server shares that contained sensitive information. As a result, increased risk exists that unauthorized users will gain access to sensitive information or circumvent security controls.

Sensitive Data Is Sent Across the IRS Network Unencrypted

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption. 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. The *Internal Revenue Manual* 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.

IRS configured routers to use protocols that allow unencrypted transmission of sensitive information. For example, 18 routers we reviewed at the three computing centers used a protocol that was configured to authenticate information using plain text. In addition, IRS did not use encryption for routing table[9] messages for six routers we reviewed at two of the centers. Enabling encryption on routing table messages helps to prevent someone from purposely or accidentally adding an unauthorized router to the network and either corrupting routing tables or launching a denial of service attack. Further, IRS had not corrected a previously identified weakness related to encrypting administrator login data to a key application. By not encrypting these data, IRS is at increased risk that an unauthorized individual could view and then use the data to gain unwarranted access to its system and/or sensitive information.

IRS Did Not Always Log and Monitor Security Events

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to know 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*

[9] The routing table routes messages to their destination.

Revenue Manual requires that audit records be created, protected, and retained to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. In addition, the manual also states that the IRS shall monitor its networks for security events.

IRS did not always log and monitor important security events on its systems. For example, IRS did not have event logging enabled for an application that supports its procurement system. In addition, although IRS's CSIRC was successful in logging most security events, it did not monitor activity on all critical ports.[10] By not logging and monitoring system activities, IRS has limited assurance that it will be able to detect security-relevant events that could adversely affect operations.

IRS Restricted Physical Access, But Certain Controls Were Not Effectively Implemented

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. The *Internal Revenue Manual* requires department managers of restricted areas to review, validate, sign, and date monthly, the authorized access list for restricted areas and then forward the list to the physical security office for review of employee access. The manual also requires that users activate the password-protected screen saver or lock their workstation when leaving the machine unattended.

Although IRS had implemented numerous physical security controls, certain controls were not working as intended, such as the following:

- Department managers did not always validate and sign access lists within the required month timeframe. We have previously reported this weakness and recommended that managers sign and date authorized access lists for restricted areas.

[10] A port can be either a physical location for connecting a computer or other telecommunication device to some other device, or a logical connection in which a client program specified a server program in a network. In this case, port refers to a logical connection.

- The physical security office at one center did not promptly remove access to restricted areas for 5 out of 15 employees after managers requested their removal. Specifically, 4 employees whose managers marked their name for removal from the authorized access lists between March and June 2009, still had access as of July 2009. A fifth employee was removed 2 months after department managers noted the employee for removal from the access list.

- Two of five consoles that were part of the operating environment for a key system were not locked with password-protected screen savers while they were left unattended, which could have allowed unauthorized access to this system used for accessing taxpayer information.

Because employees still had unnecessary access to restricted areas and computers in the restricted areas were not always secured when left unattended, IRS has reduced assurance that computing resources and taxpayer information are adequately protected from unauthorized access.

Weaknesses in Other Information Security Controls Increase Risk

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

Outdated and Unsupported Software Exposes IRS to Known Vulnerabilities

Configuration management involves, among other things, (1) verifying the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) obtaining reasonable assurance that systems are configured and operating securely and as intended. Patch management is an important element in mitigating the risks associated with software vulnerabilities. When software vulnerabilities are discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. Outdated and unsupported software are more vulnerable to attacks and exploitation because vendors no longer provide updates, including security updates. Accordingly, the *Internal Revenue Manual* states that system administrators will ensure the operating system version is a version for which the vendor still offers standardized technical support.

IRS was running outdated and unsupported software, exposing servers to known vulnerabilities. For example, the operating system software supporting the administrative accounting system reached its "end of service" life[11] on March 31, 2009. As a result, IRS may receive limited or no vendor maintenance support, including security patches, thus increasing the risk that known information security vulnerabilities may be exploited. In addition, IRS used outdated and unsupported software on the five critical servers we reviewed at two centers, exposing the organization to a vulnerability that could allow a malicious user to capture user IDs and passwords by re-directing internal users' access requests to other systems without their knowledge.

Incompatible Duties Were Not Always Segregated

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

IRS did not always segregate incompatible duties. Specifically, IRS permitted an individual to hold and execute the roles and responsibilities of both a database and system administrator for the procurement system. By not properly segregating incompatible duties, IRS may have an increased risk that improper program changes could be intentionally or inadvertently implemented. Subsequent to our site visit, IRS informed us

[11] A vendor will typically make support available to a buyer for a number of years after the product is shipped. However, after the product has reached its "end of service" life, the buyer will not receive patches, including security patches, unless it purchases additional services.

that it had corrected this weakness. However, we have not yet evaluated the action taken.

IRS Has Not Fully Implemented All Elements of Its Information Security Program

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 magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems;
- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security policies, procedures, or practices; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

IRS has made important progress in developing and documenting elements of its information security program. However, not all components of its program have been fully implemented.

Risk Assessment Process Is Implemented, but Assessments Are Still Not Always Reviewed Annually

According to the National Institute of Standards and Technology (NIST), risk is determined by identifying potential threats to the organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data. Identifying and assessing information security risks are essential to determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that these policies and controls operate as intended. Consistent with NIST guidance, IRS requires its risk assessment process to detail the residual risk[12] assessed, as well as potential threats, and to recommend corrective actions for reducing or eliminating the vulnerabilities identified. The *Internal Revenue Manual* also requires system risk assessments be reviewed annually.

IRS had implemented a documented methodology for conducting risk assessments that includes threat and vulnerability identification, impact analysis, risk determination, and recommended corrective actions. The risk assessments for the six systems we reviewed included the identification of threats and vulnerabilities. The assessments also included impact analysis, risk determination, and recommended corrective actions for mitigating or eliminating the threats and vulnerabilities that were identified. However, IRS officials indicated that they had not corrected a weakness we previously reported regarding not annually reviewing system risk assessments. Until IRS annually reviews such assessments, potential risks to these systems and the adequacy of their security controls to reduce risk may be unknown.

Policies and Procedures Were Not Always Comprehensive or Documented

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 associated with unauthorized access or disruption of services. Technical security standards can provide consistent implementation guidance for each computing environment. Developing, documenting, and implementing security policies are the important primary mechanisms by which management communicates its views and requirements; these policies also serve as the basis for adopting specific

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

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 had 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 for securing network devices or informing CSIRC of network changes. For example, IRS policy lacked specific guidance on how to more securely configure routers to encrypt network traffic and help protect the network from denial of service, spoofing, and man-in-the-middle attacks.[13] In addition, IRS did not have guidance on how to configure network switches to defend against certain attacks that could crash an entire network or network segment. Further, IRS had not developed and implemented procedures for notifying CSIRC of changes that would affect the center's ability to detect unauthorized access. For example, IRS instructed administrators to change a certain port from the default port number to a lesser known port number. However, according to an IRS official, administrators were never instructed to inform CSIRC of the change, and therefore, the new port number was not being monitored. As a result, IRS's ability to detect unauthorized access and trace or recreate events was diminished.

Security Plans Adequately Documented Management, Operational, and Technical Controls

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. The Office of Management and Budget's (OMB) Circular A-130 requires that agencies develop system security plans for major applications and general support systems, and that these plans address policies and procedures for providing management, operational, and technical controls. Furthermore, the *Internal Revenue Manual* requires that security plans be developed,

[13] Denial of service is a method of attack that denies system access to legitimate users without actually having to compromise the targeted system. It can also prevent one system from being able to exchange data with other systems. Spoofing involves the ability to receive a message by masquerading as the legitimate destination or masquerading as the sending machine and sending a message to a destination. A man-in-the-middle attack is an attack where an attacker is positioned between two parties in order to intercept and alter data traveling between them.

documented, implemented, and periodically updated for the controls in place or planned for an information system.

IRS had developed, documented, and updated the plans for six systems we reviewed. Furthermore, those plans documented the management, operational, and technical controls in place and included information required per OMB Circular A-130 for applications and general support systems.

Security Awareness Training Was Not Always Provided to Contractors

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 sufficient training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks. IRS's manual requires that all system users, including contractors, receive security awareness training within the first 10 working days.

Although IRS provided security awareness training to new employees as part of its new hire orientation process, IRS did not always provide security awareness training to its contractors. We reviewed training documentation for five contractors newly assigned between January and May 2009, and found that four of them had not received any security awareness training as required. As a result, IRS has less assurance that contractors are aware of the information security risks and responsibilities associated with their activities.

Although Controls Were Tested and Evaluated, Test Results Were Not Always Clearly Documented or Effectively Reviewed

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

Although IRS had tested and evaluated the six systems we reviewed, the test results were not always clearly documented or thoroughly reviewed. IRS has developed a process to test and evaluate their applications on a yearly basis. However, several tests were labeled "pass" based on draft documents or actions that would be completed in the future, and several other tests did not address the entire documented control. In addition, according to IRS, there were a few instances where the tester misinterpreted the control or did not include enough detail in the test results to conclude on whether a control was effective or not. Further, the results of these tests were not effectively reviewed. Although a review and approval was indicated, these shortcomings would have likely been identified had the review been effective. As a result, IRS has limited assurance that controls over its systems are being effectively implemented and maintained.

System Remedial Action Plans Were Complete, but Corrective Actions Were Not Effectively Validated

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

Although remedial action plans were in place, corrective actions were not always appropriately verified. IRS had developed system-specific remedial action plans for six systems and also developed and implemented a remedial action process to address deficiencies in its information security policies, procedures, and practices. However, the verification process used to determine whether remedial actions were implemented was not always effective. To illustrate, IRS informed us that they had corrected 42 of the 89 previously reported weaknesses. However, our tests determined that IRS had not fully implemented the remedial actions it reported for 14 weaknesses that it considered corrected. These weaknesses had not been effectively mitigated. We have previously reported a similar weakness and recommended that IRS revise its remedial action verification process to ensure actions are fully implemented, but the condition continued to exist.

Until IRS takes additional steps to fully implement our previous recommendation of improving its remedial action process, it will have limited assurance that weaknesses are being properly corrected and that controls are operating effectively.

Although Contingency Plans were Tested and Updated, IRS Could Not Readily Locate a Critical Recovery Document for its Administrative Accounting System

Continuity of operations planning, which includes developing and testing contingency plans and disaster recovery plans, is a critical component of information protection. To ensure that mission-critical operations continue, organizations develop the ability to detect, mitigate, and recover from service disruptions while preserving access to vital information. In developing this ability, organizations prepare plans that are to be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. In addition, system documentation and operating procedures should be available to adequately provide for recovery and reconstitution of information systems to its original state after a disruption or failure. IRS's manual requires, among other things, that contingency plans be reviewed and tested at least annually and that individuals with responsibility for disaster recovery be provided copies of or access to application disaster recovery plans.

Although contingency plans were tested for the six systems we reviewed, IRS could not readily locate a critical disaster recovery document. Specifically, IRS could not provide, in a timely manner, the appropriate contact or the location of the keystroke manual with the application recovery steps. A keystroke manual provides detailed step-by-step instructions, including keystroke-by-keystroke details, used by individuals with responsibility for disaster recovery to fully recover an application from a significant event. Without a contact and appropriate access to the manual, increased risk exists that IRS could be unable to restore its administrative accounting system to its full operational status after a major disruption.

Conclusions

IRS has made progress in correcting or mitigating previously reported weaknesses, implementing controls over key financial systems, and developing and documenting a framework for its agencywide information security program. IRS also has targeted initiatives covering identity and access management, auditing and monitoring, and disaster recovery for fiscal year 2010. 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 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 certain elements of its agencywide information security program. The financial and taxpayer information on IRS systems will remain particularly vulnerable to insider threats until the agency (1) begins to address and correct prior weaknesses across the service and (2) fully implements a comprehensive agencywide information security program that ensures policies and procedures are appropriately specific, contractors receive security awareness training, tests and evaluations are effectively documented and reviewed, and key documents are readily available to support disaster recovery. Until IRS takes these steps, financial and taxpayer information are at increased risk of unauthorized disclosure, modification, or destruction, and the agency's management decisions may be based on unreliable or inaccurate financial information.

Recommendations for Executive Action

In addition to implementing our previous recommendations, we recommend that you take the following four actions to fully implement an agencywide information security program:

- Develop and implement policies and procedures for more securely configuring routers to encrypt network traffic, configuring switches to defend against attacks that could crash the network, and for notifying CSIRC of network changes that could affect its ability to detect unauthorized access.
- Ensure contractors receive security awareness training within the first 10 working days.
- Ensure the results of testing and evaluating controls are effectively documented and reviewed.
- Ensure key disaster recovery documentation, such as keystroke manuals, are available in a timely manner, and appropriate contacts are readily identified.

We are also making 23 detailed recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct specific information security weaknesses related to access controls, configuration management and segregation of duties identified during this audit.

Agency Comments

In providing written comments (reprinted in app. II) on a draft of this report, the Commissioner of Internal Revenue stated that he appreciated that the draft report recognized the progress IRS has made in improving its information security program, and that the security and privacy of taxpayer and financial information is of the utmost importance to the agency. He also noted that IRS is committed to securing its computer environment and will continually evaluate processes, promote user awareness, and apply innovative ideas to increase compliance. Further, he stated that IRS will develop a detailed corrective action plan addressing each of our recommendations.

This report contains recommendations to you. As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform not later than 60 days from the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report. Because agency personnel serve as the primary source of information on the status of recommendations, GAO requests that the agency also provide us 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, the Secretary of the Treasury, and the Treasury Inspector General for Tax Administration. The report also is available at no charge on the GAO Web site at http://www.gao.gov.

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

Sincerely yours,

Nancy R. Kingsbury

Nancy R. Kingsbury
Managing Director, Applied Research and Methods

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to determine (1) the status of the Internal Revenue Service's (IRS) actions to correct or mitigate previously reported information security weaknesses and (2) whether controls over key financial and tax processing systems were effective in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer information. This work was performed in connection with our audit of IRS's financial statements for the purpose of supporting our opinion on internal controls over the preparation of those statements.

To determine the status of IRS's actions to correct or mitigate previously reported information security weaknesses, we reviewed our prior reports to identify previously reported weaknesses and examined IRS's corrective action plans to determine which weaknesses IRS reported corrective actions as being completed as of April 30, 2009. For those instances where IRS reported it had completed corrective actions, we assessed the effectiveness of those actions by, for example:

- reviewing databases to determine if vendor-supplied accounts and passwords were changed;
- examining scripts to determine if they contained clear text passwords;
- analyzing system registry keys to determine whether access was properly controlled, and that they were configured properly;
- examining application accounts to determine whether the accounts of separated employees had been removed in a timely manner;
- observing data transmissions across the network to determine whether sensitive data was being encrypted;
- reviewing physical access to determine if proximity cards for separated employees was deactivated in a timely manner and whether managers were periodically evaluating employees' access for restricted areas;
- observing security guards to determine whether procedures for screening packages and briefcases were followed;
- examining system software to determine if it was patched in a timely manner; and
- reviewing mainframe policies and procedures to determine if they provide the necessary detail for controlling and logging changes.

We evaluated IRS's implementation of these corrective actions for the Enterprise Computing Centers in Detroit, Martinsburg, and Memphis, and an additional facility in Oxon Hill, Maryland.

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

Our evaluation was based on 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; National Security Agency guidance; and IRS's policies and procedures. We evaluated controls by

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

- analyzing users' system access to determine whether they had more permissions than necessary to perform their assigned functions;

- observing physical access controls to determine if computer facilities and resources were being protected;

- inspecting key servers to determine whether critical patches had been installed or software was up-to-date;

- examining user access and responsibilities to determine whether incompatible functions were segregated among different individuals; and

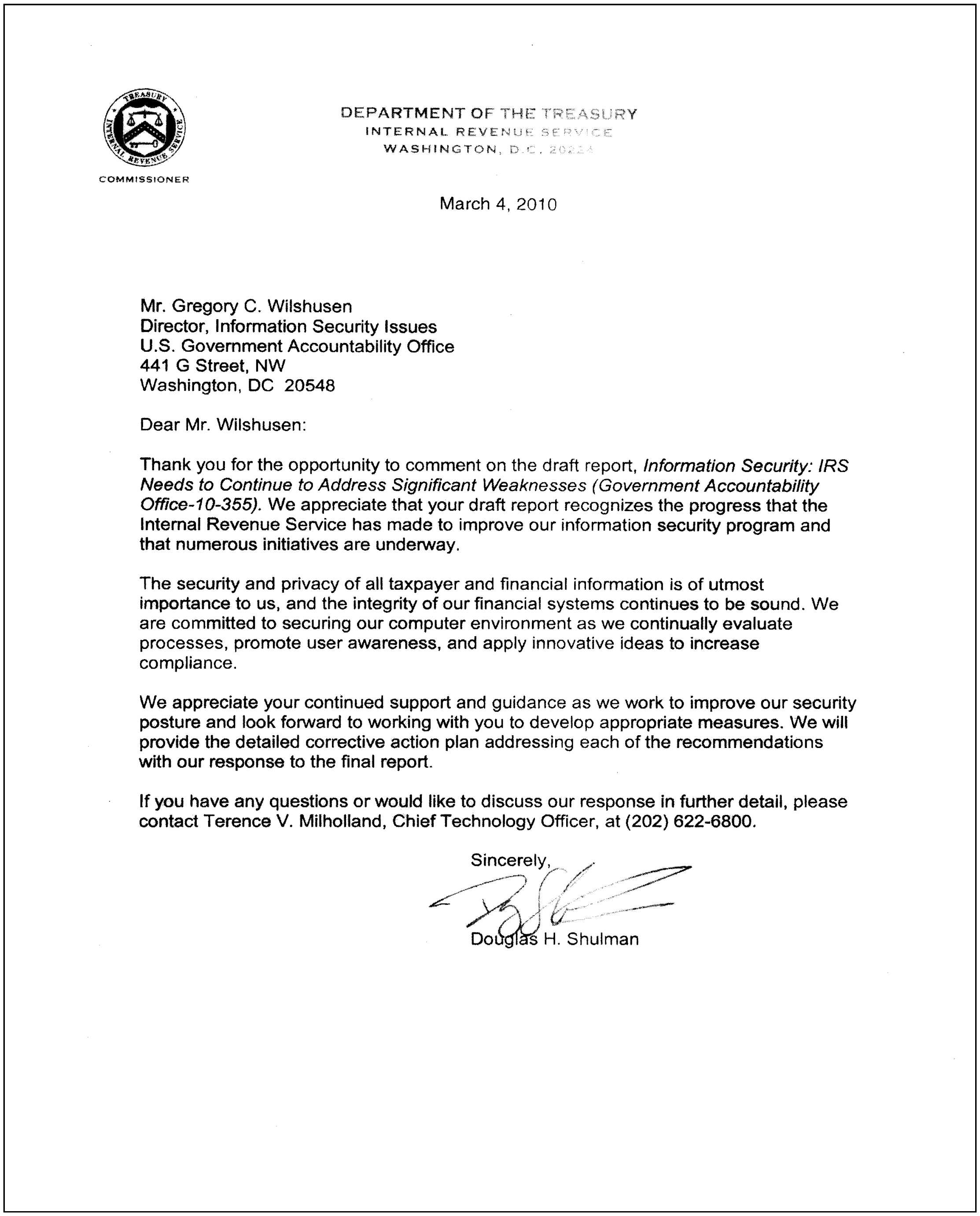
- reviewing system back up and recovery procedures to determine if they adequately provide for recovery and reconstitution to the system's original state after a disruption or failure.

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

- analyzing IRS's risk assessment process and risk assessments for six IRS financial and tax processing systems which are key to supporting the agency's financial statements, to determine whether risks and threats were documented;
- comparing IRS's policies, procedures, practices, and standards to actions taken by IRS personnel to determine whether sufficient guidance was provided to personnel responsible for securing information and information systems;
- analyzing security plans for six systems to determine if management, operational, and technical controls were documented and if security plans were updated;
- examining the security awareness training process for employees and contractors to determine if they received system security orientation within the first 10 working days;
- analyzing test plans and test results for six IRS systems to determine whether management, operational, and technical controls were tested at least annually and based on risk;
- reviewing IRS's system remedial actions plans to determine if they were complete, and reviewing IRS's actions to correct weaknesses to determine if they effectively mitigated or resolved the vulnerability or control deficiency; and
- examining contingency plans for six IRS systems to determine whether those plans had been tested or updated.

We also reviewed or analyzed our previous reports. In addition, we discussed with management officials and key security representatives, such as those from IRS's Computer Security Incident Response Center, whether information security controls were in place, adequately designed, and operating effectively.

Appendix II: Comments from the Internal Revenue Service



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

COMMISSIONER

March 4, 2010

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

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report, *Information Security: IRS Needs to Continue to Address Significant Weaknesses (Government Accountability Office-10-355).* We appreciate that your draft report recognizes the progress that the Internal Revenue Service has made to improve our information security program and that numerous initiatives are underway.

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

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

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

Sincerely,

Douglas H. Shulman

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Staff Acknowledgments

In addition to the individuals named above, David Hayes (Assistant Director), Jeffrey Knott (Assistant Director), Angela Bell, Clayton Brisson, Mark Canter, Larry Crosland, Saar Dagani, Rebecca Eyler, Mickie Gray, Nicole Jarvis, Sharon Kittrell, George Kovachick, Sean Mays, Mark Reid, Eugene Stevens, and Michael Stevens made key contributions to this report.

(311043)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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