United States Government Accountability Office

Report to the Commissioner of Internal Revenue

April 2014

INFORMATION SECURITY

IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk

GAO Highlights

Highlights of GAO-14-405, a report to the Commissioner of Internal Revenue

April 2014

INFORMATION SECURITY

IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk

Why GAO Did This Study

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

As part of its audit of IRS's fiscal years 2013 and 2012 financial statements, GAO assessed whether controls over key financial and tax processing systems are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. To do this, GAO examined IRS information security policies, plans, and procedures; tested controls over key financial applications; and interviewed key agency officials at six sites.

What GAO Recommends

GAO is recommending that IRS take 3 actions to more effectively implement portions of its information security program. In a separate report with limited distribution, GAO recommends that IRS take 23 specific actions to address identified control weaknesses. In commenting on a draft of this report, IRS agreed to develop a detailed corrective action plan to address each recommendation.

View GAO-14-405. For more information, contact Nancy R. Kingsbury at (202) 512-2700 or kingsburyn@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The Internal Revenue Service (IRS) continued to make progress in addressing information security control weaknesses and improving its internal control over financial reporting; however, weaknesses remain that could affect the confidentiality, integrity, and availability of financial and sensitive taxpayer data. During fiscal year 2013, IRS management devoted attention and resources to addressing information security controls, and resolved a number of the information security control deficiencies that were previously reported by GAO. However, significant risks remained. Specifically, the agency had not always (1) installed appropriate patches on all databases and servers to protect against known vulnerabilities, (2) sufficiently monitored database and mainframe controls, or (3) appropriately restricted access to its mainframe environment. In addition, IRS had allowed individuals to make changes to mainframe data processing without requiring them to follow established change control procedures to ensure changes were authorized, and did not configure all applications to use strong encryption for authentication, increasing the potential for unauthorized access.

An underlying reason for these weaknesses is that IRS has not effectively implemented portions of its information security program. The agency has established a comprehensive framework for the program, and continued to improve its controls; however, components of the program did not always function as intended. For example, IRS's testing procedures over financial reporting systems were not always thorough in that its testing methodology did not always determine whether required controls were operating effectively. In addition, IRS had not updated key mainframe policies and procedures to address issues such as users accessing files used by one processing environment from a different environment. Further, IRS did not include sufficient detail in its authorization procedures to ensure that access to systems was appropriate.

Until IRS takes additional steps to (1) more effectively implement its testing and monitoring capabilities, (2) ensure that policies and procedures are updated, and (3) address unresolved and newly identified control deficiencies, its financial and taxpayer data will remain vulnerable to inappropriate and undetected use, modification, or disclosure. These deficiencies, including shortcomings in the information security program, were the basis of our determination that IRS had a significant deficiency in its internal control over its financial reporting systems for fiscal year 2013.

Contents

Abbreviations

CIO	chief information officer
ESAT	Enterprise Security Audit Trails
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
TIGTA	Treasury Inspector General for Tax Administration

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

April 8, 2014

The Honorable John Koskinen
Commissioner of Internal Revenue

Dear Mr. Koskinen:

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

As part of our audit of IRS's fiscal years 2013 and 2012 financial statements,[2] we assessed the effectiveness of the agency's information security controls over its key financial and tax processing systems, information, and interconnected networks at six locations. These systems support the processing, storage, and transmission of financial and sensitive taxpayer information. As highlighted in our report on IRS's fiscal years 2013 and 2012 financial statements, during fiscal year 2013 IRS continued to devote significant attention and resources to securing its information systems and protecting sensitive taxpayer and financial information. During fiscal year 2013, IRS addressed a large number of system control deficiencies that we had previously reported and implemented a new procurement system and upgraded software for its administrative accounting system. These actions are important steps toward improving the overall effectiveness of its information system controls and therefore the reliability of its financial data.

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

[2] GAO, *Financial Audit: IRS's Fiscal Years 2013 and 2012 Financial Statements*, GAO-14-169 (Washington, D.C.: Dec. 12, 2013).

However, the remaining deficiencies in information security, along with new deficiencies we identified during this year's audit and discuss in this report, are important enough to merit the attention of those charged with governance of IRS and continue to represent a significant deficiency in IRS's internal control over its financial reporting systems as of September 30, 2013.[3]

Our objective was to determine whether IRS's controls over its 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 the agency's information security policies, plans, and procedures; tested controls over key financial applications; interviewed key agency officials; and reviewed our prior reports to identify previously reported weaknesses and assessed the effectiveness of corrective actions taken. Our evaluation was limited to systems relevant to financial management and reporting and was concentrated on threats emanating from sources internal to IRS's computer networks.

We conducted this audit from April 2013 to April 2014 in accordance with generally accepted government auditing standards. We believe our audit provides a reasonable basis for our opinions and other conclusions. For additional information about our objective, scope, and methodology, refer to appendix I.

Background

The use of information technology has created many benefits for agencies such as IRS in achieving their mission and providing information and services to the public, but challenges continue to exist as computerized information and resources grow with increasing demand and various threats continue to plague security. Information security is

[3] A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit the attention of those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

especially important for government agencies, where maintaining the public's trust is essential.

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. Cyber-based threats to information systems and cyber-related critical infrastructure can come from sources internal and external to the organization. Internal threats include errors or mistakes, as well as fraudulent or malevolent acts by employees or contractors working within an organization. External threats include the ever-growing number of cyber-based attacks that can come from a variety of sources such as hackers, criminals, and foreign nations. 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, a designation that remains in force today.[4]

Information security programs and practices performed by an agency are essential to creating and maintaining effective internal controls within an organization's critical information technology infrastructure. The *Federal Managers' Financial Integrity Act*[5] requires the Comptroller General to prescribe standards for internal control. The standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance and management challenges and areas at greatest risk of fraud, waste, abuse, and mismanagement.[6] The term internal control covers all aspects of an agency's operations (programmatic, financial, and compliance). Information system controls consist of those internal controls that are

[4] GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: February 2013).

[5] Pub. L. No. 97-255, 96 Stat. 814 (1982). The *Federal Managers' Financial Integrity Act* (FMFIA) was codified at 31 U.S.C. § 3512.

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

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

The *Federal Information Security Management Act* (FISMA)[7] is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. 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; plans for providing adequate information security for networks, facilities, and systems; providing security awareness and specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; procedures for detecting, reporting, and responding to security incidents; and ensuring continuity of operations. The act also assigned to the National Institute of Standards and Technology the responsibility for developing standards and guidelines that include minimum information security requirements.

IRS Is the Tax Collector for the United States

The mission of the IRS is to provide America's taxpayers top-quality service by helping them to understand and meet their tax responsibilities and enforce the law with integrity and fairness to all. In carrying out this mission and responsibilities of administering our nation's tax laws, the IRS relies extensively on its computer systems. As such, it must ensure that its computer systems are effectively secured to protect sensitive financial and taxpayer data for the collection of taxes, the processing of tax returns, and the enforcement of federal tax laws. In fiscal years 2013 and 2012, IRS collected about $2.9 trillion and $2.5 trillion, respectively, in federal tax payments, processed about 241 million and 239 million,

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

respectively, in tax and information returns, and paid about $364 billion and $373 billion, respectively, in refunds to taxpayers. Further, the size and complexity of IRS add unique operational challenges.

IRS employs approximately 98,000 people (which includes temporary and seasonal staff) in its Washington, D.C., headquarters and over 600 offices in all 50 states and U.S. territories and in some U.S. embassies and consulates. IRS relies extensively on computerized systems to support its financial and mission-related operations. To manage its data and information, the agency operates three enterprise computing centers located in Detroit, Michigan; Martinsburg, West Virginia; and Memphis, Tennessee. IRS also collects and maintains a significant amount of personal and financial information on each U.S. taxpayer. Protecting 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 (CIO) or comparable official at a federal agency to be responsible for developing and maintaining an information security program. IRS has delegated this responsibility to the Associate CIO, who heads the IRS Information Technology Cybersecurity organization. This organization's mission is to protect taxpayer information and the IRS's systems, services, and data from internal and external cyber-related threats by implementing security practices in planning, implementation, management, and operations. IRS develops and publishes its information security policies, guidelines, standards, and procedures in its *Internal Revenue Manual* and other documents in order for IRS divisions and offices to carry out their respective responsibilities in information security. In November 2013, the Treasury Inspector General for Tax Administration (TIGTA) stated that security of taxpayer data, including securing computer systems, was the top priority in its list of top 10 management challenges for IRS for fiscal year 2014.[8]

[8] TIGTA, *Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2014* (Washington, D.C.: November 2013).

IRS Continued to Make Progress, but Control Weaknesses Place Taxpayer and Financial Data at Risk

IRS had implemented numerous controls over its systems, including controls for identification and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, and contingency planning. However, it had not always effectively implemented access and other controls to protect the confidentiality, integrity, and availability of its financial systems and information. These weaknesses and others in IRS's security program increase the risk that taxpayer and other sensitive information could be disclosed or modified without authorization.

Access Control Weaknesses Reduced Security over Systems

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities.

Access controls include those related to user identification and authentication, authorization, cryptography, audit and monitoring, and physical security. However, IRS did not fully implement effective controls in these areas. Without adequate access controls, unauthorized individuals, including infiltrators and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users could intentionally or unintentionally read, add, delete, or modify data or execute changes that are outside their span of authority.

IRS had identification and authentication controls in place, but they were inconsistently implemented

Identification is the process of distinguishing one user from all others, usually through user IDs. These are important because they are the means by which specific access privileges are assigned and recognized by the computer. However, the confidentiality of a user ID is typically not protected. For this reason, other means of authenticating users—that is, determining whether individuals are who they say they are—are typically implemented (for example, passwords, security tokens, etc.). IRS's *Internal Revenue Manual* specifies security configurations for its database systems and network infrastructure systems that cover how authentications are to be performed and how passwords are to be configured. The manual also requires the use of a strong password for authentication (defined as a minimum of eight characters, containing at least one numeric or special character, a mixture of at least one uppercase and one lowercase letter, and no words found in a dictionary), and that passwords be set to expire every 90 days. Further, the manual states that passwords for service accounts shall expire within 366 days.

IRS improved identification and authentication controls for several databases and one of its major operating systems. For example:

- authentication controls for databases supporting the agency's access authorization and procurement systems were set to prevent a user from connecting to a database without a password;
- controls over complexity of passwords for certain databases were adequate; and
- passwords were stored with adequate controls to prevent them from being disclosed.

However, identification and authentication control weaknesses continued to reduce IRS's ability to effectively control access to systems and data. Specifically:

- controls over the length of passwords for certain network infrastructure systems were not adequate and
- the agency used passwords that could be easily guessed.

Further, IRS did not always ensure that all database accounts were set to have a maximum expiration of 90 days. In addition, the agency had not consistently applied proper password settings to mainframe service accounts. Of the 81 mainframe service accounts, 31 were configured to never require password changes. As a result of these weaknesses, IRS had reduced ability to control who was accessing its systems and data.

IRS had a framework in place to manage authorization, but some users had more access than necessary to perform their duties

Access rights and privileges are used to implement security policies that determine what a user can do after being allowed into a system. Access rights, also known as permissions, allow the user to read or write to a certain file or directory. Privileges are a set of access rights permitted by the access control system. A key component of authorization is the concept of "least privilege," which means that users should have the least amount of privileges necessary to perform their duties. Maintaining access rights, permissions, and privileges is one of the most important aspects of administering system security. According to the *Internal Revenue Manual*, the agency should implement access control measures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. The manual also requires that system access be granted based on the principle of least privilege.

IRS had strengthened several authorization controls, including:

- implementing programming changes to an application to correct a vulnerability that allowed users of that application to view sensitive

system information by using unintended capabilities in the user interface of the application and
- consistently providing access privileges on all mainframe systems to prevent users from having a greater level of access than needed to perform their duties.

However, numerous authorization control weaknesses existed in IRS's computing environment, including:

- Access privileges allowed all users of IRS's internal network to read and write files containing sensitive system information, including passwords, that were used to support automated data transfer operations between numerous systems. Unauthorized access privileges to these files jeopardized the integrity of the data and the availability of applications.
- Administrators had more access than needed in certain instances. On one server, IRS had configured multiple databases supporting different business units to operate using the same username. As a result, any administrator with access to the username could have access to all databases, exceed his or her job duties, and affect IRS's ability to control the integrity of the data.
- Nine contractors were collectively assigned 14 mainframe security software user profiles that had password expiration dates set beyond the end of the contract period. Six contractors were collectively assigned 9 mainframe security software user profiles that had no expiration dates set. Maintaining contractor user IDs on the system after the contract date has expired could allow unauthorized use of their username and passwords, and would expose system information and render sensitive data vulnerable to unauthorized access. As a result, IRS had reduced ability to control who was accessing its systems and data.

Until IRS appropriately controls users' access to its systems and effectively implements its procedures for authorization, the agency has limited assurance that its information resources are being protected from unauthorized access, alteration, and disclosure.

IRS inconsistently employed cryptography controls for authentication, resulting in transmission of weakly encrypted or unencrypted authentication information across its internal network

Cryptography controls can be used to identify and authenticate users and help protect the integrity and confidentiality of data and computer programs by rendering data unintelligible to unauthorized users and by protecting the integrity of transmitted or stored data. Cryptography involves the use of mathematical functions called algorithms and strings of seemingly random bits called keys to (1) encrypt a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential; (2) provide an electronic signature that can be used to determine if any changes have been made to the related file, thus ensuring the file’s integrity; or (3) link a message or document to a specific individual’s or group’s key, thus ensuring that the “signer” of the file can be identified. According to the *Internal Revenue Manual*, the confidentiality of transmitted data must be protected by encrypting the data to prevent unauthorized disclosure. In addition, the policy states that the use of insecure protocols should be restricted because their widespread use can allow passwords, taxpayer information, and other sensitive data to be transmitted unencrypted across its internal network.

IRS made progress in its implementation of data encryption controls by:

- configuring network equipment to use encrypted authentication protocols,
- discontinuing the use of an unencrypted protocol to transmit sensitive information on a server supporting the IRS’s tax payment system, and
- disabling an unencrypted authentication method on e-mail servers.

However, many of IRS’s servers were configured to use weak encryption for authentication. Further, the agency did not configure servers that supported the administration of automated file transfers of financial data to use encryption for authentication. Until these weaknesses are corrected, IRS’s ability to reliably control access to some systems and data is undermined.

Although IRS had numerous audit and monitoring processes in place, it had not effectively implemented a monitoring process for several of its database and mainframe environments

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Audit and monitoring controls can help information systems security professionals routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack. Audit and monitoring technologies include network and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. The *Internal Revenue Manual* requires that audit logging be enabled and configured on all systems to aid in the detection of security violations, performance problems, and flaws in applications. Additionally, the manual states that security controls in information systems shall be monitored on an ongoing basis.

IRS had strengthened its audit and monitoring processes by:

- enabling security event auditing[9] and system privilege auditing[10] features on databases that support its access authorization, administrative accounting, and procurement systems;
- configuring mainframe audit logging to record the newer types of network activity that are supported by the operating system; and
- enabling user auditing for users with account attributes that are needed to perform sensitive mainframe system administration tasks.

However, IRS did not always effectively implement audit and monitoring controls on internal systems. Specifically, despite ongoing efforts dating back to 2007, IRS's enterprisewide mainframe security monitoring program, known as Enterprise Security Audit Trails (ESAT), has yet to deliver operational mainframe security monitoring reports to system owners or stakeholders. Without effective audit and monitoring, IRS's ability to establish individual accountability, monitor compliance with security and configuration management policies, and investigate information systems security violations is limited.

Although IRS had implemented numerous physical security controls, weaknesses reduced control effectiveness

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Adequate physical security controls over computer resources (e.g., computer facilities, network devices such as routers and firewalls, telecommunications equipment, and transmission lines) should be established that are commensurate with the risks of physical damage or access. Physical security controls over the overall facility and areas housing sensitive information technology components include, among other things, policies and practices for granting and discontinuing access authorizations; controlling badges, ID cards, smartcards, and other entry devices; controlling entry during and after normal business hours; and controlling the entry and removal of computer resources (such as equipment and storage media) from the facility. Physical security controls also include environmental controls, such as smoke detectors, fire alarms, extinguishers, uninterruptible power supplies, and redundancy in air cooling systems. At IRS, physical access control measures, such as

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

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

physical access cards that are used to permit or deny access to certain areas of a facility, are vital to safeguarding facilities, computing resources, and information from internal and external threats. The *Internal Revenue Manual* requires a short-term uninterruptible power supply be provided to facilitate an orderly shutdown of information systems in the event of a primary power loss. The manual also requires that access controls be implemented to safeguard assets against possible theft and malicious actions. Further, the manual states that department managers of restricted areas are to review, validate, sign, and date the authorized access list for the restricted area on a monthly basis, and then forward the list to the physical security office for review.

IRS had implemented physical security controls at its enterprise computing centers to carry its facilities through a short power outage, and provide time to back up data and perform orderly shutdown procedures during extended power outages. For example, IRS installed redundant critical systems, such as uninterruptible power supplies and backup generators, at all three computing centers so that power would be adequate for an orderly shutdown. Further, IRS implemented safeguards to protect its assets against theft and malicious actions. For example, IRS reviewed visitor physical access cards at one computing center to ensure that they provided only the authorized levels of access to the restricted areas within the center.

However, physical security controls were not always effectively implemented. For example, during monthly reviews of individuals with an ongoing need to access restricted areas at two of the three computing centers, officials did not consistently indicate the need to remove individuals who no longer needed access. We previously made a recommendation in fiscal year 2011 to address this issue at one of the two computing centers.[11] Because employees and visitors may be allowed inappropriate access to restricted areas, IRS has reduced assurance that its computing resources and sensitive information are being adequately protected from unauthorized access.

[11] GAO, *Information Security: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data*, GAO-11-307SU (Washington, D.C.: March 2011).

IRS Had Contingency Plans in Place, but Weaknesses in Other Information Security Controls Introduce Risk

In addition to access controls, other controls should be in place to ensure the confidentiality, integrity, and availability of an agency's information. These controls include policies, procedures, and techniques for securely configuring information systems with software updates and planning for continuity of operations. Weaknesses in system configurations increase the risk of unauthorized use, disclosure, modification, or loss of information to financial and tax processing systems and taxpayer data.

Weaknesses continued to exist in updating software

Configuration management controls are intended to prevent unauthorized changes to information system resources (for example, software programs and hardware configurations) and to provide reasonable assurance that systems are configured and operating securely and as intended. Change control procedures, a component of configuration management, are important to ensure that only authorized and fully tested systems are placed in operation. To ensure that changes to systems are necessary, work as intended, and do not result in the loss of data or program integrity, such changes should be documented, authorized, tested, and independently reviewed. Patch management, yet another component of configuration management, is an important element in mitigating the risks associated with known vulnerabilities. When vulnerabilities are discovered, the vendor may release an update to mitigate the risk. Without the update applied in a timely manner, an attacker may exploit a vulnerability not yet mitigated, enabling unauthorized access to an information system or enabling users to have access to greater privileges than authorized. Unsupported software increases risk because vendors no longer provide updates to known vulnerabilities. Accordingly, the *Internal Revenue Manual* states that all changes to production systems and processing must be requested and approvals documented. The manual also requires IRS to reduce vulnerabilities to systems by installing patches in a timely manner. Specifically, it states that IRS should implement critical priority security-related patches within 72 hours of patch availability and high-priority security-related patches within 5 business days of patch availability. Further, the manual states that the agency should ensure that the version of an application being used is one for which the vendor continues to offer technical support, and that database software be removed or updated prior to a vendor dropping support.

Although IRS has change control and patch management processes in place, it did not effectively document and approve changes or install patches in a timely manner. For example, of 32 changes to mainframe production processing recorded in the system logs during the 1-week period we reviewed, no requests or approvals had been made or documented. This activity had not been detected by system monitoring processes. By not enforcing change controls in the production mainframe system, the integrity and availability of IRS's data and systems are jeopardized. Also, IRS had not applied critical patches within required time frames to servers supporting multiple systems we reviewed, including the authorization, procurement, and e-mail systems. By not installing critical patches in a timely fashion, IRS increases the risk that known vulnerabilities in its systems may be exploited. Further, the agency used an unsupported software application on its workstations, and database software used to support the access authorization system was no longer supported. Running outdated and unsupported software increases security exposure, as the vendor will not be supplying any security patches to the unsupported software.

IRS had contingency plans in place for systems reviewed

Contingency planning, which includes developing contingency and business continuity plans, should be tested to ensure that when unexpected events occur, critical operations can continue without interruption or can be promptly resumed, and that information resources are protected. The *Internal Revenue Manual* requires the agency to develop, test, and maintain information system contingency plans for all systems. In addition, according to the manual, IRS shall implement and enforce backup procedures for all systems and information and test the plans to determine their effectiveness and the agency's readiness to execute the plans.

IRS had processes in place to ensure recovery of their information system resources through continuity of operations, which included contingency plans and their associated test plans. For the seven contingency plans we reviewed, the agency had appropriately documented and maintained current plans and had tested the plans, and had the appropriate backup procedures in place to ensure recovery of its data and information system resources.

IRS Had Developed an Information Security Program, but Had Not Always Effectively Implemented Elements of the Program

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 a comprehensive agencywide information security program, it had not effectively implemented elements of it.

An agencywide information security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. 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, performed with a frequency depending on risk, but no less than annually, and that include 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 information security policies, procedures, or practices; and
- procedures for detecting, reporting, and responding to security incidents.

Further, the current administration has made continuous monitoring of federal information systems a top cyber-security priority. Continuous monitoring of security controls employed within or inherited by the system is an important aspect of managing risk to information from the operation and use of information systems. An effective information security program also includes a rigorous continuous monitoring program integrated into the system development life cycle. As described by the National Institute of Standards and Technology,[12] effective continuous monitoring begins with development of a strategy that addresses requirements and activities

[12] National Institute of Standards and Technology, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, *Special Publication 800-137* (Gaithersburg, Md.: September 2011).

at each organizational tier. The *Internal Revenue Manual* states that the agency should document its continuous monitoring strategy as defined by this guidance.

IRS had implemented a comprehensive information security program, as illustrated by the following examples:

- IRS had developed and documented an information technology security risk management policy that required all sensitive applications to be periodically assessed for the risk and magnitude of harm that could result from vulnerabilities and potential threats.
- The agency had developed policies and procedures that considered risk, appropriately addressed purpose, scope, roles, responsibilities, and compliance, and were approved by management.
- IRS had developed and documented security plans for all of its major systems that we reviewed that addressed policies and procedures for providing management, operational, and technical controls.
- IRS had a process in place for providing employees with security awareness and specialized training. All employees with specific security-related roles that we reviewed met the required minimum specialized training hours.
- The agency had implemented numerous processes for testing and evaluating the effectiveness of controls, and told us that it had previously identified many of the issues we raise in this report.
- IRS had completed actions to address 42[13] of the 91 recommendations we reported in 2013 that were still unresolved at the time of our last review (as of September 30, 2012).[14]
- IRS had a process in place to ensure that its Computer Security Incident Response Center incident tickets were opened, managed, and closed in accordance with IRS's policies and procedures governing incident detection, handling, and response. Of the 45 incident tickets we reviewed, we validated that each had been opened, managed, and closed by center personnel and handled according to its proper incident categorization as outlined by the National Institute of Standards and Technology.

[13] We consider six additional recommendations to no longer be relevant due to the changing operating environment; however, we are making three new specific technical recommendations that address similar issues in the current environment.

[14] GAO, *Information Security: IRS Has Improved Controls but Needs to Resolve Weaknesses*, GAO-13-350 (Washington, D.C.: March 2013).

However, not all elements of IRS's information security program had been effectively implemented, as illustrated in the following examples:

- Although IRS had developed and documented information security policies and procedures covering key topics such as risk assessments, security awareness training, testing and evaluation of security controls, configuration management, continuity of operations, and incident response, shortcomings existed with policies and procedures.
    - IRS had not updated policies and procedures to ensure that they address (1) both methods available for granting all users access to mainframe resources, (2) audit and monitoring of access from one processing environment to another, (3) use of appropriate accounts by multiple databases on a single server, (4) data storage shared between systems, (5) out-of-date security standards, and (6) reconciliation of access privileges. We previously made a recommendation to address these issues.[15]
    - IRS does not record or maintain sufficiently detailed or organized information of system access requests and access assignments to facilitate effective review or verification of users' system access privileges. The *Internal Revenue Manual* contains no requirements for the content of access information to be entered or maintained in the IRS on-line access request and approval system. As a result, individual users' access privileges for both mainframe and distributed computing-based applications cannot be accurately verified. This increases the likelihood that erroneous and outdated access privileges will not be detected.
    - Internal system documentation entries for important automated mainframe processes that were recently added to the system were not completed. IRS procedures did not specify the information required to be recorded in the internal system documentation. Absent this system documentation, the effectiveness of monitoring of these important automated processes is diminished.
- Although IRS had processes in place for providing employees with security awareness and specialized training, the agency did not always ensure that contractors received security awareness training. The *Internal Revenue Manual* requires that all new employees and contractors receive security awareness training within 5 days of

[15] GAO-13-350.

receiving system access. Processes for ensuring contractors received required training were not in place. We reported in 2013 that more than half of the contractors we evaluated had not met IRS' security awareness training requirement. We previously made a recommendation in 2010 to address contractor security awareness training.[16]

- IRS's procedures for testing and evaluating controls were not always effective. A key element of an information security program is conducting tests and evaluations of policies, procedures, and controls to determine whether they are effective and operating as intended. However, for one financial reporting system that we reviewed, the testing methodology did not always determine whether required authentication controls were operating effectively. Also, IRS had not identified some of the other issues raised in this report, including weaknesses involving missing patches and undocumented mainframe changes. In addition, IRS had not yet updated mainframe test and evaluation processes to improve periodic monitoring of compliance with policies, including the shortcomings with its ESAT program discussed in this report. We previously made recommendations to address these issues.[17]
- Although IRS had a process in place for evaluating and tracking remedial actions, it had not consistently developed a remedial action plan for known vulnerabilities. The *Internal Revenue Manual* requires that such a plan be developed for information systems to document the planned remedial actions to correct weaknesses or deficiencies noted during an assessment of security controls and to reduce or eliminate known vulnerabilities in the system. However, IRS had not developed a plan to document remedial actions to eliminate known vulnerabilities in one of its workload automation software environments.
- As we reported in 2013, IRS had not fully documented its continuous monitoring strategy. The agency created a diagram that logically depicts certain information security continuous monitoring data flows and activities; had developed various standard operating procedures; and is collecting, analyzing, and reporting on certain data. However, it had not developed a strategy that addresses requirements and

[16] GAO, *Information Security: IRS Needs to Continue to Address Significant Weaknesses*, GAO-10-355 (Washington, D.C.: March 2010).

[17] GAO-13-350.

activities at each organizational tier. We previously made a recommendation to address this issue.[18]

Until IRS effectively implements all key elements of its information security program, the agency will not have reasonable assurance that computing resources are consistently and effectively protected from inadvertent or deliberate misuse, including fraud or destruction.

Conclusions

IRS continued to make progress in addressing information security control weaknesses, improving its internal control over financial reporting; however, serious weaknesses remain that could affect the confidentiality, integrity, and availability of financial and sensitive taxpayer data. During fiscal year 2013, IRS management continued to devote attention and resources to addressing information security controls, and resolved a significant number of the information security control deficiencies that we previously reported. However, information security weaknesses existed in access and other information system controls over IRS's financial and tax-processing systems. The financial and taxpayer information on IRS systems will remain particularly vulnerable to internal threats until the agency (1) addresses weaknesses pertaining to identification and authentication, authorization, cryptography, audit and monitoring, physical security, and configuration management; and (2) effectively implements key components of its comprehensive information security program that ensure processes intended to test, monitor, and evaluate internal controls are appropriately detecting vulnerabilities, including updating policies and procedures for system-level authentication and authorization, and developing remedial action plans for identified weaknesses. These deficiencies are the basis of our determination that IRS had a significant deficiency in internal control over financial reporting in its information security in fiscal year 2013. Continued and consistent management commitment and attention to an effective information security program will be essential to the maintenance of, and continued improvements in, the agency's information security controls.

Recommendations for Executive Action

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

[18] GAO-13-350.

- Update access request policies and procedures to ensure that they contain sufficiently detailed information of access requests and access assignments to facilitate effective review and verification of appropriate access privileges.
- Update procedures to specify the information required to be recorded in the internal system documentation for important mainframe system processes.
- Develop a remedial action plan to address known information system weaknesses or deficiencies in the workload automation software environment.

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 identification and authentication, authorization, cryptography, and configuration management.

Agency Comments and Our Evaluations

In providing written comments (reprinted in app. II) on a draft of this report, the Commissioner of Internal Revenue stated that the security and privacy of taxpayer and financial information is of the utmost importance to the agency and that IRS will provide a detailed corrective action plan addressing each of our recommendations. Further, the Commissioner stated that the integrity of IRS's financial systems continues to be sound. However, as we noted in this report, although IRS has continued to make progress in addressing information security control weaknesses, it had not always effectively implemented access and other controls to protect the confidentiality, integrity, and availability of its financial systems and information. The effective implementation of our recommendations in this report and in our previous reports will assist IRS in protecting taxpayer and financial information.

This report contains recommendations to you. As you know, 31 U.S.C. § 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform not later than 60 days from the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report. Because agency personnel serve as the primary source of information on the status of recommendations, we request that the agency also provide us with a copy of the agency's statement of action to serve as preliminary information on the status of open recommendations.

We are also sending copies of this report to the Secretary of the Treasury, the Treasury Inspector General for Tax Administration, and interested congressional parties.

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. 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: Objective, Scope, and Methodology

The objective of our review was to determine whether controls over key financial and tax processing systems were effective in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer information at the Internal Revenue Service (IRS). To do this, we examined IRS information security policies, plans, and procedures; tested controls over key financial applications; and interviewed key agency officials. This enabled us to (1) assess the effectiveness of corrective actions taken by IRS to address weaknesses we previously reported and (2) determine whether any additional weaknesses existed. This work was performed in connection with our audit of IRS's fiscal years 2013 and 2012 financial statements for the purpose of supporting our opinion on internal control over the preparation of those statements and may not be sufficient for other purposes.

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

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 Institute of Standards and Technology guidance; and IRS policies, procedures, practices, and standards. We evaluated controls by

- testing the complexity, expiration, and policy for passwords on databases to determine if strong password management was being enforced;
- examining IRS's implementation of encryption to secure transmissions on its internal network;
- analyzing the audit logs recorded by the mainframe environment, which processes tax data and supports revenue and unpaid assessment financial reporting;

- reviewing physical security processes and procedures at each of the enterprise computing centers;
- evaluating the mainframe operating system controls that support the operation of applications and databases that support revenue accounting;
- evaluating the controls of mainframe configurations that shared disk storage with multiple mainframe processing environments;
- reviewing access configurations on key systems and database configurations;
- examining the status of patching for key databases and system components to ensure that patches are up to date;
- reviewing the process for IRS's risk assessment reviews to determine if risk assessment reviews were being performed at least annually; and
- examining documentation to determine the extent to which IRS was performing internal controls reviews of key financial systems.

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

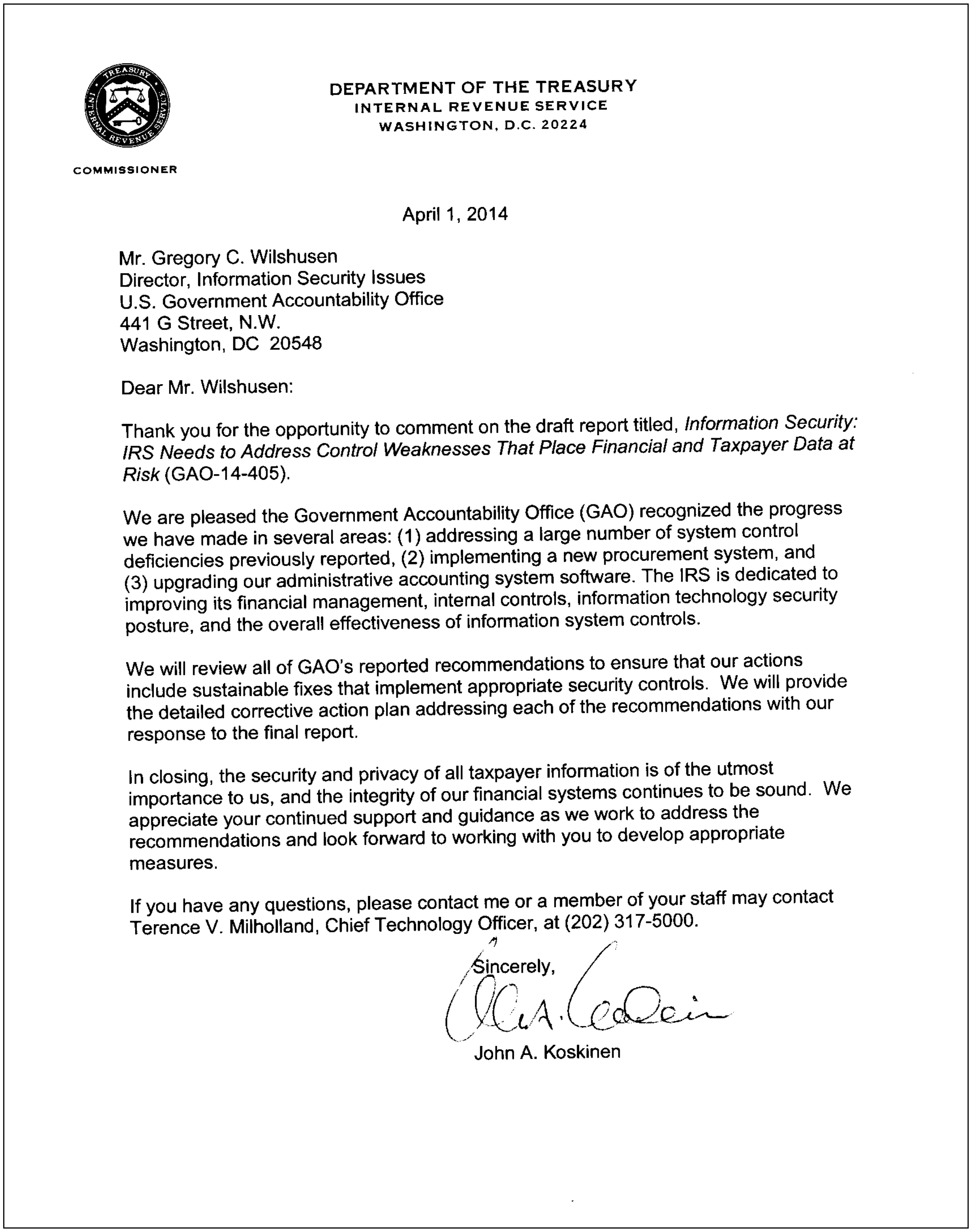
- reviewing risk assessments to determine whether the assessments were up to date, documented, and approved;
- reviewing IRS's policies, procedures, practices, and standards to determine whether its security management program had been documented, approved, and was up to date;
- reviewing IRS's system security plans for specified systems to determine the extent to which the plans had been reviewed, and included information as required by the National Institute of Standards and Technology;
- verifying whether employees with security-related responsibilities had received specialized training within the year;
- analyzing documentation to determine if the effectiveness of security controls had been periodically assessed;
- reviewing IRS's actions to correct weaknesses to determine if they had effectively mitigated or resolved the vulnerability or control deficiency;
- reviewing IRS's Computer Security Incident Response Center incident tickets to determine if security violations and activities had been reported and investigated, and validating that the agency was correctly categorizing incidents per federal guidance; and

- reviewing continuity-of-operations planning documentation for seven systems to determine if such plans had been appropriately documented and tested.

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

We performed our audit from April 2013 to April 2014 in accordance with U.S. generally accepted government auditing standards. We believe our audit provides a reasonable basis for our opinions and other conclusions in this report.

Appendix II: Comments from the Internal Revenue Service



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

COMMISSIONER

April 1, 2014

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

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report titled, *Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk* (GAO-14-405).

We are pleased the Government Accountability Office (GAO) recognized the progress we have made in several areas: (1) addressing a large number of system control deficiencies previously reported, (2) implementing a new procurement system, and (3) upgrading our administrative accounting system software. The IRS is dedicated to improving its financial management, internal controls, information technology security posture, and the overall effectiveness of information system controls.

We will review all of GAO's reported recommendations to ensure that our actions include sustainable fixes that implement appropriate security controls. We will provide the detailed corrective action plan addressing each of the recommendations with our response to the final report.

In closing, the security and privacy of all taxpayer information is of the utmost importance to us, and the integrity of our financial systems continues to be sound. We appreciate your continued support and guidance as we work to address the recommendations and look forward to working with you to develop appropriate measures.

If you have any questions, please contact me or a member of your staff may contact Terence V. Milholland, Chief Technology Officer, at (202) 317-5000.

Sincerely,

John A. Koskinen

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Staff Acknowledgments

In addition to the individuals named above, David Hayes and Jeffrey Knott (assistant directors), Mark Canter, Jennifer R. Franks, Nancy Glover, Mickie Gray, J. Andrew Long, Linda Kochersberger, Kevin Metcalfe, Eugene Stevens, Michael Stevens, and Daniel Swartz made key contributions to this report.

(311312)

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

Please Print on Recycled Paper.