



March 2015

INFORMATION SECURITY

IRS Needs to Continue Improving Controls over Financial and Taxpayer Data

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 data that resides on those systems.

As part of its audit of IRS's fiscal year 2014 and 2013 financial statements, GAO assessed whether controls over key financial and tax-processing systems were 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; interviewed key agency officials; and tested controls over key financial applications at four sites.

What GAO Recommends

GAO is recommending that IRS take 5 additional actions to more effectively implement elements of its information security program. In a separate report with limited distribution, GAO is recommending 14 actions that IRS can take to address newly identified control weaknesses. In commenting on a draft of this report, IRS agreed to develop corrective action plans where appropriate to address these recommendations.

INFORMATION SECURITY

IRS Needs to Continue Improving Controls over Financial and Taxpayer Data

What GAO Found

The Internal Revenue Service (IRS) made progress in implementing information security controls; however, weaknesses limit their effectiveness in protecting the confidentiality, integrity and availability of financial and sensitive taxpayer data. During fiscal year 2014, IRS continued to devote attention to securing its information systems that process sensitive taxpayer and financial information. Key among its actions were improving the security over the software that manages changes to its mainframe environment and upgrading secure communications enterprise-wide for sensitive data. However, significant control deficiencies existed. For example, IRS did not install appropriate security updates on all of its databases and servers, and did not sufficiently monitor control activities that support its financial reporting. In addition, IRS did not effectively maintain the secure configuration of a key application, or appropriately segregate duties by allowing a developer unnecessary access to the application.

An underlying reason for these weaknesses is that IRS has not effectively implemented elements of its information security program. The agency had a comprehensive framework for its program, such as assessing risk for its systems, developing security plans, and providing employees with security awareness and specialized training. However, aspects of its program were not yet effectively implemented. For example, IRS's testing methodology did not always determine whether required controls were operating effectively; consequently, GAO continued to identify control weaknesses that had not been detected by IRS. Also, IRS had not updated key mainframe policies and procedures to address issues such as comprehensively auditing and monitoring of access, thereby increasing the risk of unauthorized access to tax processing systems not being detected. In addition, IRS did not reassess controls for a key system after significant changes had been made in the operating environment. Further, IRS had not ensured that many of its corrective actions to address previously identified deficiencies were effective. For example, of 69 previously reported weaknesses that remained unresolved at the end of GAO's last audit, IRS indicated it had implemented corrective actions for 24 of them; however, GAO determined that 10 of the 24 weaknesses had not been fully resolved.

Until IRS takes additional steps to (1) address unresolved and newly identified control deficiencies and (2) effectively implements elements of its information security program, including, among other things, updating policies, test and evaluation procedures, and remedial action procedures, its financial and taxpayer data will remain unnecessarily vulnerable to inappropriate and undetected use, modification, or disclosure. These shortcomings were the basis for GAO's determination that IRS had a significant deficiency in internal control over financial reporting systems for fiscal year 2014.

Contents

Letter		1
	Background	2
	IRS Made Progress in Addressing Control Weaknesses but Taxpayer and Financial Data Continued to Be at Risk	6
	Conclusions	19
	Recommendations for Executive Action	20
	Agency Comments and Our Evaluation	20
Appendix I	Objective, Scope, and Methodology	22
Appendix II	Comments from the Internal Revenue Service	25
Appendix III	GAO Contacts and Staff Acknowledgments	26

Abbreviations

CIO	chief information officer
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
RPO	recovery point objective

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



March 19, 2015

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 controls¹ 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 2014 and 2013 financial statements,² we assessed the effectiveness of the agency's information security controls over its key financial and tax processing systems, information, and interconnected networks at four locations. These systems support the processing, storage, and transmission of financial and sensitive taxpayer information. As highlighted in our report on IRS's fiscal years 2014 and 2013 financial statements, during fiscal year 2014 IRS continued to devote attention to securing its information systems to appropriately protect sensitive taxpayer and financial information. Key among its actions during fiscal year 2014 were improving the security over the software that manages changes to its mainframe environment and upgrading secure communications enterprise-wide for sensitive data. The agency was also in the process of upgrading user workstations to a more secure operating system. These actions are important steps toward improving the overall effectiveness of its information system controls and therefore the reliability of its financial data.

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

²GAO, *Financial Audit: IRS's Fiscal Years 2014 and 2013 Financial Statements*, [GAO-15-173](#) (Washington, D.C.: Nov. 12, 2014).

However, deficiencies in information security from prior years that continued to exist in fiscal year 2014, 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 therefore represent a significant deficiency in IRS's internal control over financial reporting systems as of September 30, 2014.³

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.

We conducted this audit from April 2014 to March 2015 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. Agencies have become dependent on information technology, as they rely on systems to carry out their operations, including processing, maintaining and reporting large volumes of sensitive data, such as personal information. Accordingly, information security is especially important for government agencies, where maintaining the public's trust is essential.

³A 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.

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—individuals, groups, and countries who wish to do harm to an organization’s systems. 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 dependent on information systems processing and include general controls (such as managing security, appropriately restricting access to data and systems, securely configuring systems, segregating

⁴GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: February 2015).

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

⁶GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

incompatible duties, and planning for continuity of operations) 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 computerized systems to support its financial and mission-related operations. As such, it must ensure that they 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 2014 and 2013, IRS collected about \$3.1

⁷The *Federal Information Security Management Act of 2002 (FISMA '02)* was enacted as Title III, *E-Government Act of 2002*, Pub L. No. 107-347 (Dec. 17, 2002). In December 2014, subsequent to our evaluation of controls, FISMA '02 was partially superseded by enactment of the *Federal Information Security Modernization Act of 2014 (FISMA '14)*, Pub. L. No. 113-283 (Dec. 18, 2014). The new law incorporates and continues the requirements from FISMA '02 applicable to IRS that we relied upon in our report. Accordingly, no changes to our findings were necessary.

trillion and \$2.9 trillion, respectively, in federal tax payments, processed about 199 million and 241 million, respectively, in tax and information returns, and paid about \$374 billion and \$364 billion, respectively, in refunds to taxpayers. Further, the size and complexity of IRS add unique operational challenges.

IRS employs approximately 94,000 people (which includes temporary and seasonal staff) in its Washington, D.C., headquarters and over 600 offices in all 50 states, U.S. territories, and in some U.S. embassies and consulates. To manage its data and information, the agency operates three enterprise computing centers located in Detroit, Michigan; Martinsburg, West Virginia; and Memphis, Tennessee. IRS also collects and maintains a significant amount of personal and financial information on each 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 October 2014, the Treasury Inspector General for Tax Administration 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 2015.⁸

⁸Treasury Inspector General for Tax Administration, *Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2015* (Washington, D.C.: October 2014).

IRS Made Progress in Addressing Control Weaknesses but Taxpayer and Financial Data Continued to Be at Risk

IRS had implemented numerous controls over its systems. However, it had not always effectively implemented access and other controls, including elements of its information security program, to protect the confidentiality, integrity, and availability of its financial systems and information. These weaknesses—including both previously reported and newly identified—increase the risk that taxpayer and other sensitive information could be disclosed or modified without authorization.

IRS Improved Access Controls, but Weaknesses Remained

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 identifying and authenticating users, authorizing access needed to perform job duties, encrypting sensitive data, auditing and monitoring system activities, and physically protecting computing resources.

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. Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric). The combination of identification and authentication—such as user account-password combinations—provides the basis for establishing accountability and for controlling access to the system.

IRS has established policies for identification and authentication. IRS's *Internal Revenue Manual* requires that *Homeland Security Presidential Directive 12* (HSPD-12)⁹ compliant multifactor authentication be implemented for local and network access accounts. The manual also specifies security configurations for its database and network infrastructure systems that cover how authentications are to be performed and how passwords are to be configured. For example, the manual requires that user account passwords be at least eight characters in length and be set to expire at a maximum of 90 days or sooner, and passwords for service accounts should be set to expire within 366 days. Further, the manual states that use of generic accounts shall not be permitted.

IRS improved identification and authentication controls for its computing environments. For example, the agency expanded the use of two-factor HSPD-12 access for identification and authentication to its network.

Nevertheless, identification and authentication control weaknesses reduced IRS's ability to effectively control access to systems and data. Specifically:

- Controls over the length of passwords for certain network infrastructure devices were set to less than eight characters.
- IRS did not ensure that all user account passwords were set to expire every 90 days or sooner on two databases.
- The agency had not consistently applied proper password settings to mainframe service accounts. Out of 112 mainframe service accounts detected, none were configured to require a password change.
- The agency used a generic account to administer an application.

As a result of these weaknesses, IRS had reduced ability to control who was accessing its systems and data.

⁹In an effort to increase the security of federal facilities and information systems where there is potential for terrorist attacks, the President issued *Homeland Security Presidential Directive 12* (HSPD-12) in August 2004. This directive ordered the establishment of a mandatory governmentwide standard for secure and reliable forms of identification for federal government employees and contractor personnel who access government-controlled facilities and information systems.

IRS had a framework in place to manage authorization, but authorization controls were inconsistently implemented

Access rights and privileges are used to implement security policies that determine what a user can do after being allowed into the 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 be granted 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.

IRS has established policies for authorizing access to information technology systems. 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, which allows access at the minimum level necessary to support a user’s job duties. Further, the manual requires that system access be approved using the agency’s access request and approval system prior to an account being created or enabled, and that an account be disabled or removed when a request is made to do so.

IRS improved its authorization process. For example, IRS had strengthened several authorization controls, including removing excessive privileges that allowed users to change mainframe system files.

However, numerous authorization control weaknesses existed in IRS’s computing environment.

- IRS allowed users to have excessive privileges to an application used to process electronic tax payment information. Specifically, IRS did not appropriately limit the ability of users to enter commands using the application’s user interface. As a result, users could access or change tax payment-related data.
- IRS did not appropriately configure Oracle databases running on a server that supported multiple applications. IRS had configured multiple Oracle databases operating on a server to run under one account. As a result, any administrator with access to the account would have access to all of these databases; potentially exceeding his/her job duties, and affecting IRS’s ability to control the integrity of the data.

-
- At least five accounts were active on an application's database, although they had been requested for removal in IRS's access request and approval system, with removal request dates ranging from April 2009 through March 2014.

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

IRS continued to enhance its use of encryption to protect sensitive data, but shortcomings remained

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.

IRS established a policy for encrypting data. According to the *Internal Revenue Manual*, the confidentiality of transmitted data must be protected by encrypting the data to prevent unauthorized disclosure. The manual also states that IRS shall implement encryption mechanisms for authentication that meet the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

IRS continued to enhance its use of encryption to protect sensitive data, but shortcomings remain. IRS made progress in its implementation of data encryption controls by enforcing the use of strong encryption for its Windows environment. However, agency servers used weak or no encryption for authentication. For example, the agency did not configure a server that supported the administration of automated file transfers of financial data to use encryption for authentication. By not encrypting sensitive authentication data, increased risk exists that an unauthorized individual could view and then use the data to gain unwarranted access to its system and to sensitive information.

Although IRS had numerous audit and monitoring processes in place, it had not effectively implemented monitoring for a key 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.

IRS established policies and procedures for auditing and monitoring information technology systems. 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 continued to enhance its audit and monitoring capability, but weaknesses remain. IRS had strengthened its audit and monitoring processes of the mainframe by enabling monitoring of changes to certain controls over the management of data. However, IRS did not always effectively implement audit and monitoring controls on its systems. For example, the agency did not enable logging for the database supporting the utility used to transfer financial data. In addition, IRS allowed changes to be made from its test systems that affect controls in systems used to support production applications, despite a continuing lack of monitoring of mainframe test systems. 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.

Physical access control procedures were not consistently implemented

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. 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; periodically reviewing access authorizations in order to ensure that access continues to be appropriate; and controlling the entry, storage, and removal of computer resources (such as equipment and storage media) from the facility.

IRS developed and documented policies for physically protecting its computer resources. The *Internal Revenue Manual* states that digital media, such as magnetic tapes, shall be securely stored when not in use. Further, the manual requires that records be established to track all deposits and withdrawals from media storage facilities and libraries. The manual also requires 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.

IRS established physical security controls at its enterprise computing centers to protect its magnetic tapes. For example, the agency securely stored magnetic tapes when not in use, and established records to track deposits and withdrawals from its media storage facilities.

However, physical security controls were not always effectively implemented. Monthly reviews of individuals with an ongoing need to access restricted areas at two of the three computing centers were not being conducted in a way that would ensure that such access was still appropriate. For example, the monthly review process at one of the computing centers had not identified an individual who had separated from IRS and did not result in the removal of his/her access privileges. In addition, in fiscal year 2014, the monthly review process at one of these centers did not include all access groups for restricted areas for at least 3 months. 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.

Weaknesses in Other Information Security Controls Introduced Risk

Although IRS improved its change management process, weaknesses continued to exist in updating software

In addition to access controls, other 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 with software updates; segregating incompatible duties; and planning for continuity of operations.

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 information systems or enabling users to have access to greater privileges than authorized.

IRS has developed policies for the managing the configuration of its information technology systems. Accordingly, the *Internal Revenue Manual* requires that the ability to make configuration changes be granted based on the principle of least privilege—allowing access at the minimum level necessary to support a user’s job duties. Further, the manual states that all changes to configuration items supporting any IRS system will be approved prior to implementation, with the allowed exception of emergency changes. The manual also requires that IRS manage systems to reduce vulnerabilities by installing patches in a timely manner. Specifically, it states that IRS should begin distribution of critical priority security-related patches within 72 hours of patch availability and high-priority security-related patches within 5 business days of patch availability, and that all systems should be patched within 30 days.

IRS improved change controls for its mainframe environment. Specifically, during fiscal year 2014, the agency substantially reengineered its control architecture for its automated mainframe change management process by limiting access to files for individuals who do not have systems administrative duties.

Although IRS has change control and patch management processes in place, it did not effectively enforce its change control or patch management procedures. For example, IRS did not maintain change control documentation demonstrating that configuration changes to a utility used to transfer data were properly approved prior to their implementation. By not enforcing change controls in this production system, the integrity and availability of IRS’s data and systems are jeopardized. Also, IRS did not effectively apply security patch updates in a timely manner. For example, at the time of our site visit in June 2014, IRS had not applied critical security patches to the database supporting a payroll application and the database supporting its access request and approval system, even though some of these patches had been available since January 2014. By not installing critical patches in a timely manner,

IRS did not always appropriately segregate incompatible duties

IRS increases the risk that known vulnerabilities in its systems may be exploited.

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. Conversely, 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.

IRS developed policies for dividing and separating incompatible duties and responsibilities. The *Internal Revenue Manual* requires that the agency divide and separate duties and responsibilities of functions among different individuals in order to prevent harmful activity without collusion. According to the manual, separation of duties includes dividing mission functions and distinct information system support functions among different individuals or roles, and conducting information system support functions with different individuals.

IRS generally implemented appropriate segregation of duties controls, but did not always divide system support functions. The agency implemented controls to prevent the assignment of incompatible database and system access privileges that could allow for the compromise of segregation of duties controls. However, for one key system we reviewed, a developer had access to the production environment, allowing an incompatible duty between system support functions. As a result, IRS is at an increased risk that an unauthorized individual could modify the production environment.

IRS had contingency plans in place, but did not always adhere to its approved plans

Contingency planning includes developing, testing, and maintaining contingency plans to ensure that when unexpected events occur, critical operations can continue without interruption or can be promptly resumed, and that information resources are protected. Further, contingency

planning also includes determining for each system, based on an accepted level of risk, an appropriate recovery point objective (RPO).¹⁰

IRS developed policies for developing information system contingency plans. 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 provide for the recovery and reconstitution of information systems to a known state after a disruption, compromise, or failure. Further, the manual requires all IRS systems and applications to have sufficient capability to recover systems and information according to agreed upon, pre-defined RPOs, as documented in the information system contingency plans.

Although IRS had processes in place to ensure recovery of its information system resources through continuity of operations, which included contingency plans and associated test plans, the agency did not always adhere to its contingency plans. For the nine contingency plans we reviewed, the agency had documented, tested, and generally maintained the plans. However, for the systems associated with two of these nine plans, although IRS was backing up the data on these systems, the agency was not backing up the systems to reflect the approved RPO. Specifically, the approved RPO for its access request and approval system was 4 hours, but IRS was conducting backups in intervals larger than 4 hours, leaving potential data loss gaps larger than what management had approved as allowable. In addition, for its network boundary systems, the approved RPO was 12 hours; however, IRS was only conducting backups every 24 hours, leaving a gap of 12 hours.

Until IRS ensures that it consistently backs up its systems in accordance with approved RPOs, the agency will not have reasonable assurance that it will be able to recover data in a manner that meets agency needs.

¹⁰The RPO represents a point in time, prior to a disruption or system outage, to which data must be recovered after an outage. It covers the maximum amount of data that can be lost before there is an unacceptable impact on other system resources, applications, business processes, or the mission of the organization. RPOs are often used as the basis for the development of a backup strategy and to determine the amount of data that might need to be recreated after the systems or functions have been recovered.

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 agency-wide information security program, it had not effectively implemented elements of it.

An agency-wide 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 the following components:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or 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 or group of information systems, as appropriate;
- 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; and
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, or practices of the agency.

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,¹¹ effective continuous monitoring begins with development of a strategy that addresses requirements and activities at each organizational tier.

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 *Internal Revenue Manual* requires that the agency identify and document threats, vulnerabilities, and potential impacts and review the results at least annually. We reviewed 10 risk assessments and found that they included information related to the identification of threats, vulnerabilities, and potential impacts to agency operations and were updated annually.
- 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 processes in place for providing employees with security awareness and specialized training.
 - According to IRS, almost 99 percent of the agency's employees completed required security awareness training in 2014.

¹¹National Institute of Standards and Technology, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, Special Publication (SP) 800-137 (Gaithersburg, Md.: September 2011).

-
- With minor exceptions, the agency documented and monitored employees with significant security responsibilities to ensure they were provided specialized training.
 - The agency had implemented numerous processes for testing and evaluating the effectiveness of controls, and told us that, through these processes, it had already identified many of the issues we raise in this report.
 - IRS had fully documented its continuous monitoring strategy that addresses requirements and activities at each organizational tier.

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, and continuity of operations, shortcomings existed with policies and procedures. For example:
 - IRS had not updated policies and procedures to ensure that they address (1) 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.¹²
 - IRS procedures did not specify the information required to be recorded in the documentation for important mainframe system processes. Absent this system documentation, the effectiveness of monitoring of these important automated processes is diminished. We previously made a recommendation to address this issue.¹³

¹²GAO, *Information Security: IRS Has Improved Controls but Needs to Resolve Weaknesses*, [GAO-13-350](#) (Washington, D.C.: March 2013).

¹³GAO, *Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk*, [GAO-14-405](#) (Washington, D.C.: April 2014).

-
- Although IRS has a policy establishing the minimum mandatory security settings for its mainframe operating systems, the policy was not comprehensive. According to the mainframe manufacturer, policy should address who can administer the security software configurations that control access to mainframe programs. However, IRS's mainframe security policy did not address who can administer these configurations.
 - The agency did not always ensure that contractors received security awareness training. The *Internal Revenue Manual* requires that all new contractors receive security awareness training within 5 business days of receiving system access. According to IRS officials, processes for ensuring contractors received required training within 5 business days were not in place.
 - 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. Shortcomings existed in IRS's testing and evaluation process as illustrated by the following:
 - Test and evaluation procedures did not ensure that control testing methodology and results fully met the intent of the control objectives being tested for three systems that we reviewed. For example, for one of the three systems, the agency documented it had met one of its risk assessment control objectives without performing any testing for that objective.
 - IRS had not yet updated mainframe test and evaluation processes to improve monitoring of compliance with policies. We previously made recommendations to address this issue.¹⁴

As a result, IRS had not identified key issues raised in this report, including weaknesses involving unauthorized system access and missing patches.

- The *Internal Revenue Manual* requires that system security authorizations be updated whenever there is a significant change to

¹⁴[GAO-13-350](#).

the operating environment.¹⁵ However, IRS did not update the security authorization for the access request and approval system to reflect the significant changes to the operating environment.

Although IRS had a remedial process in place, it did not ensure that corrective actions had been effectively implemented. The *Internal Revenue Manual* requires that the agency verify that each weakness is corrected before closing that item. IRS has a remedial action verification process in place to verify that weaknesses are corrected before closing them, but the process did not always ensure corrective actions were fully implemented. Specifically, IRS informed us that it had addressed 24 of the 69 weaknesses we previously identified that remained unresolved at the end of our fiscal year 2013 audit; however, we found that the agency had only resolved 14 of the 24 weaknesses IRS said it had mitigated.

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 made progress in implementing information security controls; however, weaknesses in the controls limited their effectiveness in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer data. During fiscal year 2014, IRS management continued to devote attention and resources to addressing information security controls, and resolved a 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 vulnerable until the agency (1) addresses weaknesses pertaining to identification and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning and (2) effectively implements elements of its information security program, including updating policies, test and evaluation procedures, remedial action procedures, and a security authorization, as well as ensuring contractors receive security awareness

¹⁵Security authorization is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk, which has been determined based on the testing of security controls.

training. 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 2014. 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 five actions to effectively implement key elements of the IRS information security program:

- Update the policy for mainframe security to ensure that it addresses who can administer the security software configurations that control access to mainframe programs.
- Ensure contractors receive security awareness training within 5 business days of being granted access to an IRS information system.
- Ensure that control testing methodology and results fully meet the intent of the control objectives being tested.
- Update the security authorization for the access request and approval system to reflect the significant changes to the operating environment.
- Update the remedial action verification process to ensure actions are fully implemented.

We are also making 14 technical recommendations in a separate report with limited distribution. These recommendations address information security weaknesses related to identification and authentication, authorization, cryptography, physical security, configuration management, segregation of duties, and contingency planning.

Agency Comments and Our Evaluation

In providing written comments (reprinted in app. II) on a draft of this report, the Commissioner of Internal Revenue stated that the agency remains committed to its ongoing programs to manage the security risks in its information technology infrastructure. He stated that IRS will review all of GAO's reported recommendations associated with this report, and will evaluate them in light of its security controls and processes currently in place, associated risks, and recent budget constraints, and provide corrective action plans where appropriate to address the recommendations. Further, the Commissioner stated that the security and

privacy of taxpayer information and the integrity of IRS's financial systems continue 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 its statement of action to serve as preliminary information on the status of open recommendations.

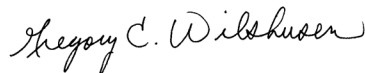
We are also sending copies of this report to the Secretary of the Treasury, the Treasury Inspector General for Tax Administration, and interested congressional parties.

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
Managing Director, Applied Research and Methods



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objective, Scope, and Methodology

The objective of our review was to determine whether controls over key financial and tax processing systems were effective in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer information at the Internal Revenue Service (IRS). To do this, we examined IRS information security policies, plans, and procedures; tested controls over key financial applications; and interviewed key agency officials. 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 2014 and 2013 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 an IRS facility in New Carrollton, Maryland. 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*,¹ 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 systems and databases to determine if strong password management was being enforced;
- examining IRS's implementation of encryption to secure transmissions on its internal network;

¹GAO, *Federal Information System Controls Audit Manual* (FISCAM), [GAO-09-232G](#) (Washington, D.C.: February 2009).

- 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 of 2002*,² which established elements for an agency-wide 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;

²In December 2014, subsequent to our evaluation of controls, FISMA (FISMA '02) was partially superseded by enactment of the *Federal Information Security Modernization Act of 2014* (FISMA '14), Pub. L. No. 113-283 (Dec. 18, 2014). The new law incorporates and continues the requirements from FISMA '02 applicable to IRS that we relied upon in our report. Accordingly, no changes to our findings were necessary.

- 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; and
- reviewing continuity-of-operations planning documentation for nine 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 2014 to March 2015 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



COMMISSIONER

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

March 11, 2015

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 Continue Improving Controls over Financial and Taxpayer Data* (GAO-15-337).

We are pleased the Government Accountability Office (GAO) recognized our progress in addressing a number of information technology (IT) security areas to include improving configuration and change controls in the mainframe environment, upgrading encryption across the network, and enabling a more secure communications environment for sensitive data. The security and privacy of taxpayer information and the integrity of our financial systems continues to be sound, and we remain committed to our ongoing programs to manage the security risks in our IT infrastructure as required by the Federal Information Security Management Act, National Institute of Standards and Technology guidance, and other appropriate standards. Our commitment to these standards and our efforts to address identified weaknesses is evidenced not only by the progress you noted in this report, but also by the fact that we continue to decrease the number of unresolved weaknesses.

We will review all of GAO's reported recommendations associated with this report, and will evaluate them in light of our security controls and processes currently in place, associated risks, and recent budget constraints. We will provide corrective action plans where appropriate to address recommendations with our response to the final report.

In closing, we appreciate your continued support and guidance as we strive to maintain effective security controls over IRS's financial and tax processing systems 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,

A handwritten signature in blue ink, appearing to read "John A. Koskinen".

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, Lon Chin, David Hayes, and Jeffrey Knott (assistant directors), Mark Canter, Nancy Glover, Mickie Gray, Charles Hubbard, Linda Kochersberger, J. Andrew Long, Kevin Metcalfe, Tyler Mountjoy, Eugene Stevens, Michael Stevens, and Daniel Swartz made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's 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

