United States Government Accountability Office

Report to the Commissioner of Internal Revenue

March 2016

INFORMATION SECURITY

IRS Needs to Further Improve Controls over Financial and Taxpayer Data

Accessible Version

GAO-16-398

March 2016

INFORMATION SECURITY

IRS Needs to Further Improve Controls over Financial and Taxpayer Data

GAO Highlights

Highlights of GAO-16-398, a report to the Commissioner of Internal Revenue

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 2015 and 2014 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 locations.

What GAO Recommends

In addition to the prior recommendations that have not been implemented, GAO is recommending that IRS take 2 additional actions to more effectively implement security-related policies and plans. In a separate report with limited distribution, GAO is recommending 43 actions that IRS can take to address newly identified control weaknesses. In commenting on a draft of this report, IRS agreed with our recommendations.

View GAO-16-398. For more information, contact Nancy 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) 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 2015, IRS continued to devote attention to securing its information systems that process sensitive taxpayer and financial information. Key among its actions were further restricting access privileges on key financial applications and continuing its migration to multifactor authentication across the agency. However, significant control deficiencies remained. For example, the agency had not always (1) implemented controls for identifying and authenticating users, such as applying proper password settings; (2) appropriately restricted access to servers; (3) ensured that sensitive user authentication data were encrypted; (4) audited and monitored systems to ensure compliance with agency policies; and (5) ensured access to restricted areas was appropriate. In addition, unpatched and outdated software exposed IRS to known vulnerabilities.

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 had not yet been effectively implemented. For example, IRS had not updated key mainframe policies and procedures to address issues such as comprehensively auditing and monitoring access. In addition, IRS did not include sufficient detail in its authorization procedures to ensure that access to systems was appropriate. Further, IRS had not ensured that many of its corrective actions to address previously identified deficiencies were effective. For example, for the 28 prior recommendations that IRS informed us that it had addressed, 9 of the associated weaknesses had not been effectively corrected.

Until IRS takes additional steps to (1) address unresolved and newly identified control deficiencies and (2) effectively implement 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 2015.

Contents

Abbreviations

CIO	chief information officer
FISMA	*Federal Information Security Modernization Act*
HSPD-12	*Homeland Security Presidential Directive 12*
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	plan of action and milestones
TIGTA	Treasury Inspector General for Tax Administration

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 28, 2016

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 2015 and 2014 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 2015 and 2014 financial statements, during fiscal year 2015 IRS continued to focus on securing its information systems and protecting sensitive taxpayer and financial information. Key actions taken by IRS were further restricting access privileges on key financial applications and continuing its migration to multifactor authentication across the agency.

However, the collective effect of the deficiencies in information security from prior years that continued to exist in fiscal year 2015, along with the

[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, systems are securely configured to avoid exposure to known vulnerabilities, and backup and recovery plans are adequate and tested to ensure the continuity of essential operations.

[2]GAO, *Financial Audit: IRS's Fiscal Years 2015 and 2014 Financial Statements*, GAO-16-146 (Washington, D.C.: Nov. 12, 2015).

new deficiencies we identified during this year's audit (discussed in this report), are serious 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, 2015.[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 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, relying on systems to carry out their operations of processing, maintaining, and reporting large volumes of sensitive data, such as personal information. Accordingly, information security is a critical consideration for any government agency that depends on information systems and computer networks to carry out its mission and is especially

[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.

important for government agencies such as IRS, 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 individuals, groups, and countries who wish to do harm to an organization's systems.

For example, in June 2015, the Commissioner of the IRS testified that unauthorized third parties had gained access to taxpayer information from its "Get Transcript" application. According to officials, criminals used taxpayer-specific data acquired from non-department sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included Social Security information, dates of birth, and street addresses. In an August 2015 update, the IRS reported this number to be about 114,000, and that an additional 220,000 accounts had been inappropriately accessed, which brings the total to about 330,000 accounts. In a February 2016 update, the IRS reported that an additional 390,000 accounts had been inappropriately accessed, which brings the total to about 720,000.[4]

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, since 1997, we have designated federal information security as a government-wide high-risk area.[5] Most recently, in the February 2015 update to our High-Risk list, we expanded this

[4]The "Get Transcript" application was not within the scope of our review.

[5]GAO, *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).

area to include protecting the privacy of personally identifiable information[6]—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities.[7]

Federal Law and Guidance Provide a Framework for Protecting Federal Information and Systems

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*[8] 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.[9] 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 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).

Federal law and guidance specify requirements for protecting federal information and systems. The *Federal Information Security Modernization*

[6]Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, or mother's maiden name, and any other personal information that is linked or linkable to an individual.

[7]See GAO-15-290.

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

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

Act (FISMA)[10] is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. To accomplish this, FISMA requires each agency to develop, document, and implement an agencywide information security program to provide information security for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management. Such a program includes assessing risk; developing and implementing cost-effective security plans, policies, and procedures; 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 (NIST) 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 2015 and 2014, IRS collected about $3.3 trillion and $3.1 trillion, respectively, in federal tax payments, processed about 201 million and 199 million, respectively, in tax and information returns, and paid about $403 billion and $374 billion, respectively, in refunds to taxpayers. Further, the size and complexity of IRS add unique operational challenges.

[10]The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) partially superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

IRS employs approximately 90,000 people (who include temporary and seasonal staff) in its Washington, D.C., headquarters and more than 550 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 two enterprise computing centers located in 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 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 2015, the Treasury Inspector General for Tax Administration (TIGTA) stated that security for taxpayer data, including securing computer systems, was the top priority in its list of top ten management challenges for IRS for fiscal year 2016.[11]

[11]Treasury Inspector General for Tax Administration, *Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2016*, Memorandum for Secretary Lew (Washington, D.C.: October 2015).

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 automated mechanisms centrally manage, apply, and verify configuration settings. The manual also

requires that *Homeland Security Presidential Directive 12* (HSPD-12)[12] - compliant multifactor authentication be implemented for local and network access accounts. In addition, it states that password complexity is required for all IRS information systems with password-based authentication and specifies how passwords are to be configured. This includes passwords that are not found in the dictionary and contain at least one numeric character, one special character, a mixture of at least one uppercase and one lowercase letter, and that passwords be set to expire at a maximum of 90 days or sooner for people and within 366 days for service accounts. Further, the manual states that the creation and usage of generic accounts shall not be permitted.

IRS improved identification and authentication controls for its computing environments. For example, IRS expanded the use of an automated mechanism to centrally manage, apply, and verify configuration settings such as password requirements including password length and complexity, for its Windows environment.

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

- While IRS has continued to expand the use of two-factor HSPD-12 access for identification and authentication to its network, in a September 2015 report, TIGTA reported that the IRS had not fully implemented unique user identification and authentication or remote electronic authentication that complies with HSPD-12 requirements.[13]

- The agency used passwords that could be easily guessed on servers supporting its procurement system, access request and approval system, system used to support the administration of automated file transfers of financial data, system used for the access and

[12]In 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 government-wide standard for secure and reliable forms of identification for federal government employees and contractor personnel who access government-controlled facilities and information systems.

[13]Treasury Inspector General for Tax Administration, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015*, 2015-20-092 (Sept. 25, 2015).

management of taxpayer accounts, system used to process electronic tax payment information, as well as one of its human resource management systems.

- IRS did not ensure that all user account passwords were set to expire every 90 days or sooner on 2 of 13 databases reviewed.
- The agency had not consistently applied proper password settings to service accounts. For example, out of 112 mainframe service accounts detected, none were configured to require a password change. In addition, of the 40 service accounts on a server that supports the administration of automated file transfers of financial data, 2 were not set to expire within 366 days.
- The agency used a shared generic account, created during installation, to administer an application.

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

Users have more system access than needed to perform their jobs

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.

Although IRS had taken steps to control access to some systems, it continued to permit excessive access to others. IRS had corrected a previously identified weakness by properly restricting user access to sensitive configuration files on the system supporting the administration of automated file transfers of financial data. However, it continued to permit excessive access to 11 of 14 systems reviewed by granting rights and permissions that gave users more access than they needed to perform

their assigned functions. For example, 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, exceeding the access needed to support their job duties. In addition, although IRS corrected another previously identified weakness by restricting user access to several sensitive database packages[14] that allowed them to manipulate data and gain access to sensitive files and directories on its access authorization, administrative accounting, and procurement systems, IRS did not restrict user access to a sensitive database package on one of its human resource management systems.

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

IRS continued to expand its use of encryption, but did not encrypt sensitive user authentication data

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 has established policies for encrypting data. The *Internal Revenue Manual* states that IRS shall implement cryptographic mechanisms to prevent the unauthorized disclosure of information (confidentiality) and to detect changes to information (integrity). The manual also requires that IRS implement encryption mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal

[14]According to Oracle, a package is an encapsulated collection of related program objects stored together in the database. Program objects are procedures, functions, variables, constants, cursors, and exceptions.

laws, executive orders, directives, policies, regulations, standards, and guidance for such standards.

IRS continued to expand its use of encryption to protect sensitive data, but cryptography control weaknesses continued. For example, while IRS made progress in its implementation of encryption controls by configuring a system used to support scheduling and workload monitoring tasks of the mainframe to encrypt user authentication, 11 systems we reviewed had not been configured to encrypt sensitive user authentication data. By not encrypting sensitive user authentication data, increased risk exists that an unauthorized individual could view and then use the data to gain unwarranted access to its system or sensitive information.

Although IRS had enhanced its audit and monitoring capabilities, audit plans were outdated

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 and that audit logs be reviewed and communicated with the appropriate personnel within a timely manner. The manual also requires that audit plans, which are to be used to document system and application-specific auditing and monitoring requirements, be developed for all systems and applications required to have a plan, and that the plans be updated to reflect the current version of referenced policies and guidelines and when significant changes are made to a system or application.

IRS continued to enhance its audit and monitoring capability, but weaknesses remain. IRS configured logging capabilities for selected systems. For example, the agency had implemented an automated mechanism to log user activities on its access request and approval system. However, shortcomings existed in audit and monitoring controls.

For example, the agency had not enabled logging for two key applications used to support the administration of automated file transfers of financial data and to access and manage taxpayer accounts. In addition, IRS did not consistently review mainframe security events. Further, IRS was not consistently maintaining key system and application audit plans. Audit plans for 11 systems we reviewed reflected prior versions of IRS policies, NIST guidance, and industry security publications and at least 2 of the 11 audit plans had not been updated since significant changes were made to their respective systems' operating environment.

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 control over unissued keys or other entry devices. At IRS, physical access control measures, such as physical access cards that are used to permit or deny access to certain areas of a facility, are vital to safeguarding its facilities, computing resources, and information from internal and external threats.

IRS developed and documented policies for physically protecting its computer resources. The *Internal Revenue Manual* requires access controls to protect employees and contractors, information systems, and the facilities in which they are located. Further, the manual 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, but weaknesses remain. IRS implemented physical security measures to safeguard its assets against possible theft and malicious actions. For example, IRS had a dedicated guard force at each of its computing centers to, among other things, aid in controlling physical access to restricted areas. However, physical security weaknesses identified during previous audits remain unresolved. For example, IRS has yet to address weaknesses pertaining to its review of authorized access lists to sensitive areas for both employees and visitors at one of

its computing centers. 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

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 and planning for continuity of operations.

Although IRS improved its change management process, 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 information systems or enabling users to have access to greater privileges than authorized.

IRS developed policies for managing the configuration of its information technology systems. The *Internal Revenue 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, and that configuration change decisions be documented and associated records retained for a period of 3 years. 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. 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 improved some configuration management controls, weaknesses continued to exist in its patch management process. IRS improved change controls for its system that supports the administration of automated file transfers of financial data. Specifically, IRS corrected a previously identified weakness by ensuring requests and approvals for configuration changes made to the system were documented and retained. In addition, although IRS had patch management processes in place, it did not always ensure security patch updates were applied to its systems in a timely manner. For example, at the time of our site visit in June 2015, databases supporting 2 of the 12 systems we reviewed had not been updated with the latest critical patches. At least one of the critical patches that had not been applied had been available since August 2012. By not installing critical patches in a timely manner, IRS increases the risk that known vulnerabilities in its systems may be exploited.

Further, although IRS corrected a previously identified weakness by upgrading an unsupported software application on its workstations to a vendor-supported version of the software, since April 2011 the agency has continued to use unsupported database software on a system used to access and manage taxpayer accounts. 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 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.[15]

[15]The recovery point objective 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. Recovery point objectives 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 policies for developing information system contingency plans. The *Internal Revenue Manual* requires the agency to develop contingency plans for all information systems and to test the plans to determine their effectiveness and the agency's readiness to execute the plans. The manual also requires the agency to 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 consistent with the recovery point objectives, as documented in the information system contingency plans.

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. For the ten contingency plans we reviewed, the agency had documented and tested the plans. In addition, IRS improved continuity of operations controls for its access request and approval system as well as for its network boundary systems. Specifically, IRS had corrected a previously identified weakness by ensuring that information on these systems was being backed up in accordance with approved recovery point objectives.

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 had a comprehensive framework for its information security program, some aspects of it continued to be ineffectively implemented.

An 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. In accordance with their responsibilities under FISMA, each agency is required 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;
- 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; and
- procedures for detecting, reporting, and responding to security incidents.

IRS had documented risk assessments

According to NIST Special Publication 800-30 Revision 1,[16] risk is determined by identifying potential threats to the organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data. Identifying and assessing information security risks are essential to determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that the policies and controls operate as intended. The *Internal Revenue Manual* requires that the agency identify and document threats, vulnerabilities, and potential impacts and review the results at least annually.

IRS had developed and documented an information technology security risk management policy that required all sensitive applications to be

[16]National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, Special Publication 800-30 Revision 1 (Gaithersburg, Md.: September 2012).

periodically assessed for the risk and magnitude of harm that could result from vulnerabilities and potential threats. We reviewed ten 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.

IRS had developed and documented policies and procedures covering multiple information security components, but some had not been fully developed, documented, or updated

A key element of an effective information security program is to develop, document, and implement risk-based policies, procedures, and technical standards that govern the security of an agency's computing environment. If properly developed and implemented, policies and procedures should help reduce the risk associated with unauthorized access or disruption of services. Technical security standards can provide consistent implementation guidance for each computing environment. Developing, documenting, and implementing security policies are the primary mechanisms by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls. In addition, agencies need to take the actions necessary to effectively implement or execute these procedures and controls. Otherwise, agency systems and information will not receive the protection that the security policies and controls should provide.

Although IRS had developed and documented its information security policies and procedures covering multiple information security components, including risk assessment, security planning, security training, testing and evaluating information security controls, and contingency planning, we noted instances where documentation had not been fully developed, documented, or updated for systems that we reviewed. For example:

- IRS had not updated policies and procedures to ensure that they address, among other things, (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, and (5) reconciliation of access privileges. We previously made a recommendation to address these issues.[17]

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

- IRS did 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 online access request and approval system. As a result, individual users' access privileges for both mainframe and distributed computing-based applications cannot be accurately verified, increasing the likelihood that erroneous and outdated access privileges will not be detected. We previously made a recommendation to address these issues.[18]

- 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 these important automated processes is diminished. We previously made a recommendation to address this issue.[19]

- IRS's mainframe security policy did not address who can administer the security software configurations that control access to mainframe programs. 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. We previously made a recommendation to address this issue.[20]

Without comprehensive and fully documented policies and procedures, IRS has limited assurance that staff will consistently implement effective controls over systems and that its information systems will be protected as intended. Further, as illustrated by the weaknesses identified in this report, IRS has not yet fully implemented its policies, standards, and guidelines.

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

[19]GAO-14-405.

[20]GAO, *Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data*, GAO-15-337 (Washington, D.C.: March 2015).

Security plans were developed and documented, but a security plan had not been updated to reflect changes to the operating environment

An objective of system security planning is to improve the protection of information technology resources. A system security plan provides an overview of the system's security requirements and describes the controls that are in place or planned to meet those requirements. The Office of Management and Budget Circular A-130 requires that agencies develop system security plans for major applications and general support systems, and that these plans address policies and procedures for providing management, operational, and technical controls. Furthermore, the *Internal Revenue Manual* requires that security plans be reviewed, at a minimum, annually or as a result of a significant change and updated to address changes to the information system, the system's environment of operation, or problems identified during plan implementation or security control assessments.

Although the agency had developed and documented security plans for the major systems that we reviewed, one of the plans had not been appropriately updated. All of the plans addressed policies and procedures for providing management, operational, and technical controls. However, for 1 of 11 security plans we reviewed, IRS had not updated the plan to reflect changes to the operating environment. This plan covered systems that provide network infrastructure services to IRS personnel and information systems. Without an updated system security plan, IRS cannot ensure that the most appropriate security controls are in place to protect its critical information.

IRS did not always ensure that contractors received security awareness and specialized training

People are one of the weakest links in attempts to secure systems and networks. Therefore, an important component of an information security program is providing sufficient training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks. The *Internal Revenue Manual* requires that users be trained on topics including recognizing and reporting potential indicators of insider threat and ensuring workstations are adequately protected from theft, particularly in regard to a laptop being used as a workstation. The manual also requires that security awareness training be provided to all information system users, including employees and contractors, within 5 business days of being granted access to an IRS information system and annually thereafter. Further, it requires that role-based security training be provided to personnel assigned security roles and responsibilities, that security training activities be documented and monitored, and that personnel requiring specialized training meet a minimum number of hours of role-based security training per year, depending on their specific role.

IRS had processes in place for providing employees with security awareness training, but not for ensuring its contractors receive the training in a timely manner. We performed a content review of IRS's fiscal year 2015 security awareness training program and found that it included information on security risks including recognizing and reporting potential indicators of insider threat and ensuring that workstations are adequately protected from theft. According to IRS, almost 99 percent of the agency's employees completed the required security awareness training for fiscal year 2015.[21] However, we have previously made a recommendation for IRS to address deficiencies in contractors receiving timely security awareness training.[22] In fiscal year 2015, the agency indicated that it had not yet addressed this issue.

IRS also had processes in place for providing employees with specialized training. For the 45 employees with security roles and responsibilities that we reviewed, all received the required security training and met the minimum number of hours of role-based security training, based on their specific role. However, in September 2015, TIGTA reported that the IRS did not identify and track the status of specialized training for all of its contractors with significant information security responsibilities who require specialized training.[23]

Without adequately ensuring that contractors take required security awareness and specialized training, IRS faces an increased risk that contractors may not recognize and respond appropriately to potential security threats and vulnerabilities.

Tests and evaluations of policies, procedures, and controls were not always effective

Another 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. This type of oversight is fundamental because it demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies areas of noncompliance and ineffectiveness. Although tests and evaluations of policies, procedures, and controls may encourage compliance with security policies, the full benefits are not achieved unless the results improve the security program

[21]We did not perform testing of employees completing required security awareness training.

[22]GAO-15-337.

[23]Treasury Inspector General for Tax Administration, 2015-20-092.

through implementation of compensating or mitigating controls if needed. The *Internal Revenue Manual* requires management testing and evaluation of the effectiveness of information security policies and procedures. It further requires that the agency assess the security controls in an IRS information system and its environment of operations at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.

IRS had implemented numerous processes for testing and evaluating the effectiveness of policies, procedures, and controls to determine whether they are effective and operating as intended, and told us that it had previously identified many of the issues we raised this fiscal year. In addition, the agency had processes in place to verify configuration management compliance. For example, in addition to tests and evaluations conducted on a yearly basis, IRS used an automated compliance verification tool to periodically test compliance with its security policies for its UNIX environment, including testing whether appropriate security patches had been applied.

However, shortcomings existed in IRS's testing and evaluation processes, as illustrated by the following:

- IRS had not updated mainframe test and evaluation processes to improve monitoring of compliance with policies. We previously made a recommendation to address this issue.[24]

- Test and evaluation procedures did not ensure that control testing methodology and results fully met the intent of the control objectives being tested for two of the three system control test procedures and results that we reviewed. For example, for one of the two systems, the agency documented that it had met one of its risk assessment control objectives without performing any testing for that objective. We previously made a recommendation to address this issue.[25]

Because of the shortcomings in the testing and evaluation processes, IRS may not be fully aware of vulnerabilities that could adversely affect critical applications and data.

[24]GAO-13-350.

[25]GAO-15-337.

Shortcomings existed in IRS's remedial process

A remedial action plan is a key component of an agency's information security program, as described in FISMA. Such a plan, also known as a plan of action and milestones (POA&M), assists agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses that are found in information systems. According to the *Internal Revenue Manual*, the agency should document weaknesses found during security assessments in a POA&M, as well as planned, implemented, and evaluated remedial actions to correct any deficiencies. IRS policy further requires tracking the resolution status of all weaknesses and verification that each weakness is corrected before closing that item.

Although IRS had a remedial process in place, it did not ensure that corrective actions had been effectively implemented. During fiscal year 2015, IRS made progress toward correcting previously reported information security weaknesses, correcting or mitigating 21 of the 70 previously identified weaknesses that were unresolved at the end of our prior audit.[26] However, at the time of our review, 49 of 70—about 70 percent—of the previously reported weaknesses remained unresolved or unmitigated, of which 7 of the 70 weaknesses have been unresolved since 2012.

Further, the agency's process for verifying whether an action had corrected or mitigated the weakness was not working as intended. Specifically, for the 28 prior recommendations that IRS informed us that it had addressed, 9 of the associated weaknesses had not been effectively corrected. In addition, in September 2015, TIGTA reported that the IRS did not always ensure that weaknesses were corrected prior to POA&M closure.[27] We previously made a recommendation to address this issue.[28]

Until the agency takes additional steps to implement a more effective verification process, it will have limited assurance that weaknesses are being properly mitigated or corrected and that controls are operating effectively.

[26]GAO-15-337.

[27]Treasury Inspector General for Tax Administration, 2015-20-092.

[28]GAO-15-337.

IRS had a security incident response process in place

Security incident response is an important component of information technology programs. According to NIST, cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. Because not all incidents can be prevented, an incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. Therefore, an important component of an information security program is procedures for detecting, reporting, and responding to security incidents. The *Internal Revenue Manual* requires the implementation of an incident handling capability for incidents and requires that incidents be categorized, documented, and tracked.

IRS had a process in place to ensure that its Computer Security Incident Response Center tracked and documented cybersecurity-related incidents in accordance with IRS's policies and procedures governing incident handling and response. We reviewed 45 incident tickets and determined that each had been opened, managed, and closed by center personnel and handled according to its proper incident categorization.

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 2015, 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 (including associated audit plans), physical security, and configuration management and (2) effectively implements elements of its information security program, including updating its security plan to reflect the current operating environment. 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 2015. 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 two actions to more effectively implement security-related policies and plans:

- Update system and application audit plans based on the current version of referenced policies and guidelines and when significant changes are made to a system or application.
- Update the security plan for systems that provide network infrastructure services to IRS personnel and information systems to reflect changes to the operating environment.

We are also making 43 technical recommendations in a separate report with limited distribution. These recommendations address information security control weaknesses related to identification and authentication, authorization, cryptography, audit and monitoring, and configuration management.

Agency Comments and Our Evaluation

We provided a draft of this report to the IRS for review and comment. In its written comments, reproduced in appendix II, the Commissioner of Internal Revenue stated that although IRS agrees with our recommendations, they plan to review them to ensure that their actions include sustainable fixes that implement appropriate security controls. In addition, he stated that the security and privacy of taxpayer information is of the utmost importance to the agency and that he was pleased that the draft report recognized the progress IRS has made in addressing a number of information security areas. Further, he noted that IRS is currently in the process of implementing numerous additional safeguards.

The Commissioner also asserted 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

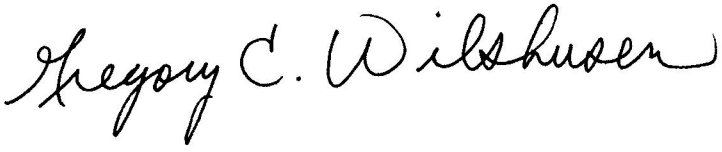
Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform not later than 60 days from the date of the report and to the House and Senate Committees on Appropriations, with the agency's first request for appropriations made more than 60 days after the date 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 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 assess the effectiveness of corrective actions taken by IRS to address weaknesses we previously reported and determine whether any additional weaknesses existed. This work was performed in connection with our audit of IRS's fiscal years 2015 and 2014 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 two enterprise computing centers located in Martinsburg, West Virginia, and Memphis, Tennessee, as well as IRS facilities in Detroit, Michigan, and 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;

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

- 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; and
- examining the status of patching for key databases and system components to ensure that patches are up-to-date.

Using the requirements in the *Federal Information Security Modernization Act of 2014*,[2] 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 assessments were being performed at least annually;
- reviewing IRS's policies, procedures, practices, and standards to determine whether its security management program had been documented, approved, and was up-to-date;

[2]The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) partially superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

- 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;
- examining documentation to determine the extent to which IRS was performing internal controls reviews of key financial systems;
- 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 cybersecurity-related incidents were being handled as required by IRS's policies and procedures governing incident handling and response and as outlined by the National Institute of Standards and Technology; and
- reviewing continuity-of-operations planning documentation for ten 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 two computing centers, whether information security controls were in place, adequately designed, and operating effectively.

We performed our audit 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 15, 2016

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

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report entitled, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data* (GAO-16-398).

We are pleased GAO recognized our progress in addressing a number of information technology security areas. The IRS successfully executed another filing season that included the development, testing, and release of a large number of tax modifications including many late legislative changes; participated in the Office of Management and Budget's (OMB) Cyber Sprint initiative; and made significant progress towards implementation of multi-factor authentication.

We also appreciate your willingness to provide more specificity in the recommendations associated with this audit. In prior years, some GAO recommendations were quite general in nature. While the increased level of detail has likely resulted in more recommendations, it will allow the IRS to better address cybersecurity risk.

As you know, the IRS is committed to improving its financial management, internal controls, information technology security posture, and the overall effectiveness of information system controls. Currently, the IRS is in the process of implementing numerous additional safeguards, many of which are outlined in OMB's Cybersecurity Strategy and Implementation Plan (CSIP), such as Continuous Diagnostics and Mitigation (CDM).

While we agree with GAO's recommendations, we will review them to ensure that our actions include sustainable fixes that implement appropriate security controls balanced against information technology and human capital resource limitations. We will provide the detailed corrective action plan addressing each of the recommendations in our 60 day letter response to Congress.

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 and implement 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, Lon Chin, David Hayes, and Jeffrey Knott (assistant directors), Mark Canter, Kristi Dorsey, Nancy Glover, Mickie Gray, Tyrone Hutchins, Kevin Metcalfe, Eugene Stevens, Michael Stevens, Daniel Swartz, and Marshall Williams, Jr. made key contributions to this report.

Appendix IV: Accessible Data

Agency Comment Letter

Text of Appendix II: Comments from the Internal Revenue Service

Page 1

DEPARTMENT OF THE TREASURY

INTERNAL REVENUE SERVICE

WASHINGTON, D.C. 20224

COMMISSIONER

March 15, 2016

Mr. Gregory C. Wilshusen

Director, Information Security Issues

U.S. Government Accountability Office (GAO)

441 G Street, N.W.

Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report entitled, Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data (GA0-16-398).

We are pleased GAO recognized our progress in addressing a number of information technology security areas. The IRS successfully executed another filing season that included the development, testing, and release of a large number of tax modifications including many late legislative changes; participated in the Office of Management and Budget1s (OMB) Cyber Sprint initiative; and made significant progress towards implementation of multi-factor authentication.

We also appreciate your willingness to provide more specificity in the recommendations associated with this audit. In prior years, some GAO recommendations were quite general in nature. While the increased level of detail has likely resulted in more recommendations, it will allow the IRS to better address cybersecurity risk.

As you know, the IRS is committed to improving its financial management, internal controls, information technology security posture, and the overall effectiveness of information system controls. Currently, the IRS is in the process of implementing numerous additional safeguards, many of which are outlined in OMB's Cybersecurity Strategy and Implementation Plan (CSIP), such as Continuous Diagnostics and Mitigation (COM).

While we agree with GAO's recommendations, we will review them to ensure that our actions include sustainable fixes that implement appropriate security controls balanced against information technology and human capital resource limitations. We will provide the detailed corrective action plan addressing each of the recommendations in our 60 day letter response to Congress.

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 and implement appropriate measures.

Page 2

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

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 and read The Watchblog.
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