United States Government Accountability Office

Report to the Commissioner of Internal Revenue

July 2017

INFORMATION SECURITY

Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data

GAO-17-395

July 2017

INFORMATION SECURITY

Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data

GAO Highlights

Highlights of GAO-17-395, a report to the Commissioner of Internal Revenue

Why GAO Did This Study

The IRS has a demanding responsibility to collect taxes, process tax returns, and enforce 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 2016 and 2015 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; tested controls over key financial applications; and interviewed key agency officials at four locations.

What GAO Recommends

In addition to the prior recommendations that have not been implemented, GAO is recommending that IRS take 10 additional actions to more effectively implement security-related policies and plans. In a separate report with limited distribution, GAO is recommending 88 actions that IRS can take to address newly identified control deficiencies. In commenting on a draft of this report, IRS neither agreed nor disagreed with the recommendations, but stated that it would review each of the recommendations and ensure that its corrective actions include sustainable fixes that implement appropriate security controls.

View GAO-17-395. For more information, contact Nancy R. Kingsbury at (202) 512-2700 or kingsburyn@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The Internal Revenue Service (IRS) made progress in addressing previously reported control deficiencies; however, continuing and newly identified control deficiencies limited the effectiveness of security controls for protecting the confidentiality, integrity, and availability of IRS's key financial and tax processing systems. During fiscal year 2016, IRS made improvements in access controls over a number of system administrator accounts and updated certain software to prevent exposure to known vulnerabilities. However, the agency did not always (1) limit or prevent unnecessary access to systems, (2) monitor system activities to reasonably assure compliance with security policies, (3) reasonably assure that software was supported by the vendor and was updated to protect against known vulnerabilities, (4) segregate incompatible duties, and (5) update system contingency plans to reflect changes to the operating environment.

An underlying reason for these control deficiencies is that IRS had not effectively implemented components of its information security program. The agency had a comprehensive framework for its program, including developing and documenting security plans; however, it did not fully implement other program components. For example, IRS did not always effectively manage information security risk or update certain policies and procedures. GAO has made recommendations to IRS to correct the identified security control deficiencies (see table). However, corrective actions for a number of the deficiencies have not been completed and the associated recommendations remained open at the conclusion of the audit of IRS's financial statements for fiscal year 2016.

Status of GAO Information Security Recommendations to IRS for Correcting Control Deficiencies at the Conclusion of Fiscal Year 2016 Audit

Information security control area	Prior recommendations open at the beginning of FY 2016 audit	Recommendations closed at the end of FY 2016 audit	New recommendations resulting from FY 2016 audit	Total outstanding recommendations at the conclusion of FY 2016 audit
Access controls	62	(12)	70	**120**
Other controls	22	(11)	21	**32**
Information security program	10	(3)	7	**14**
Total	**94**	**(26)**	**98**	**166**

Legend: FY = fiscal year

Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-17-395

Until IRS takes additional steps to address unresolved and newly-identified control deficiencies and effectively implements components of its information security program, its financial reporting 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 2016.

Contents

Abbreviations

GSS	general support system
CIO	chief information officer
FISMA	*Federal Information Security Modernization Act of 2014/Federal Information Security Management Act of 2002*
FMFIA	*Federal Managers' Financial Integrity Act*
ID	identification
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	plan of action and milestones
SSAE	Statement on Standards for Attestation Engagements
TIGTA	Treasury Inspector General for Tax Administration

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

July 26, 2017

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 2016 and 2015 financial statements, 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 2016 and 2015 financial statements,[2] during fiscal year 2016, the agency made progress addressing previously reported control deficiencies related to its financial reporting systems. Key among its corrective actions were improvements in access controls over certain system administrator accounts and updates to certain software to prevent exposure to known vulnerabilities.[3]

[1]Information security controls include logical and physical access controls, configuration management, segregation of duties, and continuity of operations. These controls are designed to ensure that access to data is appropriately restricted, physical access to sensitive computing resources and facilities is protected, systems are securely configured to avoid exposure to known vulnerabilities, incompatible duties are segregated among individuals, and backup and recovery plans are adequate and tested to ensure the continuity of essential operations.

[2]GAO, *Financial Audit: IRS's Fiscal Years 2016 and 2015 Financial Statements,* GAO-17-140 (Washington, D.C.: Nov. 10, 2016).

[3]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.

However, the collective effect of the deficiencies in information security from prior years that continued to exist in fiscal year 2016, along with the 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 represented a significant deficiency[4] in IRS's internal control over financial reporting systems as of September 30, 2016.

This report presents the details of, and recommendations for, specific information security control deficiencies we identified as part of our fiscal year 2016 audit of IRS's financial statements. This report also provides the status of IRS's corrective actions to address the security control deficiencies that we have reported in previous reports. Our objective for this audit was to determine whether IRS's controls over its key financial and tax processing systems were 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 selected financial applications; reviewed our prior reports to identify previously reported control deficiencies and assessed the effectiveness of corrective actions taken; and interviewed key agency officials. Our evaluation was focused on systems relevant to financial management and reporting. See appendix I for more details on our objective, scope, and methodology.

We performed our work in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objective.

Background

The use of information technology has created many benefits for federal 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 information systems to carry out their

[4]A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is important enough to merit the attention of those charged with governance. 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.

operations and for processing, maintaining, and reporting large volumes of sensitive data, such as personal information. Accordingly, information security should be a key consideration for any agency that depends on information systems and computer networks to carry out its mission, and is especially important for IRS, where maintaining the public's trust is essential.

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud 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.

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] In the February 2015 update to our High-Risk list, we expanded this 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] Our February 2017 High-Risk list update continues to designate federal information security, including protecting

[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).

[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]GAO-15-290.

the privacy of personally identifiable information, as a government-wide high-risk area.[8]

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*[9] requires the Comptroller General to issue standards for internal control in the federal government. These standards provide the overall framework for establishing and maintaining an effective internal control system and describe internal control as a process put in place by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives (operations, reporting, and compliance) of an entity will be achieved.[10]

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 entitywide, 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 Act of 2014* (FISMA)[11] is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over

[8]GAO, *High-Risk Series: An Update*, GAO-17-317 (Washington, D.C.: February 2017).

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

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

[11]The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely 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.

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 training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; implementing 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 its 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 its information systems are effectively secured to protect sensitive financial and taxpayer data for the collection of taxes, the processing of tax returns, and the enforcement of federal tax laws. In fiscal year 2016, IRS collected about $3.3 trillion in federal tax payments, processed about 202 million in tax and information returns, and paid about $426 billion in refunds to taxpayers.

IRS employs approximately 85,000 people (which includes about 16,000 temporary and seasonal staff) in its Washington, D.C., headquarters and more than 540 offices in every state, U.S. territory, as well as in a few 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.

The IRS collects and maintains a significant amount of personal and financial information on each U.S. taxpayer. Protecting this sensitive information is essential to protecting taxpayers' privacy and preventing financial loss and damages that could result from identity theft and other financial crimes. Further, the size and complexity of the IRS add unique operational challenges.

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. Within IRS, the senior agency official responsible for information security is 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 2016, the Treasury Inspector General for Tax Administration (TIGTA) stated that security over taxpayer data and protection of IRS resources was the top priority in its list of top ten management challenges for IRS for fiscal year 2017.[12]

IRS Made Progress in Addressing Previously Reported Control Deficiencies, but Financial and Taxpayer Data Continued to Be at Risk

IRS has implemented a number of our recommendations to address previously reported control deficiencies over its systems. However, it has not always effectively implemented access and other controls, including components of its information security program, to protect the confidentiality, integrity, and availability of its financial and tax processing systems and information. As illustrated in table 1, we have made a number of recommendations to IRS for correcting these control deficiencies. These deficiencies—including both previously reported and newly identified—increase the risk that taxpayer and other sensitive information could be disclosed or modified without authorization.

[12]Treasury Inspector General for Tax Administration, *Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2017*, Memorandum for Secretary Lew (Washington, D.C.: October 2016).

Table 1: Status of GAO Information Security Recommendations to IRS for Correcting Control Deficiencies at the Conclusion of Fiscal Year 2016 Audit

Information security control area	Prior recommendations not implemented at the beginning of fiscal year 2016 audit	Recommendations implemented or considered no longer relevant at the end of fiscal year 2016 audit[a]	Prior recommendations not fully implemented at the end of fiscal year 2016 audit	New recommendations resulting from fiscal year 2016 audit	Total outstanding recommendations at the conclusion of fiscal year 2016 audit
Access controls					
Boundary protection	—	—	—	11	**11**
Identification and authentication	14	(3)	11	24	**35**
Authorization	18	(4)	14	8	**22**
Cryptography	19	(2)	17	17	**34**
Audit and monitoring	9	(2)	7	5	**12**
Physical Security	2	(1)	1	5	**6**
Total	**62**	**(12)**	**50**	**70**	**120**
Other controls					
Configuration management	21	(10)	11	18	**29**
Segregation of duties	1	(1)	0	1	**1**
Contingency planning	0	(0)	0	2	**2**
Total	**22**	**(11)**	**11**	**21**	**32**
Information security program					
Risk assessments	—	—	—	1	**1**
Policies and procedures	4	(2)	2	3	**5**
Security plans	1	(0)	1	0	**1**
Training	1	(0)	1	0	**1**
Testing and evaluation	3	(1)	2	3	**5**
Remedial actions	1	(0)	1	0	**1**
Total	**10**	**(3)**	**7**	**7**	**14**
Grand Total	**94**	**(26)**	**68**	**98**	**166**

Legend: — = no recommendations made

Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-17-395

[a]We did not consider certain control deficiencies to be corrected or mitigated, rather the issues were no longer relevant due to IRS's changing operating environment.

IRS Improved Access Controls, but Deficiencies 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 (1) protection of system boundaries, (2) identification and authentication of users, (3) authorization of access permissions, (4) encryption of sensitive information, (5) audit and monitoring of system activity, and (6) physical security of facilities and computing resources.

IRS Implemented Controls to Protect its Network Boundaries, but Numerous Control Deficiencies Related to Network Devices Existed

Boundary protection controls the logical connectivity into and out of networks and controls connectivity to and from devices attached to the network. For example, at the application level, logical boundaries to business process applications may be controlled by access control lists in security software, or within the applications. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but also the risk of unauthorized access in a shared environment.

IRS had developed and documented policies for protecting system boundaries. The *Internal Revenue Manual* requires that communications be monitored and controlled at the external boundary and at key internal boundaries within its systems. The manual also requires that connections to external networks or information systems be done through managed boundary protection devices that comply with IRS security architecture. In addition, NIST Special Publication 800-53, Revision 4[13] recommends that devices be identified and authenticated prior to establishing a connection and that approved authorizations of information should be enforced.

IRS implemented controls to protect its network boundaries. For example, the agency implemented network boundary controls to protect the systems we reviewed from malicious code. In addition, the agency had effective controls to prevent access to its Windows computing

[13]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

environment through the implementation and enforcement of key configuration settings in its group policies.

Nevertheless, numerous deficiencies existed in IRS's controls related to its network devices. For example:

- IRS did not always ensure that its network devices were appropriately configured to protect access at external and internal boundaries of its information systems. Specifically, IRS permitted the use of an unauthenticated network protocol on 30 of the 122 network devices we reviewed.
- IRS did not adequately control the flow of information within its system and between interconnected systems by implementing access control lists[14] for certain interfaces on several of its network devices to prevent unauthorized users from logging into those devices.

The agency cited a backlog of other actions it needed to take as a cause for not implementing controls on the network devices. Without doing so, however, the cumulative effect of these deficiencies increases the risk that IRS's network devices and systems could be compromised and used by unauthorized individuals to access sensitive taxpayer data.

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 some sort of user identification (ID) process, as a prerequisite for granting access to resources in an IT system. User IDs 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 claim to be—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.

[14]An access control list is a set of rules that identify, permit, or restrict network traffic, usually based on addresses and other information from the packet headers of data traversing the network.

IRS had developed and documented policies for identification and authentication. The *Internal Revenue Manual* requires that multifactor authentication be implemented for remote access to information systems. The manual also requires that password lifetime restrictions be enforced on account passwords and that service accounts be set to expire within a defined number of days. The manual further requires that sensitive data or information, such as database account passwords, be stored using approved standards, and that user accounts be uniquely identified and authenticated.

IRS took steps that improved identification and authentication controls for its computing environments. For example, the agency implemented controls requiring that multifactor authentication be configured for remote logins to production servers used to manage an internal file transfer application. In addition, IRS corrected a previously reported identification and authentication control deficiency by enforcing password lifetime restrictions on user account passwords for the database supporting a financial system.

Nevertheless, deficiencies in identification and authentication controls continued to exist. For example, password lifetime restrictions were not being enforced by setting service account passwords to expire within a defined number of days for databases supporting 11 applications. In addition, for databases supporting 12 applications, sensitive account passwords were being stored in a format that did not meet approved standards. Further, the agency did not uniquely identify and authenticate user accounts on servers used to relay its e-mail.

Until these deficiencies are fully remediated, IRS is at increased risk that account passwords could be compromised, permitting unauthorized access to its systems.

Users had more system access than needed to perform their jobs

Access rights and privileges are used to implement security policies that specify 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 and privileges is one of the most important aspects of administering system security.

IRS had developed and documented policies for authorizing access to information technology systems. According to the *Internal Revenue Manual*, system access is to be granted based on the principle of least privilege. The manual also requires that database privileges be assigned via user roles and not directly to database accounts.

IRS had improved its authorization process by strengthening several authorization controls. For example, it had removed excessive privileges that permitted remote access to servers that support the administration of automated file transfers of financial data.

Nevertheless, numerous authorization control deficiencies still existed in IRS's computing environment. For example, the agency did not always ensure that system access was properly restricted because it permitted an excessive number of users and administrators to login to various servers in the IRS infrastructure. Specifically, the agency's computing environment was configured such that more than 450 users and administrators were permitted to login to numerous production servers even if that access was not necessary to accomplish the user's assigned job duties. Agency officials stated that they were not aware of policies requiring the number of users to be limited but nevertheless planned to review the number of users permitted to login to their production servers.

In addition, IRS did not consistently assign database privileges per its policy for three financial systems we reviewed. For these systems, the agency assigned database privileges directly to individual accounts instead of assigning the privileges to a specific role.

As a result, IRS is at increased risk that users with excessive privileges not necessary for performing their work could inadvertently or deliberately modify these servers and databases. Doing so would jeopardize the confidentiality and integrity of the data they contain.

IRS expanded its use of encryption, but cryptography control deficiencies continued

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 had developed and documented 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[15] that meets the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

IRS expanded its use of encryption to protect sensitive data, but cryptography control deficiencies continued. For example, IRS configured a server that it relies on to manage its operations to use a strong form of encryption. Nevertheless, the agency configured other systems to use encryption that was less secure since the software versions being used on those systems could not support the stronger encryption. These configurations did not meet agency policies or applicable federal standards.

By not using strong encryption, IRS has an increased risk that an unauthorized individual could exploit the weak algorithm to view and then use data to gain unwarranted access to systems or financial and sensitive taxpayer data.

Although IRS had an audit and monitoring process in place, audit plans were not implemented

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.

[15]A cryptographic module is the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

IRS had developed and documented policies for auditing and monitoring its 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; it also requires that audit logs be reviewed and communicated to the appropriate personnel in a timely manner. The manual further requires that audit plans, which are to be used to document system and application-specific audit and monitoring requirements, be developed for all systems and applications. In addition, the manual states that user activities are to be monitored and logged by application-level and user-level audit trails in accordance with approved audit plans.

IRS has improved its audit logging process. Specifically, the agency remediated a previously reported control deficiency by ensuring that audit logs were configured to consistently record the use of certain commands in the mainframe environment. In doing so, IRS has increased the likelihood that unauthorized and/or anomalous use of these commands will be detected.

Nevertheless, deficiencies in audit and monitoring controls continued to exist. For example, IRS did not include a system that processes hundreds of thousands of e-mails per day in its monitoring process, limiting its ability to detect unauthorized or unusual activity that could adversely affect this system. In addition, IRS was not consistently implementing system and application audit plans. Specifically, although IRS developed and documented audit and monitoring requirements, it had not implemented the requirements for 12 of the 23 systems and applications we reviewed.

Further, IRS's audit plan for its databases requires that system administrators and security operations analysts be alerted in the event of an audit processing failure. The audit plan also describes multiple methods by which the detection of audit processing failures is to be accomplished, including, among others, routine operational reviews for indications of audit processing failures and reviews by system administrators and security operations analysts to confirm that audit events are being received.

Nevertheless, the agency did not enable database logging, nor did it review, analyze, or report auditable and actionable events on a database supporting a tax payment system. This deficiency had not been identified by any of IRS's detection methods provided in its audit plan.

Without effective audit and monitoring controls, IRS's ability to establish individual accountability, monitor compliance with security and configuration management policies, and investigate information systems security violations is limited.

IRS implemented physical security controls, but physical security control procedures were not always effective

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. Physical security controls over the 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 had 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. The manual also requires that department managers of restricted areas approve all names added to the authorized access list for restricted areas. Further, the manual requires that department managers review, validate, sign, and date the authorized access list for the restricted area on a monthly basis, and then forward the list to the physical security office for review.

IRS had implemented physical security controls at its enterprise computing centers to safeguard assets against possible theft and malicious actions. For example, the agency had placed guards at each of its computing centers to, among other things, aid in controlling physical access to restricted areas. In addition, the agency had a process in place for approving names added to the authorized access list for restricted areas at the two computing centers.

Nevertheless, IRS's implementation of physical security controls was not always effective. For example, the agency did not perform monthly reviews of individuals with an ongoing need to access restricted areas at its two computing centers in a way that would ensure that such access was still appropriate. Specifically, the review process had not identified a small number of individuals who had separated from IRS and, consequently, had not resulted in the removal of their access privileges.

Agency officials attributed this oversight to an employee failing to follow the proper review process. They stated that the employee was retrained and the access list was corrected. We previously made a recommendation in fiscal year 2014 for IRS to address a similar issue at one of its two computing centers.[16]

Because individuals may be allowed inappropriate access to restricted areas, IRS has diminished assurance that its computing resources and sensitive information are adequately protected from unauthorized access.

Deficiencies in Other Information System 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; segregating incompatible duties; and planning for continuity of operations.

Although IRS improved its configuration management process, deficiencies continued to exist

Configuration management controls are intended to, among other things, provide reasonable assurance that systems are configured and operating securely and as intended. Patch management, a component of configuration management, is an important element in mitigating the risks associated with known vulnerabilities. When a vulnerability is discovered, the vendor may release a patch[17] to mitigate the risk. If a patch is not applied in a timely manner, information systems are vulnerable to an attacker exploiting a known vulnerability not yet mitigated, enabling unauthorized access to the system or enabling users to have access to greater privileges than authorized.

IRS had developed and documented policies for managing the configuration of its information technology systems. The *Internal Revenue Manual* requires that IRS manage systems to reduce vulnerabilities by, among other things, installing patches in accordance with the timelines defined in its policy, which align with the criticality of the updates and patches. The manual also requires that database software be removed or updated prior to a vendor dropping support for the software.

[16]GAO, *Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk*, GAO-14-401SU (Washington, D.C.: Apr. 8, 2014).

[17]A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered.

In addition, IRS corrected a previously reported patch management control deficiency by installing up-to-date patches on one of its mail servers operating in its non-production environment. Nevertheless, deficiencies in its configuration management processes continued to exist. For example, at the time of our site visit in July 2016, the agency had not installed the most up-to-date critical patches on its mail servers operating in its production environment. By not installing critical patches in a timely manner as prescribed by its own policy, IRS increases the risk that known vulnerabilities in its systems may be exploited.

Further, IRS did not consistently ensure that database software being used was supported by the vendor. For example, at the time of our site visits in June and July 2016, the agency continued to use software that the vendor stopped supporting in August 2015 on nine databases containing financial and sensitive taxpayer information.

Running outdated and unsupported software increases security risk, as the vendor may no longer be supplying security patches, thus leaving IRS systems more susceptible to known vulnerabilities.

IRS did not always appropriately segregate incompatible duties

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 had developed and documented policies for dividing and separating incompatible duties and responsibilities. The *Internal Revenue Manual* requires that the duties and responsibilities of functions be divided and separated 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.

Nevertheless, IRS did not enforce segregation of duties in a key financial system we reviewed. Specifically, five users were assigned to security roles as well as to four other roles that the agency had defined as incompatible for users who have a security role. At the time of our review, IRS had not implemented a process to ensure these users were not assigned incompatible security roles. As a result, IRS is at increased risk that the inadvertent or deliberate misuse of inappropriate privileges may occur.

Although IRS had contingency plans in place for systems reviewed, its plans were not always complete or up-to-date

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If contingency plans are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. 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.

IRS had developed and documented policies for developing and testing information system contingency plans. The *Internal Revenue Manual* requires IRS 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 that IRS have the capability to continue performance of mission essential functions during any disruption for a period up to 30 days or until normal operations can resume. Further, the manual requires the agency to review its contingency plans at least annually and update them to reflect changes to its information systems or current operating environment.

Nevertheless, although IRS had developed contingency plans and tested controls for these plans, they were not always complete or up-to-date. IRS had documented and tested the contingency plans for the 11 systems we reviewed. However, the agency did not document or demonstrate the extent to which it had capabilities to continue essential operations. For example, the agency did not identify alternative or work-around processing procedures in the contingency plan for its payment posting system to ensure that system functions would be available as soon as possible after a disruption of service. Further, while IRS ensured that contingency plans for the 11 systems were annually reviewed, the agency's review procedures did not consistently identify hardware information that required updating when the agency's operating

environment changed. Specifically, hardware lists included in 2 of the 11 plans we reviewed contained hardware that had either been retired or relocated to another computing center.

By not identifying alternative or work-around processing procedures for its payment posting system and not ensuring that contingency plans are updated to reflect changes to the operating environment, IRS has reduced assurance that it has implemented controls necessary to ensure that functions for these systems would be available in the event of a disruption of service.

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

An underlying reason for the information security control deficiencies in IRS's financial and tax processing systems was that, although the agency had developed and documented 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 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 a group of information systems, as appropriate;
- 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.

IRS had documented risk assessments, but did not effectively support a risk-based decision

Identifying and assessing information security risks is essential to determining what controls are required to cost-effectively protect information and information systems. 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 they operate as intended. According to NIST Special Publication 800-30, Revision 1,[18] risk is determined by identifying potential threats to an 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.

IRS had developed and documented policies for identifying, assessing, and managing information security risk. The *Internal Revenue Manual* requires that all information systems and data supporting critical operations and assets be periodically assessed for the risk and magnitude of harm that could result from vulnerabilities and potential threats. The manual also requires that the agency identify and document threats, vulnerabilities, and potential impacts and review the results at least annually. Further, the manual requires that any risk-based decision exceptions have a "suitable justification" documented and a thorough assessment of potential risks conducted.

IRS conducted and documented risk assessments for the 12 systems we reviewed. These 12 risk assessments documented information related to the identification of threats, vulnerabilities, and potential impacts to agency operations and were updated annually.

Nevertheless, IRS did not effectively support a risk-based decision to accept system deficiencies. Specifically, while the agency documented its acceptance of risks associated with making certain database configuration decisions in production, the vendor documentation used for

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

support advised against using the configurations in a production environment.

Until IRS ensures that suitable justifications are developed, documented, and approved for accepting system risk, the agency has less assurance that decisions to accept risk are based on sufficient information and that risk to its systems are being properly accepted by system owners.

IRS had developed and documented policies and procedures addressing several components of its agency-wide information security program, but it had not fully developed, documented, or updated other components

A key component 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. Developing, documenting, and implementing security policies are the primary mechanisms by which management communicates its views and requirements. Developing and documenting supporting procedures provide the detailed information and guidance necessary to implement the policies. If properly developed and implemented, policies and procedures should help reduce the risk associated with unauthorized system access or disruption of services.

Policies also serve as the basis for adopting specific procedures and technical controls. In addition, technical security standards can provide consistent implementation guidance for each computing environment. 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 are intended to provide.

IRS had developed and documented information security policies and procedures that addressed several components of its agency-wide program. For example, it had documented policies and procedures governing risk assessments, security planning, and testing and evaluating information security controls.

Nevertheless, we noted instances where information security policies, procedures, and guidelines had not been fully developed, documented, or updated. For example:

- IRS had not updated policies and procedures to ensure that they addressed, among other things, the (1) methods available for granting 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) sharing of data storage between systems, and (5) reconciliation of

access privileges. We previously made a recommendation to address these issues.[19]

- IRS did not have detailed procedures to perform reviews of audit records for a key financial system we reviewed. NIST Special Publication 800-53, Revision 4 recommends that organizations develop, document, and disseminate procedures to facilitate the periodic review and analysis of audit records. In addition, the *Internal Revenue Manual* requires that information system audit records be used for the monitoring, analysis, investigation, and reporting of unauthorized or inappropriate information system activity. During fiscal year 2016, IRS sequentially used three separate versions of its audit log analysis and review procedures to review the audit records for a key financial system. Nevertheless, none of the three versions contained detailed procedures for the review of the financial system's audit records.
- The *Internal Revenue Manual* requires that an enterprise-wide system owner procedural document be developed to control critical mainframe system commands and provide a clear indication of roles as well as the type of access for each role. Nevertheless, IRS did not develop the required procedural document.
- IRS's configuration standards and guidelines for its routers and switches were not current and, therefore, did not include known security vulnerabilities. The agency documents its configuration standards and guidelines for its routers and switches and, with only a few exceptions, requires that every router and switch meet those configuration standards. Nevertheless, we identified 14 deficiencies on IRS's network devices pertaining to configuration settings that had not been set to optimize network device security. For 4 of the 14 instances, network devices had not been configured to address known vulnerabilities and the agency's current version of documented network device configuration standards and guidelines had not been updated to incorporate recommendations from industry leaders, security agencies, and key practices from IRS partners to address these known vulnerabilities.
- 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

[19]GAO, *Information Security: IRS Has Improved Controls but Needs to Resolve Weaknesses*, GAO-13-350 (Washington, D.C.: Mar. 15, 2013).

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 may not 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.[20]

Without comprehensive and fully documented policies and procedures that govern the security of their computing environment, IRS has limited assurance that staff will consistently implement effective controls necessary for protecting the agency's information systems.

IRS developed and documented security plans, but did not update one plan 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's Circular A-130[21] 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. Further, the *Internal Revenue Manual* requires that security plans be reviewed, at a minimum, annually or as a result of a significant change, and be updated to address changes to the information system, the system's operating environment, or problems identified during plan implementation or security control assessments.

Although the agency had developed and documented security plans for the 13 systems we reviewed, one of the plans had not been appropriately updated to reflect changes to the operating environment. This plan is important in that it covers multiple systems that provide network infrastructure services to IRS personnel and information systems. We have previously recommended that IRS address this issue.[22] Without an updated system security plan, IRS cannot ensure that the most

[20]GAO, *Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk*, GAO-14-405 (Washington, D.C.: Apr. 8, 2014).

[21]Office of Management and Budget, *Circular No. A-130, Managing Information as a Strategic Resource* (Washington, D.C.: July 28, 2016).

[22]GAO, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, GAO-16-398 (Washington, D.C.: Mar. 28, 2016).

appropriate security controls are in place to protect its financial and sensitive taxpayer information.

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

Another key component 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 implementation of security policies, the full benefits are not achieved unless the results improve the security program through mitigation of known deficiencies in the information security policies, procedures, and practices of the agency or implementation of compensating or mitigating controls if needed.

IRS has developed and documented policies for conducting tests and evaluations of its policies and procedures. 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. In addition, the manual requires that mainframe systems be monitored and verified for configuration management compliance (i.e., implementation of configuration management controls) by using IRS-approved compliance verification applications or the approved security posture monitoring system.

IRS had implemented numerous processes for testing and evaluating its policies, procedures, and controls to determine whether they were effective and operating as intended. Agency officials stated that, through these processes, they had already identified many of the security control deficiencies we raised during the fiscal year. Specifically, IRS discovered some of the deficiencies through processes such as running their policy check programs to identify violations and FISMA reviews.

Nevertheless, shortcomings still existed in the agency'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 recommendations to address this issue.[23]
- 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 system control test procedures and results that we reviewed. For example, for one of the two systems, the agency documented it had met one of its risk assessment control objectives without performing any tests of procedures for controls related to that objective. We previously made a recommendation to address this issue.[24]
- In addition to tests and evaluations conducted on a yearly basis, IRS uses automated compliance verification tools to periodically test compliance with the security policies for its mainframe computing environment. Nevertheless, the mainframe tool only tests compliance with a limited subset of the agency's policies. For example, the tool did not verify compliance for the implementation of certain required access privilege controls or operating system configuration settings. Therefore, the results from these tools do not provide management with the information necessary to allow it to arrive at appropriate conclusions about the security status of these systems. Accordingly, IRS may not be fully aware of vulnerabilities that could adversely affect its applications and data.

IRS also had not always considered and documented the results of its review of internal controls related to financial reporting. The Office of Management and Budget's Circular No. A-123 and its related implementation guide (A-123 guide) define requirements for internal control.[25] The documents require agency management to monitor and assess controls, including those controls over automated information

[23]GAO-13-350.

[24]GAO, *Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data*, GAO-15-337 (Washington, D.C.: Mar. 19, 2015).

[25]The Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, is the policy document that implements the requirements of 31 U.S.C. 3512 (c), (d) (commonly known as the *Federal Managers' Financial Integrity Act* or FMFIA). Circular No. A-123's focus for internal controls is primarily on providing agencies with a framework for assessing and managing risks more strategically and effectively. The circular was recently revised to reflect changes incorporated in GAO's updated *Standards for Internal Control in the Federal Government*.

systems that affect financial reporting, and provide an annual assurance statement on the overall adequacy and effectiveness of internal control within the agency. The A-123 guide also specifies that a service organization's systems are considered to be part of an entity's information system.[26]

To that end, the *Internal Revenue Manual* requires that IRS review GAO and TIGTA audits related to financial reporting to determine potential agency risk and the impact to various business and reporting processes. The manual also requires that the agency review and follow up on known significant GAO and TIGTA audit findings and recommendations that directly relate to the objectives of Circular A-123 internal control assessments and document the review activities. In addition, IRS's documented procedures for reviewing external systems that support financial reporting require that IRS review external systems annually and, when available, review those system's Statement on Standards for Attestation Engagements (SSAE) No. 16 reports.[27]

Nevertheless, IRS did not perform reviews in accordance with its policy:

- The agency had not reviewed all pertinent information during its Circular A-123 review process of internal systems. Although IRS documented its review of GAO published financial management reports as part of their fiscal year 2016 Circular A-123 internal control assessment, they did not include all the reports containing significant GAO findings and recommendations. For example, two of IRS's assessments did not include a documented review of a GAO financial management report published in March 2016. This report included technical findings and recommendations related to specific IRS systems, including a system critical to its financial reporting. As a result, IRS's internal control effectiveness assessment results may not adequately describe the agency's financial reporting control environment.

[26]Agencies are responsible for assessing the extent to which they rely on the internal controls of its service organization and, where appropriate, monitoring the effectiveness of internal control over its financial reporting at service organizations.

[27]Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization* (March 2010) contains standards for a service organization's auditors to use in reporting on the service organization's controls over the services it provides to user entities (such as IRS) when those controls are likely to be relevant to user entities' internal control over financial reporting.

- IRS had not reviewed SSAE No. 16 reports for two external systems used for financial reporting. Specifically, IRS had not identified and documented which user controls from two SSAE No. 16 reports the agency deemed to be relevant. In addition, since the agency had not identified the relevant user controls, it had not documented testing of the operating effectiveness for those controls. Without identifying, verifying, and reviewing user controls, IRS has limited assurance that it has the appropriate controls in place or will draw adequate conclusions on the operating effectiveness of these controls.

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

Shortcomings existed in IRS's remedial process

FISMA requires that agency-wide information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency. Agencies should establish procedures to reasonably ensure that all information security control weaknesses, regardless of how or by whom they are identified, are addressed through the agency's remediation processes. For each identified control deficiency, the agency is to develop and implement a plan of action and milestones (POA&M) based on findings from security control assessments, security impact analyses, continuous monitoring of activities, audit reports, and other sources. According to the *Internal Revenue Manual*, the agency should document weaknesses identified 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 verifying that each weakness is corrected before closing that item.

Although IRS had a remedial process in place, it had not ensured that corrective actions had been effectively implemented. Specifically, the agency made progress in correcting previously reported information security deficiencies. For example, by the end of our fiscal year 2016 audit,[28] IRS had corrected or mitigated 26 of the 94 previously reported unresolved deficiencies. Nevertheless, other corrective actions had not been effectively implemented. Particularly, at the time of our review, 68 of 94—about 72 percent—of the previously reported deficiencies remained

[28]GAO-16-398.

unresolved or unmitigated, of which 11 of the 94 deficiencies have been outstanding since 2013.

In addition, the agency's process for verifying whether an action had corrected or mitigated the deficiency was not working as intended. Specifically, for the 21 previously reported recommendations that IRS informed us that it had addressed, actions for 5 of the recommendations had not been effectively implemented. We have previously made a recommendation to IRS to improve its process for verifying corrective actions to address deficiencies.[29]

Until the agency takes additional steps to implement a more effective verification process, it will have limited assurance that control deficiencies are being properly mitigated or corrected.

Conclusions

IRS made progress in addressing previously reported control deficiencies related to its financial systems. Nevertheless, continuing and newly identified control deficiencies limited the effectiveness of security controls for protecting the confidentiality, integrity, and availability of IRS's key financial and tax processing systems. During fiscal year 2016, 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. Nevertheless, information security deficiencies continued to exist in access and other information system controls over the agency's financial and tax processing systems, exposing financial and sensitive taxpayer information to unnecessary risk of unauthorized access, use, disclosure, and modification.

The financial and taxpayer information on IRS systems will remain vulnerable until the agency (1) addresses control deficiencies pertaining to boundary protection, identification and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning and (2) effectively implements components of its information security program, including updating its security plan to reflect the current operating environment. The collective effect of these deficiencies in information security is the basis of our determination that IRS had a significant

[29]GAO-15-337.

deficiency in internal control over financial reporting systems as of September 30, 2016. 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

To help strengthen information security controls over key financial and tax processing systems, we recommend that the Commissioner of Internal Revenue, in addition to addressing previously made but still unresolved recommendations from our prior audits, take the following 10 actions to more effectively implement security-related policies and plans.

- Implement the audit plans for the 12 systems and applications that we reviewed in the production computing environment.
- Ensure that system administrators and security operations analysts are alerted in the event of audit processing failures.
- Update information contingency plan test procedures to include updating contingency plans to reflect changes to the current operating environment.
- Ensure that approved risk-based decisions pertaining to database configurations are based on suitable justification.
- Develop, document, and implement the use of detailed procedures to facilitate the periodic review and analysis of audit records for its financial systems.
- Develop an enterprise-wide system owner procedural document to control critical mainframe operating system commands.
- Regularly update configuration standards and guidelines for network devices to incorporate recommendations from industry leaders, security agencies, and key practices from IRS partners to address known vulnerabilities applicable to IRS's environment.
- Implement a compliance verification application, or other appropriate process, to ensure configuration policies are comprehensively tested on the mainframe.
- Ensure that all known significant audit findings and recommendations related to financial reporting, which includes those in GAO's public and limited official use only reports, that directly relate to the objective of A-123 internal control tests are reviewed and monitored.

- Identify and review service organizations' listing of user controls that are deemed relevant and test those controls to appropriately draw conclusions about the operating effectiveness of controls.

We are also making 88 technical recommendations in a separate report with limited distribution. These recommendations address information security control deficiencies related to boundary protection, identification and authentication, authorization, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning.

Agency Comments and Our Evaluation

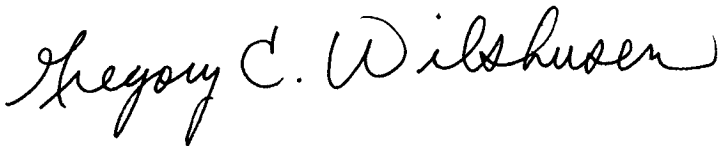
We provided a draft of this report to the IRS for review and comment. In its written comments, reproduced in appendix II, the agency neither agreed nor disagreed with our recommendations. Nevertheless, the agency stated that it is committed to improving the overall effectiveness of information security controls and would review each of our recommendations and ensure that its corrective actions include sustainable fixes that implement appropriate security controls. Further, the agency said it is reviewing all GAO prior year open recommendations to ensure they continue to be relevant in IRS's current environment.

The agency 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 deficiencies, it has 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.

If you have any questions about this report, please contact Nancy R. Kingsbury at (202) 512-2700 or kingsburyn@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. GAO staff who made key contributions 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 and tax processing applications; and interviewed key agency officials. This enabled us to assess the effectiveness of corrective actions taken by IRS to address control deficiencies we previously reported and to determine whether any additional deficiencies existed. This work was performed in connection with our audit of IRS's fiscal years 2016 and 2015 financial statements[1] 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 control deficiencies 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. We focused our evaluation primarily on the controls for key financial and taxpayer information systems.

Our evaluation was based on our *Federal Information System Controls Audit Manual*,[2] 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

- reviewing configurations on IRS's network devices to determine if implemented configurations would protect the devices against malicious code and unauthorized access;

[1]GAO, *Financial Audit: IRS's Fiscal Years 2016 and 2015 Financial Statements*, GAO-17-140 (Washington, D.C.: Nov. 10, 2016).

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

- comparing the complexity, expiration, and policy settings for passwords on systems and databases to IRS and federal guidelines to determine if strong password management was being enforced;
- evaluating whether the agency had implemented controls to ensure access to key systems and databases were appropriately limited according to IRS policy, and federal and vendor best practices;
- examining IRS's implementation of cryptography to secure data transmissions from one information system to another in order to determine if implemented cryptographic mechanisms met the requirements of applicable federal standards;
- analyzing audit logs that record events occurring in system environments responsible for taxpayer data processing and the support of refunds disbursements, revenue, unpaid assessments, and payroll financial reporting;
- observing and reviewing physical security controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft at each of the enterprise computing centers;
- evaluating the mainframe configuration controls supporting system applications and revenue accounting databases;
- evaluating the access controls of mainframe configurations over shared disk storage across multiple mainframe processing environments;
- evaluating the mainframe access controls of the mainframe operating systems that support payroll and taxpayer data processing;
- comparing security configurations on key systems and database configurations to IRS and federal guidelines to determine if systems were configured and operating securely;
- examining the status of vendor-supplied software installations on key system components by comparing the release dates of vendor-supplied software to the install dates of the software running on IRS's systems to ensure that software was up-to-date; and
- reviewing continuity of operations planning documentation to determine if such plans contained the details necessary for the recovery of system and business functions, and assessing the extent to which those details had been documented and tested.

Using the requirements in the *Federal Information Security Modernization Act of 2014*,[3] which established components for an agencywide information security program, we reviewed and evaluated IRS's implementation of its security program by

- reviewing risk assessments to determine whether the assessments were being updated at least annually;
- examining IRS's approach to risk management, including its approach to risk-based decisions;
- 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;
- examining documentation to determine the extent to which IRS was performing internal control 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 previously reported control deficiencies to determine if they had effectively mitigated or resolved the control deficiencies; and
- reviewing continuity of operations planning documentation for 11 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.

[3]The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely 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.

We performed our work in accordance with U.S. generally accepted government auditing standards. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Internal Revenue Service

COMMISSIONER

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

June 22, 2017

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 titled, *Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data*, *GAO-17-395* (public version).

We are pleased GAO recognized our progress in addressing a number of Information Technology (IT) security controls. We also appreciate acknowledgement that the IT organization is relied upon extensively to achieve the IRS mission.

In fact, IRS IT applications, infrastructure and network systems have run with exceptional precision during Filing Season 2017, processing more than 140 million individual returns, issuing refunds of approximately $287 billion, and supporting more than 12 million taxpayer calls. As of May 3, 2017, our modernized Return Review Program (RRP) system has selected approximately 865,000 potentially fraudulent tax returns claiming approximately $7.6 billion in refunds. This system is the government's primary line of defense against the perpetration of tax refund identity theft, fraud, and noncompliance.

As you are aware, the IRS is committed to improving its financial management, internal controls, and the overall effectiveness of information system controls. In addition to the filing season accomplishments mentioned above, the IRS accelerated implementation of numerous cybersecurity safeguards that are outlined in the Office of Management and Budget (OMB) Cybersecurity Strategy and Implementation Plan (CSIP). We have enhanced protections to defend against malicious actors attempting to visit irs.gov; expanded use of continuous application security monitoring, including the IRS-strengthened eAuthentication platform; and improved the security of our IT infrastructure by replacing obsolete equipment. The IRS has also applied additional resources and established rigorous new processes to address the root cause of all identified weaknesses systematically.

Nonetheless, we are aware that much work remains to be done to ensure our large and complex IT ecosystem is fully secure and protects our financial and taxpayer data. We appreciate the recommendations associated with this audit, and in particular your

response to our request for an increased level of detail in your audit findings. While this has resulted in a marked increase in the overall number of recommendations, your identification of the multiple systems and applications associated with the same finding is very helpful. We will review each of your recommendations carefully and ensure our corrective actions include sustainable fixes that implement appropriate security controls within our technology and human capital resource limitations, and provide the detailed corrective action plans in our 60-day letter response to Congress. We are also reviewing all prior year open recommendations to ensure they continue to be relevant in our current environment.

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

If you have any questions, please contact me, or a member of your staff may contact Gina Garza, Chief Information 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, Mark Canter, Larry Crosland, and David Hayes (assistant directors); Daniel Swartz (analyst-in-charge); Kevin Cotter, Saar Dagani, Kristi Dorsey, Nancy Glover, Mickie Gray, Tyrone Hutchins, Fatima Jahan, J. Andrew Long, Vernetta Marquis, Sean Mays, Kevin Metcalfe, Rebecca Perkins, Matthew Smagin, Eugene Stevens, Michael Stevens, Richard Sayoc, and Kimberly Washington made key contributions to this report.