



July 2018

INFORMATION SECURITY

IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data

Accessible Version

GAO Highlights

Highlights of [GAO-18-391](#), 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 sensitive financial and taxpayer information that reside on those systems.

As part of its audit of IRS's fiscal year 2017 and 2016 financial statements, GAO assessed whether controls over 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 selected financial systems and applications; and interviewed key agency officials at four IRS locations.

What GAO Recommends

In addition to the prior recommendations that have not been implemented, GAO is recommending that IRS take 5 additional actions to more effectively implement security-related policies and plans. In a separate report with limited distribution, GAO is recommending 32 actions that IRS can take to address newly identified control deficiencies. In commenting on a draft of this report, IRS agreed with GAO's recommendations and stated that it would review each of the recommendations and ensure that its corrective actions include a root cause analysis for sustainable fixes that implement appropriate security controls.

View [GAO-18-391](#). 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

July 2018

INFORMATION SECURITY

IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data

What GAO Found

The Internal Revenue Service (IRS) has made progress in resolving a number of previously reported control deficiencies. During fiscal year 2017, the agency made improvements in access controls by, for example, restricting unnecessary user access to certain applications and enforcing strong encryption on certain systems. IRS also corrected a previously identified contingency planning weakness for one system.

Nevertheless, continuing and newly identified control deficiencies limited the effectiveness of security controls for protecting the confidentiality, integrity, and availability of IRS's financial and tax processing systems. For example, IRS did not consistently (1) implement access controls by enforcing password expirations and minimum password lengths or by updating expiration dates for contractor passwords; (2) apply configuration management controls by documenting authorizations and approvals for changes to mainframe data and processing, or by installing critical security patches on multiple devices; and (3) implement certain components of its security program by correcting weaknesses in procedures or by updating system security plans. GAO has made recommendations to IRS to correct the identified security control deficiencies (see table). However, many deficiencies have not been corrected, and a large number of recommendations remained open at the conclusion of the audit of IRS's financial statements for fiscal year 2017.

Status of GAO Information Security Control Recommendations to IRS to Correct Control Deficiencies at the Conclusion of Fiscal Year 2017

Information security control area	Prior recommendations open at the beginning of FY 2017	Prior recommendations closed at the end of FY 2017	New recommendations resulting from FY 2017 audit	Total outstanding recommendations at the end of FY 2017
Access controls	120	(35)	21	106
Configuration management	29	(10)	13	32
Segregation of duties	1	(0)	0	1
Contingency planning	2	(1)	1	2
Security program	14	(3)	2	13
Total	166	(49)	37	154

Legend: FY = fiscal year

Source: GAO analysis of Internal Revenue Service (IRS) data. | [GAO-18-391](#)

Until IRS takes additional steps to address unresolved and newly identified control deficiencies and effectively implements components of its information security program, IRS 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 2017.

Contents

Letter	1
Background	3
IRS Made Progress in Addressing Previously Reported Control Deficiencies, but Sensitive Financial and Taxpayer Data Continue to Be at Risk	6
Conclusions	25
Recommendations for Executive Action	26
Agency Comments and Our Evaluation	27

Appendix I: Objective, Scope, and Methodology	29
Appendix II: Comments from the Internal Revenue Service	32
Appendix III: GAO Contacts and Staff Acknowledgments	35
Appendix IV: Accessible Data	36
Agency Comment Letter	36

Table	
Table 1: Status of GAO Information System Security Control Recommendations to IRS to Correct Control Deficiencies at the Conclusion of Fiscal Year 2017	7

Abbreviations

CFO	chief financial officer
FIPS	Federal Information Processing Standard
FISCAM	Federal Information Systems Controls Audit Manual
FISMA	Federal Information Security Modernization Act
FMFIA	Federal Managers' Financial Integrity Act
ID	identification
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	personal identity verification
SOC	service organization controls
Treasury	Department of the Treasury

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



July 31, 2018

The Honorable David J. Kautter
Acting Commissioner of Internal Revenue

The Internal Revenue Service (IRS) has a demanding responsibility to collect taxes, process tax returns, and enforce the nation's tax laws. A bureau of the U.S. Department of the Treasury, IRS relies extensively on computer systems to support its financial and mission-related operations. IRS also relies on information system security controls to protect the confidentiality, integrity, and availability of the sensitive financial and taxpayer information that resides on its systems.

GAO audits IRS's financial statements in accordance with authority conferred by the *Chief Financial Officers (CFO) Act of 1990*, as amended by the *Government Management Reform Act of 1994*. As part of our audit of IRS's fiscal year 2017 and 2016 financial statements, we assessed the effectiveness of the agency's information system security controls over selected financial and tax processing systems, information, and interconnected networks at four IRS locations. These systems support the processing, storage, and transmission of sensitive financial and taxpayer data.

On November 9, 2017, we issued our report on the results of our audit of IRS's fiscal year 2017 and 2016 financial statements, and on the effectiveness of its internal control over financial reporting¹ as of September 30, 2017.² During that audit, we identified continuing and new internal control deficiencies³ concerning IRS's financial reporting systems that are important enough to merit the attention of those charged with governance of IRS. Therefore, we considered these continuing and new

¹We audited IRS's internal control over financial reporting as of September 30, 2017, based on criteria established under 31 U.S.C. § 3512(c), (d), commonly known as the *Federal Managers' Financial Integrity Act (FMFIA)*.

²GAO, *Financial Audit: IRS's Fiscal Years 2017 and 2016 Financial Statements*, [GAO-18-165](#) (Washington, D.C.: Nov. 9, 2017).

³A 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.

issues affecting IRS's internal control over financial reporting systems collectively to be a significant deficiency⁴ in internal control in fiscal year 2017.⁵

Our objective for that audit was to assess whether IRS's controls over its financial and tax processing systems were effective in ensuring the confidentiality, integrity, and availability of sensitive financial and taxpayer data. To accomplish the objective, we examined the agency's information security policies, plans, and procedures;⁶ tested controls over selected financial systems; reviewed previously reported control deficiencies; and assessed the effectiveness of corrective actions taken. We also interviewed key agency officials responsible for managing and operating the selected systems. The focus of our evaluation was limited to systems relevant to financial management and reporting. Appendix I provides additional 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 provides a reasonable basis for our findings and conclusions based on our audit objective.

This report is an integral part of our audit of IRS's fiscal years 2017 and 2016 financial systems. In this regard, the report presents the details of information system security control deficiencies we identified as part of our fiscal year 2017 audit of IRS's financial statements, and recommendations for corrective actions to address them. Specifically, the report highlights some of our new internal control deficiencies that we identified during our fiscal year 2017 testing of information system

⁴A 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 over financial reporting, 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.

⁵[GAO-18-165](#).

⁶Most of IRS's information security policies, plans, and procedures are non-public documents that cannot be described in detail in publicly available audit reports.

security controls over financial systems that are relevant to IRS's internal control over financial reporting.⁷

This report also presents details of one information system security control deficiency we identified during our audit that does not directly affect IRS's financial reporting, but does merit management's attention due to its potential effect on information system security controls for ensuring the confidentiality, integrity, and availability of sensitive information.⁸ In addition, this report includes the results of our follow-up on the status of the agency's corrective actions to address information system security control deficiencies and associated recommendations contained in our prior years' reports that remained open at the beginning of our fiscal year 2017 audit.

The purpose of this report is solely to describe the scope and results of our testing of the effectiveness of IRS's security controls over its financial and tax processing systems relevant to financial management and reporting. Accordingly, this report is not suitable for any other purpose.

Background

As the tax collector of the United States, the IRS mission is to help taxpayers understand and meet their tax responsibilities and to enforce

⁷An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, the objectives of which are to provide reasonable assurance that (1) transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in accordance with U.S. generally accepted accounting principles, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition, and (2) transactions are executed in accordance with provisions of applicable laws, including those governing the use of budget authority, regulations, contracts, and grant agreements, noncompliance with which could have a material effect on the financial statements.

⁸Information system security controls include logical and physical access controls, configuration management, segregation of duties, continuity of operations, and security management. These controls are designed to ensure that access to data is appropriately restricted, physical access to sensitive computing resources and facilities is restricted, systems are securely configured to avoid exposure to known vulnerabilities, and incompatible duties are segregated among individuals. In addition, controls should ensure that backup and recovery plans are adequate and tested to ensure the continuity of essential operations, and that security is managed entity-wide under a framework that provides a continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

tax laws with integrity and fairness. According to publicly available IRS data, in fiscal year 2017, the agency collected about \$3.4 trillion in federal tax payments, processed a total of about 201 million returns, and paid about \$437 billion in refunds and outlays. IRS employs over 81,000 year-round and seasonal staff in its Washington, D.C. headquarters, in offices in every state and U.S. territory, and in a few U.S. embassies and consulates. The agency also operates enterprise computing centers in Martinsburg, West Virginia and Memphis, Tennessee.

In carrying out its mission and responsibilities of administering tax laws, IRS relies extensively on computer systems to support its financial and mission-related operations. As such, it must ensure that its computer systems are effectively secured to protect sensitive financial and taxpayer data gathered when the agency is collecting taxes, processing tax returns, and enforcing tax laws.

IRS also 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. IRS has an important responsibility for protecting sensitive information and implementing effective information system security controls, a component of internal control over financial reporting.

Without effective security controls, computer systems are vulnerable to human actions committed in error or with malicious intent. People acting with malicious intent can use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. These threats to computer systems and related critical infrastructure can come from sources that are internal and external to an organization. Internal threats include equipment failure, human errors, and fraudulent or malevolent acts by employees or contractors. 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. In October 2017, the Treasury Inspector General for Tax Administration stated that security over taxpayer data and protection of IRS resources was the top priority in its list of top management

challenges for the agency for fiscal year 2018.⁹ Furthermore, since 1997, we have designated federal information security as a government-wide high-risk area.¹⁰

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*¹¹ 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.¹²

Information system security 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-wide, system, and business process application levels; business process application controls (input, processing, output, interface, and data management system controls); and user controls (controls performed by people interfacing with information systems).

⁹Department of the Treasury, Treasury Inspector General for Tax Administration, *Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2018*, Memorandum for Secretary Mnuchin (Washington, D.C.: October 2017).

¹⁰GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997) and *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, [GAO-17-317](#) (Washington, D.C.: February 2017).

¹¹Pub. L. No. 97-255, 96 Stat. 814 (1982). The *Federal Managers' Financial Integrity Act* (FMFIA) was codified at 31 U.S.C. § 3512.

¹²GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

Federal law and guidance specify requirements for protecting federal information and systems. The *Federal Information Security Modernization Act of 2014* (FISMA)¹³ is intended to provide a comprehensive framework for ensuring the effectiveness of information system security controls over information resources that support federal operations and assets. To accomplish this, FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide security for the information and systems that support the operations and assets of the agency, using a risk-based approach.

Such a program includes assessing risk; developing and implementing cost-effective security controls, 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. Beyond establishing these information security program requirements, the act also assigned the National Institute of Standards and Technology (NIST) the responsibility for developing standards and guidelines that include minimum information security requirements.

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

IRS has addressed numerous information system security control issues in response to previously reported control deficiencies and our related recommendations. However, continuing and newly identified control deficiencies limited the effectiveness of the agency's implementation of access controls, configuration management, segregation of duties, contingency planning, and components of its information security

¹³The *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, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

program, to prevent or timely detect material misstatements and protect the confidentiality, integrity, and availability of its financial and tax processing systems and information. As indicated in table 1, we have previously made a number of recommendations to IRS to correct these control deficiencies, some of which still remain outstanding, in addition to making new recommendations based on our audit of IRS's fiscal year 2017 financial statements.

Table 1: Status of GAO Information System Security Control Recommendations to IRS to Correct Control Deficiencies at the Conclusion of Fiscal Year 2017

Category	Information security control area	Prior recommendations not implemented at the beginning of fiscal year 2017	Prior recommendations implemented or considered no longer relevant at the end of fiscal year 2017 ^a	Prior recommendations not fully implemented at the end of fiscal year 2017	New recommendations resulting from fiscal year 2017 audit	Total outstanding recommendations at the end of fiscal year 2017
Access controls	Boundary protection	11	(0)	11	—	11
Access controls	Identification and authentication	35	(9)	26	13	39
Access controls	Authorization	22	(6)	16	3	19
Access controls	Cryptography	34	(13)	21	—	21
Access controls	Audit and monitoring	12	(5)	7	5	12
Access controls	Physical security	6	(2)	4	—	4
n/a	Total access controls	120	(35)	85	21	106
n/a	Configuration management	29	(10)	19	13	32
n/a	Segregation of duties	1	(0)	1	—	1
n/a	Contingency planning	2	(1)	1	1	2
Information security program	Risk assessments	1	(0)	1	—	1
Information security program	Policies and procedures	5	(1)	4	—	4

Category	Information security control area	Prior recommendations not implemented at the beginning of fiscal year 2017	Prior recommendations implemented or considered no longer relevant at the end of fiscal year 2017 ^a	Prior recommendations not fully implemented at the end of fiscal year 2017	New recommendations resulting from fiscal year 2017 audit	Total outstanding recommendations at the end of fiscal year 2017
Information security program	Security plans	1	(0)	1	2	3
Information security program	Training	1	(1)	0	—	0
Information security program	Testing and evaluation	5	(1)	4	—	4
Information security program	Remedial actions	1	(0)	1	—	1
n/a	Total information security program	14	(3)	11	2	13
n/a	Grand total	166	(49)	117	37	154

Legend: — = no recommendations made

Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-18-391

^aWe 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. This is accomplished by designing and implementing controls to prevent, limit, and detect unauthorized access to programs, data, facilities, and other computing resources. Access controls include both logical and physical controls related to the (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.

Deficiencies in IRS's network boundary protection continued to exist

Boundary protection controls the logical connectivity into and out of networks and to and from devices attached to the network. 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 management traffic transmitted across an Internet protocol backbone network be encrypted to ensure confidentiality and integrity. In addition, NIST recommends that devices be identified and authenticated prior to establishing a connection, and that approved authorizations for controlling the flow of information between interconnected systems should be enforced.¹⁴

However, IRS did not correct our previously reported boundary control deficiencies, such as not implementing access control lists on certain network devices to prevent unauthorized users from logging into the network devices; and not ensuring that authenticated network protocols were being used on its network devices. Until IRS corrects these deficiencies to its network boundaries, increased risk exists that its network devices and systems could be compromised, which could affect system availability.

IRS inconsistently implemented identification and authentication controls for financial systems

Identification is the process of distinguishing one user from others as a prerequisite for granting access to resources in an information system. User identification (ID) is important because it is 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

¹⁴National 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).

whether individuals are who they claim to be—are typically implemented. Organizations may use other means of authenticating users to determine whether individuals are who they claim to be, such as tokens or biometrics.

IRS had developed and documented policies for identification and authentication. Specifically, the *Internal Revenue Manual* requires password complexity for all IRS information systems with password-based authentication. The manual also requires passwords that are not found in the dictionary and contain at least one numeric character, one special character, one uppercase letter, and one lowercase letter. Passwords for people must be set to expire within 90 days and passwords for service accounts must be set to expire within 366 days. In addition, the manual requires that service account passwords have a minimum length of 14 characters. Further, the manual requires the use of a certificate revocation list to identify personal identity verification (PIV) certificates¹⁵ that have been revoked.

IRS improved identification and authentication by enforcing password complexity for several user- and system-level accounts on various servers and by setting password expiration parameters for user and service accounts on several servers and databases. Nevertheless, deficiencies in authentication persisted. For example, IRS did not:

- enforce password expiration limits for several applications we reviewed;
- enforce minimum password lengths for service accounts supporting several applications we reviewed; and
- enable certificate revocation lists to check PIV certificates for user authentication to a financial system.

Until IRS fully remediates authentication control deficiencies, it is at increased risk that controls could be compromised, permitting unauthorized access to its systems and data.

¹⁵Personal identity verification (PIV) card is a physical identity card, such as a “smart” card, issued to an individual that contains stored identity credentials, such as a photograph, cryptographic keys, or digitized fingerprint, used to verify the identity of the cardholder against the stored credentials by another person or an automated process. PIV certificates can be used for authentication to verify that PIV credentials were issued by an authorized entity, had not expired, and had not been revoked, and that the holder of the credentials was the same individual to whom the PIV card was issued.

IRS did not always limit authorization of user access rights and privileges to only personnel who required it to perform their jobs

Authorization is the process of granting access rights and privileges to a system or a file. Access rights and privileges specify what a user can do after being authenticated to the information system, allowing the authorized user to read or write to files and directories. 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 systems security.

IRS had developed and documented policies for authorizing access to its systems. According to the *Internal Revenue Manual*, system access is to be granted based on the principle of least privilege—that is, the minimum access necessary to perform one’s duties. The manual also requires that user accounts be reviewed for compliance annually, that passwords for contractors expire at the end of the contract period of performance minus one day, and that authorizations for accounts, including non-unique accounts be approved and maintained.

IRS corrected 4 of the 22 authorization control deficiencies that we previously identified. As an example, the agency restricted unnecessary user access on Oracle databases supporting an application. The agency also restricted excessive user privileges to another application by limiting users’ ability to enter certain database commands.

However, authorization control deficiencies still existed in IRS’s computing environment. For example, IRS entered incorrect expiration dates for contractor passwords in the system used for managing user access authorizations. Specifically, the agency set passwords for 10 contractor profiles in production and 197 contractor profiles in the test environment of the mainframe to expire on dates that extended beyond the end of the contract period of performance.

In addition, IRS did not maintain and approve authorizations for 20 non-unique accounts that were used for its training environment.¹⁶ Specifically,

¹⁶A “non-unique” account is a user account that does not have a specific person assigned to that account.

the agency did not provide documentation that authorizations for any of the 20 accounts had been approved or reviewed annually.

These weaknesses place the agency at increased risk that users with excessive privileges, users who should no longer have access to a system, and unauthorized users could inadvertently or deliberately access and modify systems. These risks jeopardize the confidentiality and integrity of the data they contain.

IRS made limited progress in correcting control deficiencies for encryption of sensitive information

Cryptography can be used in identification and authorization to protect the integrity and confidentiality of computer programs and data in transmission or storage. Using algorithms (mathematical functions) and keys (strings of seemingly random bits), cryptographic modules¹⁷ (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. Specifically, the *Internal Revenue Manual* requires that the agency use 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 meet the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication. One such standard is the Federal Information Processing Standard (FIPS) 140-2,¹⁸ which is used for encryption.

¹⁷A cryptographic module is the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including algorithms, and is contained within the encrypted boundary of the module.

¹⁸National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standard 140-2, (Gaithersburg, Md.: May 2001).

IRS corrected 13 of the 34 encryption control deficiencies that we previously identified. For example, the agency encrypted the authentication from its workstations to one of its systems. In addition, the agency configured various platforms and client software to encrypt connections between systems, and used encryption on servers supporting several systems.

However, IRS had not yet addressed 21 of 34 recommendations that we previously made to the agency concerning encryption control deficiencies. For example, it had not enforced the use of FIPS 140-2 compliant encryption algorithms on some systems and applications. In addition, it had not yet encrypted sensitive data on its Oracle databases supporting 11 systems and applications we previously reviewed. As a result, the agency has an increased risk that an unauthorized individual could exploit encryption weaknesses to view and then use data, such as user IDs and passwords, to gain access to systems that contain financial and sensitive data.

IRS has made limited progress enhancing the audit and monitoring controls of its financial systems

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, recognize an ongoing attack, and perform investigations during and after an attack.

IRS had developed and documented policies for auditing and monitoring its systems, and had issued an interim update to its *Internal Revenue Manual*.¹⁹ The manual requires that IRS information systems generate audit records containing details to facilitate the reconstruction of events if unauthorized activity occurs. In addition, it requires the agency to review and analyze these audit records to determine if inappropriate or unusual

¹⁹IRS issued an interim guidance memorandum rescinding *Internal Revenue Manual* 10.8.3, which was the agency's previous standard for auditing and monitoring systems. The interim guidance made *Internal Revenue Manual* 10.8.1 the authority for these requirements.

activity has occurred. Further, the agency's procedures for audit log event identification, analysis, and reporting, require audit plans to be developed, approved, and implemented. Finally, the *Internal Revenue Manual* requires reviews of user and service accounts for compliance with account management requirements to ensure that accounts are still necessary and configured properly.

However, IRS has made limited progress in enhancing its audit and monitoring capabilities. For example, the agency corrected three previously identified weaknesses by reconfiguring the audit trails for several of its databases supporting three applications to enable the reconstruction of specific actions. Nevertheless, deficiencies in the agency's audit and monitoring capabilities persist. In this regard, the agency had not fully implemented 7 of 12 recommendations we previously made to correct deficiencies identified in audit and monitoring controls.²⁰ For example, the agency had neither updated nor implemented its audit and monitoring requirements in several system and application audit plans. Also, it had not enabled database logging, nor reviewed, analyzed, or reported auditable and actionable events on a database supporting a tax payment system. In addition, IRS did not consistently detect improperly configured encryption settings for user and service accounts or detect configuration changes made to the mainframe.

Without effective audit and monitoring controls, IRS's ability to establish individual accountability, monitor compliance with security and configuration management policies, and identify anomalous activity is reduced.

IRS improved physical security controls, but prior deficiencies remain

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. They include, among other things, policies and practices for authorizing individuals' physical access to facilities and resources; and periodically

²⁰As of September 30, 2017, we determined that IRS had addressed 4 of the 12 recommendations. For 7 of the remaining 8 recommendations, IRS had not completed corrective actions. As for the remaining recommendation, we determined that it was no longer relevant due to the changing operating environment and issued a new specific recommendation that more accurately reflects addressing the associated deficiency in the current environment.

reviewing access authorizations in order to ensure that continued access is necessary. At IRS, control measures, such as access cards that are used to permit or deny access to certain areas of a facility, are vital to safeguarding its computing resources.

IRS had developed and documented policies for physically protecting its computer resources. In this regard, the *Internal Revenue Manual* requires access controls to protect employees and contractors, information systems, and the facilities in which the personnel and systems are located. The manual also requires that department managers of restricted areas approve all names added to the authorized access list for restricted areas; and that they review, validate, sign, and date the list monthly and then forward the list to the physical security office for review.

IRS had implemented multiple physical security controls at its enterprise computing centers to safeguard assets against possible theft and malicious actions. For example, the agency implemented security measures to control physical access to restricted areas at its computing center with the use of badge sensors and keypads for card/pin number credentialing. It also corrected a previously identified deficiency by ensuring that network equipment in restricted areas was housed in locked cabinets.

However, IRS had not corrected previously identified deficiencies regarding effectively reviewing access lists of individuals with an ongoing need to access restricted areas at two computing centers. The access lists continued to include individuals who no longer required access, and who should have been removed from the lists. Because individuals may be allowed inappropriate access to restricted areas, IRS has reduced assurance that its computing resources and sensitive information are protected from unauthorized access.

IRS Improved Configuration Management Controls, but Deficiencies Remained

Configuration management administers security features for all hardware, software, and firmware components of an information system throughout its life cycle. Effective configuration management provides reasonable assurance that systems are operating securely and as intended. It encompasses policies, plans, and procedures that call for proper authorization, testing, approval, and tracking of all configuration changes; and for timely software updates to protect against known vulnerabilities.

Ineffective configuration management controls increase the risk that unauthorized changes could occur and that systems are not protected against known vulnerabilities.

IRS had not documented authorizations and approvals of changes to mainframe data and processing

IRS had developed and documented policies for managing changes to its systems. Specifically, the *Internal Revenue Manual* requires that all changes to production systems and processing be authorized in advance and that approvals be documented.

Nevertheless, IRS was unable to provide supporting documentation for 13 changes made to critical mainframe datasets. In addition, as in previous years, the agency continued to alter production data processing on the mainframe—including tax data processing—outside established change control procedures. The lack of effective change management increases the agency's risk that unauthorized changes can be made to applications that result in the loss of data or program integrity.

IRS had not applied critical security patches and used unsupported software on multiple devices

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

During 2017, the agency had not installed critical patch updates to a recently upgraded database supporting an important IRS information system, nor had it addressed deficiencies related to installing critical patch updates identified in prior years. Specifically, the agency still had not applied critical security patches to databases supporting five information systems, including its personnel and payroll system, or to servers supporting eight information systems, including its general ledger system.

In addition, IRS continued to rely on database software that was no longer supported by the vendor. Such reliance is problematic because vendors generally do not provide updates for unsupported software even

if vulnerabilities are known. By not installing patches and replacing unsupported software per its own requirements, IRS has increased the risk that individuals may exploit known vulnerabilities in its systems.

Segregation of Duties and Contingency Planning Control Deficiencies Remained

In addition to access controls and configuration management, 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 segregating incompatible duties and planning for continuity of operations.

IRS had not corrected a prior segregation of duties deficiency for one financial system

Segregation of duties helps to ensure that no single individual can independently control all key aspects of a process or computer-related operation and, thereby, make unauthorized changes. Segregation of duties increases the likelihood that errors and wrongful acts will be detected, 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 certain functions be divided and separated among different individuals in order to prevent harmful activities that can result from collusion. This includes dividing mission functions and distinct information system support functions among different individuals or roles.

However, IRS had not corrected a previously identified deficiency by implementing a process to reduce the risk of users being assigned incompatible security roles for one financial system. Specifically, users were still assigned to security roles and other roles that the agency had defined as incompatible for users who have a security role. Until IRS corrects this deficiency, increased risk exists that inadvertent or deliberate misuse of inappropriate privileges may occur on this system.

IRS developed, documented, tested, and updated contingency plans with results from testing for all but one plan

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 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 documented policies for developing and testing information system contingency plans. Specifically, 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 have the capability to continue performance of mission essential functions during any disruption for up to 30 days or until normal operations can resume. Further, the manual requires that IRS review its contingency plans annually and update them to reflect any changes to the agency's information systems and operating environment, and problems encountered during execution or testing.

IRS corrected a previously identified weakness by documenting the extent to which it had capabilities to continue its essential operations. Specifically, the agency documented the disaster recovery steps for switching two different production system platforms to a disaster recovery environment for its payment posting system. In addition, IRS had tested the 10 contingency plans we reviewed.

The agency also had updated 9 of the 10 contingency plans we reviewed to reflect changes to computer equipment and software supporting the information systems and the operating environment. However, it did not fully update one plan to document the existence of a server that was added to the operating environment for one of its tax processing systems. By not updating the contingency plan to reflect the change to the operating environment for one of its tax processing system, IRS has reduced assurance of its ability to fully restore the system in the event of a service interruption. According to IRS, subsequent to our review, the latest version update of the contingency plan for its tax processing system

was completed in March 2018; however, we have not yet validated this action, but plan to do so during our fiscal year 2018 audit.

IRS Did Not Consistently Implement Certain Components of Its Information Security Program

An underlying reason for the aforementioned information system security control deficiencies in IRS's financial and tax processing systems was that the agency had not consistently implemented components of a comprehensive information security program. An information security management program should establish a 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 (1) periodic assessments of risk; (2) risk-based policies and procedures; (3) plans for providing adequate information security for networks, facilities, and systems; (4) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices; and (5) a process for planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies.

IRS assessed risk and identified some threats and vulnerabilities for selected systems, but did not correct a prior deficiency affecting certain systems

Identifying and assessing information security risks are 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 as a result. 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.

IRS had developed and documented policies for identifying, assessing, and managing information security risk to its systems. In this regard, the *Internal Revenue Manual* requires all information systems and data supporting critical operations and assets to 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 periodically.

IRS had conducted and documented risk assessments for the financial systems we reviewed. The risk assessments identified threats, vulnerabilities, and potential impact to the agency's operations. In addition, IRS had updated the assessments within the agency defined frequency of at least 3 years. However, the agency had not corrected a previously identified deficiency where it lacked sufficient justification for its acceptance of the risks associated with making certain configuration decisions in the production environment.²¹ Until IRS corrects this weakness, the agency has reduced assurance that its process for managing risk is effectively implemented.

IRS had not yet corrected weaknesses in procedures that support components of the agency-wide information security program

A key component of an effective information security program is to develop, document, and implement risk-based policies, procedures, and technical standards. These policies, procedures, and technical standards are to govern the security of an agency's computing environment to reduce the risk associated with unauthorized system access or disruption of services.

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

Nevertheless, deficiencies that we previously reported in IRS's information security procedures, standards, and guidelines had not been fully corrected. For example, the agency

²¹GAO, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data*, [GAO-17-395](#) (Washington, D.C.: July 26, 2017).

- did not have detailed procedures for performing reviews of audit records for a financial system,²² and
- had not updated its 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.²³

Until it corrects these weaknesses, IRS has limited assurance that its staff will consistently perform reviews of the financial system audit records and configure network devices to effectively protect the agency's information systems.

IRS developed and documented security plans, but did not always update them to reflect system or operating environment changes

A system security plan provides an overview of the system's security requirements and describes the extent to which security controls are in place or are planned to meet those requirements. The Office of Management and Budget (OMB) requires that agencies develop system security plans for information systems.²⁴ Further, IRS's *Internal Revenue Manual* requires that the agency's security plans be reviewed at least annually, or as a result of a significant change; and be updated to address changes to the information system and the system's environment of operation. Security plans should also be updated to address problems identified during the plan's implementation or security control assessments.

Although IRS had developed and documented security plans for the 12 systems we reviewed, the agency had not updated 3 of the plans to reflect changes to the information systems or their current operating environment. Specifically, IRS did not update 1 plan to show that the agency had changed the system authentication mechanism to PIV cards, which replaced the weaker encryption that was previously used. In addition, plans for the other 2 systems were not updated to reflect changes in system boundaries, where their interconnections to each other were removed. IRS also did not correct a similar weakness in the plan for

²²[GAO-17-395](#).

²³[GAO-17-395](#).

²⁴Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: July 28, 2016).

a system that covered multiple sub-systems providing network infrastructure services to the agency, which we reported in fiscal year 2016.²⁵

Further, IRS did not update 5 system security plans to remove references to criteria the agency had rescinded. Specifically, IRS rescinded its IT Security Audit Logging Security Standard, effective February 28, 2017. However, at the end of our audit, the plans still referenced the rescinded standard as audit logging criteria.

Without updated system security plans, IRS has less assurance that it has documented and implemented appropriate security controls to protect its sensitive financial and taxpayer information.

Weaknesses remained in testing and evaluating controls

Another key component of an information security program is the testing and evaluation of controls to determine whether they are effective and operating as intended. IRS's *Internal Revenue Manual* requires management to test and evaluate the effectiveness of information security policies and procedures. It also requires the agency to annually test and evaluate the effectiveness of the security controls in IRS information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. The manual further requires that the agency monitor and verify the configuration compliance of mainframe systems using IRS-approved compliance verification applications or the approved security posture monitoring system.

IRS had implemented numerous processes for testing and evaluating its controls to determine whether they were effective and operating as intended. Nevertheless, uncorrected shortcomings continued to exist in the agency's testing and evaluation process. For example, the agency had not

- established test and evaluation procedures to ensure that IRS's control testing methodology and results fully met the intent of the control objectives being tested,²⁶ or

²⁵GAO, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, [GAO-16-398](#) (Washington, D.C.: Mar. 28, 2016).

- addressed limitations with the use of a mainframe tool for verifying compliance with security policies in its mainframe computing environment.²⁷

In addition, IRS had not yet corrected a previously reported shortcoming for considering and documenting the results of its review of internal controls related to financial reporting.²⁸ OMB's *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123, and its related implementation guide (A-123 guide)²⁹ require an agency's management to monitor and assess controls, including controls over automated information 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 further specifies that a service organization's systems are considered to be part of an entity's information system.³⁰ In addition, IRS's documented procedures for the review of external systems that

²⁶GAO, *Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data*, [GAO-15-337](#) (Washington, D.C.: Mar. 19, 2015).

²⁷[GAO-17-395](#).

²⁸[GAO-17-395](#).

²⁹Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123, 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*.

³⁰Agencies 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.

support the agency's financial reporting require that IRS review, when available, those systems' service organization controls (SOC) reports.³¹

Although IRS had reviewed the SOC reports received for external systems used for financial reporting, it had not identified and documented the user controls that it deemed relevant to its internal control environment. Since the agency had not identified the relevant user controls, it had not tested the operating effectiveness for those controls. We reported the same deficiency regarding the SOC reports for two of the same external systems in fiscal year 2016.³²

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 process for testing and evaluating controls, IRS may not be fully aware of vulnerabilities that could adversely affect its critical applications and data.

Deficiencies in IRS's remediation process remained

As part of an information security program, agencies are required to have a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies in information security policies, practices, and procedures. The *Internal Revenue Manual* requires that IRS, among other things, track the status and resolution of all weaknesses and verify that each weakness is corrected before closing them.

Although IRS had a process in place for tracking and implementing remedial actions to resolve known control deficiencies, it was not always effective in verifying whether the remedial actions were successfully implemented. For example, at the beginning of the fiscal year 2017 audit,

³¹American Institute of Certified Public Accountants, Auditing Standards Board, *Attestation Standards: Clarification and Recodification, AT-C Section 320 Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, Statement on Standards for Attestation Engagements No. 18 (April 2016), contains performance and reporting requirements and application guidance for a service auditor examining controls at organizations that provide services to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting.

³²[GAO-17-395](#).

the agency informed us that it had implemented 63 of the 166 recommendations that we made during prior audits. However, we determined that it had effectively implemented only 37 (about 59 percent) of these 63 recommendations.

We also concluded that 7 (of the original 166) recommendations were no longer relevant due to the changes in IRS's operating environment.³³ Further, we found that an additional 5 recommendations (of the original 166) that IRS had not submitted to us for validation, had been adequately addressed by the agency. Collectively, this indicated that the agency had corrected or mitigated deficiencies associated with 49 of the 166 recommendations to resolve control weaknesses that were open at the beginning of the audit.

Although IRS made some progress in correcting or mitigating the previously reported deficiencies, the agency still had not fully or effectively implemented corrective actions for 117—about 70 percent—of the 166 recommendations. This indicates that IRS's remedial action verification process continues to be ineffective, although we previously made a recommendation to the agency to improve its process for verifying the effectiveness of actions to remedy deficiencies.³⁴ Until IRS takes additional steps to implement a more effective process, it will have limited assurance that control deficiencies are being properly mitigated or corrected.

Conclusions

During fiscal year 2017, IRS continued to make progress in addressing deficiencies in internal control and had successfully addressed a number of our prior recommendations concerning information system security control deficiencies. However, continuing and newly identified control deficiencies limited the effectiveness of security controls for protecting the confidentiality, integrity, and availability of the agency's financial and tax processing systems. As a result, sensitive financial and taxpayer data on IRS computer systems will remain vulnerable until the agency addresses

³³These 7 recommendations no longer reflect IRS's current operating environment and will either be reissued to more closely align with the agency's current policies and environment or not be reissued due to being covered by another recommendation.

³⁴[GAO-15-337](#).

the deficiencies for which we previously made 117 recommendations, as well as the newly identified deficiencies we highlight in this report in the areas of access control, configuration management, segregation of duties, contingency planning, and security management.

The collective effect of these deficiencies in information security is the basis of our determination that IRS had a significant deficiency in internal control over financial reporting systems as of September 30, 2017. 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

We are making the following 5 recommendations to IRS:

The Commissioner of Internal Revenue should take steps to improve the implementation of IRS's information security program by entering correct contractor password expiration dates, per IRS's policy, in the system used for managing user access authorizations. (Recommendation 1)

The Commissioner of Internal Revenue should take steps to improve the implementation of IRS's information security program by documenting access authorizations for non-unique accounts. (Recommendation 2)

The Commissioner of Internal Revenue should take steps to improve the implementation of IRS's information security program by reviewing non-unique accounts at least annually, per IRS's policy. (Recommendation 3)

The Commissioner of Internal Revenue should take steps to improve the implementation of IRS's information security program by updating security plans for three systems to reflect changes to their operating environment. (Recommendation 4)

The Commissioner of Internal Revenue should take steps to improve the implementation of IRS's information security program by removing from five systems security plans, references to logging standards that IRS has rescinded. (Recommendation 5)

We are also making 32 technical recommendations in a separate report with limited distribution. These recommendations address information

system security control deficiencies related to identification and authentication, audit and monitoring, configuration management, and contingency planning.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from IRS. In its comments, reproduced in appendix II, the agency agreed with our recommendations and stated that it plans to review them carefully and ensure that its corrective actions include root cause analysis for sustainable fixes that implement appropriate security controls. According to the agency, it is committed to improving its financial management, internal controls, information technology security posture, and the overall effectiveness of its information system controls.

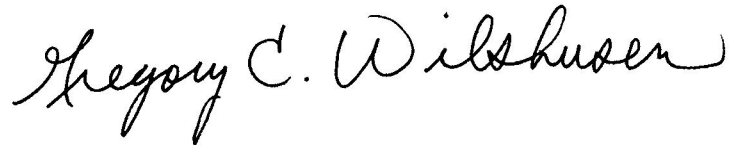
IRS also asserted that the integrity of its financial systems continues to be sound and that the agency has enhanced its ability to protect and defend against malicious acts and expanded its use of continuous application security monitoring and fraud prevention and detection. However, as we noted in this report, although the agency 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

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, stylized 'G' and 'W'.

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objective, Scope, and Methodology

Our objective for this audit was to assess whether IRS's controls over selected financial and tax processing systems were effective in ensuring the confidentiality, integrity, and availability of sensitive financial and taxpayer data.

To determine whether controls over selected 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 two IRS enterprise computing centers located in Martinsburg, West Virginia, and Memphis, Tennessee, as well as IRS facilities in Detroit, Michigan, and New Carrollton, Maryland. We concentrated our evaluation on threats emanating from sources internal to IRS's computer networks. Considering systems that directly or indirectly support the processing of material transactions that are reflected in the agency's financial statements, we focused our work on systems and applications that directly or indirectly support financial and taxpayer information systems.

Our evaluation was based on GAO's *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

- reviewing configurations on IRS's network devices to determine if implemented configurations would protect the devices against malicious code and unauthorized access;
- comparing the complexity, expiration, and other settings for passwords on systems and databases to IRS and federal guidelines to determine whether password strength requirements were being enforced;

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

- evaluating whether access to 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 in order to determine whether implemented cryptographic mechanisms met the requirements of applicable federal standards;
- analyzing audit logs of 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 at both enterprise computing centers to determine whether computer facilities and resources were protected from espionage, sabotage, damage, and theft;
- evaluating the mainframe configuration controls supporting financial management processing;
- evaluating the access controls over disk storage shared across multiple mainframe processing environments;
- evaluating the access controls of the mainframe operating systems that support payroll and taxpayer data processing;
- comparing security configurations on systems and databases to IRS and federal guidelines;
- comparing the release dates of vendor-supplied software components 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 plans to determine whether they 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*,² which established components of an agency-wide

²The *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, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

information security program, we evaluated IRS's implementation of its security program by

- reviewing risk assessments to determine whether they were being updated within the agency defined frequency of at least three years;
- 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 selected 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 financial systems;
- analyzing documentation to determine whether the effectiveness of security controls had been periodically assessed;
- reviewing IRS's actions to correct previously reported control deficiencies to determine whether the agency had effectively mitigated or resolved the control deficiencies; and
- reviewing continuity of operations plans for selected systems to determine whether such plans had been appropriately documented and tested.

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

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 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

July 12, 2018

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

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report titled, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data*, GAO-18-391 (public version).

We are pleased the Government Accountability Office (GAO) recognized our progress in addressing a number of Information Technology (IT) security controls. We also appreciate your acknowledging that the IT organization is relied upon extensively to effectively achieve the IRS mission. IRS processed 9.1 million returns on opening day of Filing Season 2018, with an average of 160 federal acknowledgements every second. IRS received more than 119 million tax returns, answered more than 23 million taxpayer questions on our toll-free help lines and provided in-person assistance to more than 860,000 people. IRS.gov has been visited more than 363 million times this year. These accomplishments are even more remarkable given that Congress enacted 30 retroactive tax law changes in early February 2018 and the IRS implemented these changes in the middle of the filing season.

In FY 2017, our increased effort to address GAO's prior recommendations resulted in successful implementation and closure of 42 prior year recommendations compared to 19 in FY 2016. We anticipate this improvement will continue in FY 2018 due to our proactive implementation of 81 additional prior year recommendations. We feel this proactive approach has also contributed to the decreased number of recommendations from 98 in FY 2016 to 38 in FY 2017.

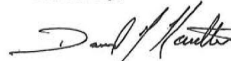
We appreciate the recommendations and are aware that much work remains. We agree with and are reviewing each of your recommendations carefully and will ensure our corrective actions include root cause analysis for sustainable fixes that implement appropriate security controls within our technology and human capital resource limitations, and we will 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.

2

As you know, the IRS is committed to improving its financial management, internal controls, information technology security posture and the overall effectiveness of its information system controls. We have enhanced our ability to protect and defend against malicious acts and expanded our use of continuous application security monitoring and fraud prevention and detection. 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,



David J. Kautter
Acting Commissioner

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 and Larry Crosland, (assistant directors); Vernetta Marquis (analyst-in-charge); William Brown, Alan Daigle, Mickie Gray, Tyrone Hutchins, Sharon Kittrell, J. Andrew Long, Lauren Parker, Brian Palmer, Priscilla Smith, Di'Mond Spencer, and Eugene Stevens, made key contributions to this report.

Appendix IV: Accessible Data

Agency Comment Letter

Accessible Text for Appendix II Comments from the Internal Revenue Service

Page 1

July 12, 2018

Mr. Gregory C. Wilshusen

Director, Information Security Issues

U.S. Government Accountability Office

441 G Street, N.W.

Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report titled, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data*, GAO-18-391 (public version).

We are pleased the Government Accountability Office (GAO) recognized our progress in addressing a number of Information Technology (IT) security controls. We also appreciate your acknowledging that the IT organization is relied upon extensively to effectively achieve the IRS mission. IRS processed 9.1 million returns on opening day of Filing Season 2018, with an average of 160 federal acknowledgements every second. IRS received more than 119 million tax returns, answered more than 23 million taxpayer questions on our toll-free help lines and provided in-person assistance to more than 860,000 people. IRS.gov has been visited more than 363 million times this year. These accomplishments are even more remarkable given that Congress enacted 30 retroactive tax

law changes in early February 2018 and the IRS implemented these changes in the middle of the filing season.

In FY 2017, our increased effort to address GAO's prior recommendations resulted in successful implementation and closure of 42 prior year recommendations compared to 19 in FY 2016. We anticipate this improvement will continue in FY 2018 due to our proactive implementation of 81 additional prior year recommendations. We feel this proactive approach has also contributed to the decreased number of recommendations from 98 in FY 2016 to 38 in FY 2017.

We appreciate the recommendations and are aware that much work remains. We agree with and are reviewing each of your recommendations carefully and will ensure our corrective actions include root cause analysis for sustainable fixes that implement appropriate security controls within our technology and human capital resource limitations, and we will 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.

Page 2

As you know, the IRS is committed to improving its financial management, internal controls, information technology security posture and the overall effectiveness of its information system controls. We have enhanced our ability to protect and defend against malicious acts and expanded our use of continuous application security monitoring and fraud prevention and detection. 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,

David J. Kautter

Acting Commissioner

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 (<https://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 <https://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, <https://www.gao.gov/ordering.htm>.

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

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

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548