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

Accessible Version

July 18, 2019

The Honorable Charles P. Rettig
Commissioner of Internal Revenue

Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls

Dear Mr. Rettig:

In connection with our audit of the Internal Revenue Service's (IRS) fiscal years 2018 and 2017 financial statements, we reported that although internal controls could be improved, IRS maintained, in all material respects, effective internal control over financial reporting as of September 30, 2018, based on criteria established under 31 U.S.C. § 3512(c), (d), commonly known as the Federal Managers' Financial Integrity Act.[1] Those controls provided reasonable assurance that misstatements material to the financial statements would be prevented, or detected and corrected, on a timely basis. However, during our fiscal year 2018 audit, we identified ongoing and new information system security control deficiencies that while not collectively considered a material weakness, were important enough to merit attention by those charged with governance of IRS and therefore represented a significant deficiency in IRS's internal control over its financial reporting systems.[2] Although the significant deficiency in internal control did not affect our opinion on IRS's fiscal year 2018 financial statements, misstatements may occur in unaudited financial information that IRS reports internally or externally because of this significant deficiency.

This report for IRS management presents the new control deficiencies we identified during our fiscal year 2018 testing of information system security controls that are relevant to IRS's internal control over financial reporting and associated recommendations to address them. The report also 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 July 2018 report that remained open at the beginning of our fiscal year 2018 audit.[3]

[1]GAO, *Financial Audit: IRS's Fiscal Years 2018 and 2017 Financial Statements*, GAO-19-150 (Washington, D.C.: Nov. 9, 2018).

[2]A material weakness is a deficiency, or a 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. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by 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.

[3]GAO, *Information Security: IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data*, GAO-18-390SU (Washington, D.C.: July 31, 2018).

This report is a public version of a LIMITED OFFICIAL USE ONLY report that we issued concurrently.[4] IRS deemed much of the information in our concurrently issued report to be sensitive information, which must be protected from public disclosure. Therefore, this report omits sensitive information about the information system security control deficiencies we identified. Although the information provided in this report is more limited, the report addresses the same objectives as the LIMITED OFFICIAL USE ONLY report and uses the same methodology.

Results in Brief

During our fiscal year 2018 audit, we identified 14 new information system security control deficiencies related to access controls, configuration management, segregation of duties, and contingency planning. Specifically, we identified eight access control deficiencies, four configuration management control deficiencies, one segregation of duties deficiency, and one contingency planning deficiency. In the LIMITED OFFICIAL USE ONLY report, we made 20 recommendations to address these control deficiencies.

In addition, we determined that as of September 30, 2018, IRS had completed corrective actions to address deficiencies associated with 46 of the 154 recommendations from our prior financial audits that we reported as open in the status of recommendations in our July 2018 report.[5] Additionally, we found that one deficiency and its associated recommendation are no longer relevant because of changes in the agency's operating environment. As a result, IRS has a total of 127 open recommendations related to the information system security control deficiencies identified during our audits, including 107 previously reported recommendations and 20 recommendations we are making in the LIMITED OFFICIAL USE ONLY report to address deficiencies identified during our fiscal year 2018 audit (see table 1). The specific recommendations from our prior audits and their status as of September 30, 2018, are presented in the LIMITED OFFICIAL USE ONLY report.

Table 1: Status of GAO Recommendations to IRS for Addressing Information System Security Control Deficiencies

Information system security control area	Open recommendations from prior audits	Prior recommendations closed as of September 30, 2018[a]	New recommendations resulting from FY 2018 audit	Total remaining open recommendations
Access controls	106	24	11	**93**
Configuration management	32	13	7	**26**
Segregation of duties	1	1	1	**1**
Contingency planning	2	2	1	**1**
Information security program	13	7	—	**6**
Total	**154**	**47**	**20**	**127**

Legend: FY = fiscal year; — = no recommendations made.

Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-19-474R

[a]We did not consider one control deficiency related to one recommendation to be corrected or mitigated; rather the issues were no longer relevant because of IRS's changing operating environment.

[4]GAO, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls*, GAO-19-473RSU (Washington, D.C.: July 10, 2019).

[5]GAO-18-390SU.

While IRS continued to make progress in addressing information system security control deficiencies and successfully addressed a number of our prior recommendations, these new and continuing information system security control deficiencies, which collectively represent a significant deficiency, increase the risk that IRS's financial reporting and taxpayer data will remain unnecessarily vulnerable to inappropriate and undetected use, modification, or disclosure.

In commenting on a draft of the separately issued LIMITED OFFICIAL USE ONLY report, IRS agreed with our recommendations and stated that it will ensure that its corrective actions include root cause analysis for sustainable fixes that implement appropriate security controls.

Background

As the tax collector of the United States, IRS's mission is to help taxpayers understand and meet their tax responsibilities and to enforce tax laws with integrity and fairness. According to publicly available agency data, in fiscal year 2018, the agency collected about $3.5 trillion in federal tax payments, processed about 225 million returns, and paid about $464 billion in refunds and outlays. IRS employs over 78,000 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 in Memphis, Tennessee.

In carrying out its mission and responsibilities for administering tax laws, 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. IRS relies extensively on computer systems to support its financial and mission-related operations. As such, the agency must ensure that its computer systems are effectively secured to protect the sensitive financial and taxpayer data it collects.

Federal law and guidance specify requirements for protecting federal information and systems. The Federal Information Security Modernization Act of 2014 (FISMA) 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.[6] 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 agency's operations and assets, 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.

Federal law also requires agencies to comply with information security standards that the National Institute of Standards and Technology (NIST) developed. In addition, our *Standards for Internal Control in the Federal Government* provides the overall framework for establishing and

[6]Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283 (Dec. 18, 2014), *codified at* 44 U.S.C. §§ 3551–3558, largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III of the 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.

maintaining an effective internal control system that provides reasonable assurance that the objectives (operations, reporting, and compliance) of an entity will be achieved.[7]

Information system security controls consist of those internal controls that depend on information systems processing, and include general controls (physical and logical access controls, configuration management, segregation of duties, contingency planning, and security management) at the entity-wide, system, and business process application levels;[8] business process application controls (input, processing, output, interface, and data management system controls);[9] and user controls (controls performed by people interfacing with information systems). Without effective information system security controls, computer systems are vulnerable to human actions committed in error or with malicious intent.[10] 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.

Objectives, Scope, and Methodology

Our objectives were to (1) evaluate whether information system security controls over IRS's financial reporting systems were effective in ensuring the confidentiality, integrity, and availability of financial reporting and sensitive taxpayer data and (2) determine the status of the agency's corrective actions as of September 30, 2018, to address information system security control deficiencies and associated recommendations contained in our prior years' reports for which actions were not complete as of September 30, 2017. This work was performed in connection with our audit of IRS's financial statements for the fiscal years ended September 30,

2018, and 2017, for the purpose of supporting our opinion on the agency's internal control over financial reporting.[11]

---

[7]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014), contains the internal control standards that executive agencies are to follow in establishing and maintaining systems of internal control as required by 31 U.S.C. § 3512 (c), (d) (commonly referred to as the Federal Managers' Financial Integrity Act).

[8]General controls help to provide reasonable assurance 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.

[9]Business process application controls help to provide reasonable assurance about the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing.

[10]These actions that threaten computer systems and related critical infrastructure can come from sources both internal and external to an agency. 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 that wish to do harm to an agency's systems.

[11]An 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.

To accomplish these objectives, we reviewed the agency's information security policies, plans, and procedures; tested controls over selected financial reporting systems; reviewed previously reported information system security control deficiencies; and assessed the effectiveness of corrective actions taken to address them. We also interviewed agency officials responsible for managing and operating the selected systems. The focus of our evaluation was limited to certain financial and tax processing systems relevant to IRS's internal control over financial reporting that could compromise the effectiveness of financial reporting and protecting sensitive taxpayer data.

Our evaluation was based on the *Federal Information System Controls Audit Manual*,[12] *Standards for Internal Control in the Federal Government*,[13] NIST guidance, and IRS policies and procedures.

During the course of our work, we communicated our findings to IRS management. We plan to follow up to determine the status of corrective actions taken on the remaining recommendations reported as open in this report during our audit of IRS's fiscal years 2019 and 2018 financial statements. We performed our audit in accordance with U.S. generally accepted government auditing standards. We believe that our audit provides a reasonable basis for our findings and recommendations in our separately issued LIMITED OFFICIAL USE ONLY report.

New Deficiencies Identified in IRS's Information System Security Controls

During our fiscal year 2018 audit, we identified 14 new information system security control deficiencies: eight access control deficiencies, four configuration management deficiencies, one segregation of duties deficiency, and one contingency planning deficiency. We are making 20 recommendations in our separately issued LIMITED OFFICIAL USE ONLY report to address these deficiencies. These 14 information system security control deficiencies are summarized here, and a more detailed discussion and our related recommendations are presented in the separately issued LIMITED OFFICIAL USE ONLY report.

Access Controls

A basic management objective for any agency 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. The eight access control deficiencies we identified during fiscal year 2018 related to the (1) identification and authentication of users, (2) authorization of access permissions, and (3) encryption of sensitive information.

Identification and Authentication

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

[12]GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009), contains the guidance for reviewing information system security controls that affect the confidentiality, integrity, and availability of information and information systems.

[13]GAO-14-704G.

the means by which a system assigns and recognizes specific access privileges. However, the confidentiality of a user ID is typically not protected. For this reason, agencies may use other means of authenticating users—that is, determining whether individuals are who they claim to be—such as tokens or biometrics. Effectively designed and implemented identification and authentication controls require users to authenticate themselves through the use of passwords and other identifiers, such as personal identity verification smart card credentials.[14]

We identified three access control deficiencies in identification and authentication. IRS did not

- enforce the requirement for using the appropriate certificates to electronically sign portable document format documents, including certain tax documents;
- consistently enforce necessary limits for maximum password age for user accounts on certain Oracle databases in accordance with its policies; and
- use multifactor authentication for accessing certain applications in accordance with Office of Management and Budget (OMB) Memorandum M-11-11.[15]

Authorization

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. Effectively designed and implemented authorization controls limit the files and other resources that authenticated users can access and the actions that they can execute based on a valid need that is determined by assigned official duties.

We identified two access control deficiencies regarding authorization. IRS did not

- disable a function within one application that allows certain user accounts to download the application's entire database of information or portions thereof, even though the function is not needed for business purposes, and
- prevent individual user accounts from having unnecessary access to certain databases supporting tax processing systems.

Cryptography

Cryptography controls 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 modules[16]

[14]A personal 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. A PIV certificate 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.

[15]Office of Management and Budget, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*, OMB Memorandum M-11-11 (Washington, D.C.: Feb. 3, 2011).

[16]A 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.

(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. Effectively designed and implemented encryption controls prevent the unauthorized access and disclosure of information (confidentiality) and detect changes to information (integrity).

We identified three access control deficiencies regarding cryptography (i.e., encryption). IRS did not

- encrypt certain servers in accordance with its policies,
- encrypt the email service in accordance with its policies, and
- enforce certain encrypted database connections.

Configuration Management

Configuration management is the administration of 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.

We identified four configuration management control deficiencies. IRS did not

- implement mandatory access controls for an application,
- update unsupported database software and apply vendor-supplied patches for certain applications,
- update third-party software on workstations consistently, and
- upgrade certain outdated and unsupported software network devices.

Segregation of Duties

Segregation of duties helps to ensure that no single individual has authorization to control all key aspects of a process or computer-related operation. Effective segregation of duties also 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 another. 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.

We identified one segregation of duties deficiency. IRS allowed a nonadministrator account to be included in an administrator group of accounts for one of its databases.

Contingency Planning

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 information resources can be protected. 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.

We identified one contingency planning deficiency. IRS assigned only one individual to administer the email service.

Status of Previously Identified Information System Security Control Deficiencies

IRS has continued to address many of the information system security control deficiencies identified in our prior financial audits. As of September 30, 2018, the agency informed us that it had implemented corrective actions to address deficiencies associated with 87 of the 154 recommendations resulting from our prior audits that we reported as open in the status of recommendations in our July 2018 report.[17] However, during our fiscal year 2018 audit, we determined that IRS's actions had effectively addressed deficiencies associated with only 43—about 49 percent—of these 87 recommendations as of September 30, 2018. Also, we determined that one of the 87 recommendations was no longer relevant because of changes in IRS's operating environment. Further, we found that IRS had adequately addressed three of the 67 recommendations that it had not submitted to us for validation. As a result, we determined that 47 of our 154 previously reported recommendations were closed.

Although IRS made some progress in correcting or mitigating the previously reported information system security control deficiencies, additional corrective actions are needed to resolve deficiencies associated with 107 recommendations that remained open as of September 30, 2018.

When combined with the 20 new recommendations we are making in our separately issued LIMITED OFFICIAL USE ONLY report, a total of 127 recommendations to IRS for addressing information system security deficiencies remain open as of September 30, 2018. See table 2 for a summary status of our recommendations to IRS for addressing these deficiencies.

[17]GAO-18-390SU.

Table 2: Summary of GAO Recommendations to IRS for Addressing Information System Security Control Deficiencies

	Information system security control area	Open recommendations from prior audits	Prior recommendations closed as of September 30, 2018[a]	New recommendations resulting from FY 2018 audit	Total remaining open recommendations
Access control	Boundary protection	11	3	—	**8**
	Identification and authentication	39	8	5	**36**
	Authorization	19	6	3	**16**
	Cryptography	21	2	3	**22**
	Audit and monitoring	12	2	—	**10**
	Physical security	4	3	—	**1**
	Total (access controls)	**106**	**24**	**11**	**93**
	Configuration management	32	13	7	**26**
	Segregation of duties	1	1	1	**1**
	Contingency planning	2	2	1	**1**
Information security program	Risk assessments	1	1	—	—
	Policies and procedures	4	3	—	**1**
	Security plans	3	2	—	**1**
	Training	—	—	—	—
	Testing and evaluation	4	1	—	**3**
	Remedial actions	1	—	—	**1**
	Total (information security program)	**13**	**7**	—	**6**
Total		**154**	**47**	**20**	**127**

Legend: FY = fiscal year; — = no recommendations made.

Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-19-474R

[a]We did not consider one control deficiency related to one recommendation to be corrected or mitigated; rather the issues were no longer relevant because of IRS's changing operating environment.

Conclusions

During fiscal year 2018, IRS continued to make progress in addressing deficiencies in internal control and 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 information system security controls for protecting the confidentiality, integrity, and availability of the agency's financial reporting systems. As a result, financial reporting and sensitive taxpayer data on IRS computer systems will remain vulnerable until the agency addresses the deficiencies for which we previously made 107 recommendations, as well as the 20 new recommendations we are making in our

separately issued LIMITED OFFICIAL USE ONLY report for deficiencies related to access control, configuration management, segregation of duties, and contingency planning that we identified during our fiscal year 2018 audit.

Recommendations for Executive Action

To help strengthen information system security controls over financial reporting systems and improve internal control over financial reporting, we recommended that the Commissioner of Internal Revenue, in addition to addressing previously issued recommendations from our prior reports, implement the 20 recommendations to address new deficiencies identified during our fiscal year 2018 audit that are discussed in our separately issued LIMITED OFFICIAL USE ONLY report. These recommendations address information system deficiencies related to identification and authentication, authorization, cryptography, configuration management, segregation of duties, and contingency planning.

Agency Comments

IRS provided comments on the detailed findings and recommendations in the separately issued LIMITED OFFICIAL USE ONLY report. In those comments, IRS agreed with our recommendations and stated that it will ensure that its corrective actions include root cause analysis for sustainable fixes that implement appropriate security controls. IRS also stated that it is committed to improving its financial management, internal controls, information technology security posture, and the overall effectiveness of its information system controls and described certain actions it is taking to do so. We will evaluate the effectiveness of IRS's efforts during our audit of its fiscal year 2019 financial statements.

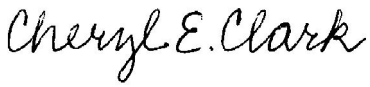
- - - - - - -

In the separately issued LIMITED OFFICIAL USE ONLY report, we noted that the head of a federal agency is required by 31 U.S.C. § 720 to submit a written statement on actions taken or planned on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Oversight and Reform, the congressional committees with jurisdiction over the agency programs and activities that are the subject of our recommendations, and GAO not later than 180 days after the date of this report. A written statement must also be sent to the Senate and House Committees on Appropriations with the agency's first request for appropriations made more than 180 days after the date of this report.

We ae sending copies of this report to Department of the Treasury officials in the Office of the Secretary, the Treasury Inspector General for Tax Administration, and interested congressional parties. In addition, this report is available at no charge on the GAO website at http://www.gao.gov.

We acknowledge and appreciate the cooperation and assistance from IRS officials and staff during our audit of IRS's fiscal years 2018 and 2017 financial statements. If you or your staff have any questions about this report, please contact Cheryl E. Clark at (202) 512-9377 or clarkce@gao.gov or Nancy R. Kingsbury at (202) 512-2700 or kingsburyn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report include Mark Canter (Assistant Director), William Brown, Larry Crosland, Nancy Glover, Tyrone Hutchins, Sharon Kittrell, J. Andrew Long, Vernetta Marquis, Sean Mays, Eugene Stevens, Mike Stevens, and Estelle Tsay-Huang.

Sincerely yours,



Cheryl E. Clark
Director
Financial Management and Assurance

Nancy R. Kingsbury
Managing Director
Applied Research and Methods

(103365)