



441 G St. N.W.
Washington, DC 20548

May 25, 2022

The Honorable Charles P. Rettig
Commissioner of the Internal Revenue Service

Management Report: IRS Needs to Improve Financial Reporting and Information System Controls

Dear Mr. Rettig:

On November 10, 2021, we issued our auditor’s report on the results of our audit of the fiscal years 2021 and 2020 financial statements of the Internal Revenue Service (IRS).¹ As part of this audit, we assessed IRS’s key financial reporting controls, including information system controls.

As we reported in connection with our audit of IRS’s fiscal years 2021 and 2020 financial statements, although certain internal controls could be improved, IRS maintained, in all material respects, effective internal control over financial reporting as of September 30, 2021. Those controls provided reasonable assurance that misstatements material to IRS’s financial statements would be prevented, or detected and corrected, on a timely basis. However, our fiscal year 2021 audit continued to identify two significant deficiencies² in internal control over financial reporting concerning IRS’s unpaid assessments³ and financial reporting systems. We also identified other deficiencies in IRS’s internal control over financial reporting that we do not consider to be material weaknesses or significant deficiencies. Nonetheless, these deficiencies warrant IRS management’s attention.

This report presents the new control deficiencies we identified during our fiscal year 2021 testing of IRS’s internal control over financial reporting. This report also includes the results of our follow-up on the status of IRS’s corrective actions to address recommendations from our prior years’ reports related to internal control over financial reporting that remained open as of September 30, 2020.⁴

¹GAO, *Financial Audit: IRS’s FY 2021 and FY 2020 Financial Statements*, [GAO-22-104649](#) (Washington, D.C.: Nov. 10, 2021).

²A 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. 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 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.

³An unpaid assessment is an enforceable claim against a taxpayer for which specific amounts are due, have been determined, and the person(s) or entities from which a tax is due have been identified. See implementing guidance in the *Internal Revenue Manual* § 1.34.4.1.6(1) p, *Terms/Definitions* (Aug. 25, 2015).

⁴GAO, *Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls*, [GAO-21-401R](#) and [GAO-21-400RSU](#) (Washington, D.C.: May 4, 2021).

This report is a public version of a LIMITED OFFICIAL USE ONLY report that we issued concurrently.⁵ IRS deemed much of the information in the LIMITED OFFICIAL USE ONLY report to be sensitive information, which must be protected from public disclosure. Therefore, this report omits sensitive information about the deficiencies. 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 2021 audit, we identified four new deficiencies in internal control over financial reporting. The new deficiencies related to information system controls, specifically in the areas of access controls and configuration management, and contributed to our reported continuing significant deficiency in IRS's internal control over financial reporting systems. In the LIMITED OFFICIAL USE ONLY report, we are making eight new recommendations to address these control deficiencies.

In addition, we determined that IRS had completed corrective actions to close 68 of 120 recommendations from our prior years' reports related to internal control over financial reporting that remained open as of September 30, 2020. Specifically, IRS's actions addressed 63 information system recommendations and five safeguarding recommendations.⁶

Therefore, including prior and new recommendations, IRS currently has the following 60 open recommendations related to internal control over financial reporting to address:

- 10 transaction cycle recommendations,⁷
- 41 information system recommendations (including eight new recommendations), and
- nine safeguarding recommendations.

Enclosure I provides the 30 open recommendations that are not sensitive in nature from our prior years' reports related to internal control over financial reporting and the status of IRS's corrective actions as of September 30, 2021. The LIMITED OFFICIAL USE ONLY report contains the open recommendations that are sensitive and not sensitive in nature from our prior years' reports related to internal control over financial reporting and the status of IRS's corrective actions as of September 30, 2021.

These new and continuing control deficiencies increase the risk of unauthorized access to, modification of, or disclosure of financial and sensitive taxpayer data and disruption of critical operations. IRS mitigated the potential effect of these control deficiencies primarily through compensating controls that management designed to help detect potential misstatements on the financial statements.

⁵GAO, *Management Report: IRS Needs to Improve Financial Reporting and Information System Controls*, GAO-22-105558SU (Washington, D.C.: May 25, 2022).

⁶Safeguarding is the processes and controls involved in protecting custodial and noncustodial assets, which includes the prevention of loss, theft, and inappropriate disclosure or misuse by employees and other individuals. Custodial and noncustodial assets consist of (1) electronic and hard-copy taxpayer receipts, (2) taxpayer information, (3) facilities (e.g., campuses, lockbox banks, computing centers, field offices, etc.), (4) general property and equipment, and (5) other nontax collections and receipts.

⁷A transaction cycle is a set of business transactions that processes control activities to provide reasonable assurance that relevant financial statement assertions are met.

In commenting on a draft of this report, IRS stated that it is committed to implementing improvements dedicated to promoting the highest standard of financial management, internal controls, and information technology security. IRS's comments are reproduced in enclosure II.

Objectives, Scope, and Methodology

Our objectives were to

- evaluate IRS's internal control over financial reporting⁸ and
- determine the status of IRS's corrective actions to address recommendations from our prior years' reports related to internal control over financial reporting that remained open as of September 30, 2020.

To accomplish these objectives, we reviewed IRS policies and procedures; interviewed IRS management and staff; observed controls in operation; and conducted tests of controls to determine whether controls were designed, implemented, and operating effectively. We performed this work in connection with our audit of IRS's fiscal years 2021 and 2020 financial statements, to support our opinion on whether IRS maintained, in all material respects, effective internal control over financial reporting as of September 30, 2021. We based our evaluation on the *Financial Audit Manual*⁹ and *Federal Information System Controls Audit Manual*.¹⁰

During the course of our work, we communicated our findings to IRS management. We plan to follow up with IRS to determine the status of corrective actions taken on our new recommendations and the recommendations reported as open in this report (see enc. I) as part of our audit of IRS's fiscal year 2022 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 Internal Control over Financial Reporting

During our fiscal year 2021 audit, we identified four new control deficiencies in internal control over financial reporting. The new deficiencies related to information system controls and contributed to our reported continuing significant deficiency in IRS's internal control over financial reporting systems. Three deficiencies related to access controls and one related to configuration management. Because of the sensitive nature involved with the deficiencies, we summarize these four new deficiencies in this report, while our LIMITED OFFICIAL USE ONLY

⁸An 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.

⁹GAO and Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual Volume 1*, [GAO-18-601G](#) (Washington, D.C.: June 2018, updated April 2020), presents a methodology for performing financial statement audits of federal entities in accordance with professional standards.

¹⁰GAO, *Federal Information System Controls Audit Manual (FISCAM)*, [GAO-09-232G](#) (Washington, D.C.: February 2009), presents a methodology for auditing information system controls in federal and governmental entities in accordance with professional standards.

report provides a more detailed discussion of these deficiencies and our associated recommendations.

Access Controls

A basic management objective for any agency is to protect the resources that support its critical operations from unauthorized access. An agency accomplishes this by designing and implementing controls to prevent, limit, and detect unauthorized access to data, programs, equipment, and facilities. Access controls include both logical and physical controls related to (1) protection of system boundaries, (2) identification and authentication, (3) authorization of access permissions, (4) sensitive system resources, (5) audit and monitoring of system activity, and (6) physical security of facilities and computing resources. Appropriately designed and implemented access controls reduce the risk of unauthorized access to, modification of, or disclosure of financial and sensitive taxpayer data and disruption of critical operations.

The three deficiencies in access controls we identified during our fiscal year 2021 audit related to (1) protection of system boundaries and (2) identification and authentication.

Protection of System Boundaries

Boundary protection pertains to protecting a logical or physical boundary around a set of information resources and implementing measures to prevent unauthorized information exchange across the boundary in either direction. Appropriately designed and implemented boundary protection controls can help prevent unnecessary connectivity to an organization's network, decrease the number of access paths that must be managed, and limit the risk of unauthorized access in a shared environment.

We identified one deficiency in access controls related to boundary protection. Specifically, IRS did not provide warning banners in certain databases when database administrators accessed them directly.

Identification and Authentication

Identification is the process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an information system. User identification (ID), which distinguishes one user from all others, is important as a means to assign specific access privileges for the system to recognize. However, the confidentiality of a user ID is typically not protected. For this reason, agencies typically use other means of authenticating users—that is, determining whether individuals are who they claim to be—such as with the use of passwords, tokens, or biometrics. To further increase security, an agency may use a combination of multiple mechanisms (also known as multifactor identification), such as a password with personal identity verification (PIV) card credentials.¹¹ Appropriately designed and implemented identification and authentication controls require users to authenticate themselves using multifactor identification.

We identified two deficiencies in access controls related to identification and authentication. Specifically, IRS did not

- enforce multifactor authentication when users accessed a certain information system and

¹¹A PIV card is a physical identity card, such as a “smart” card, issued to an individual. It 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, were not expired, and were not revoked and that the holder of the credentials was the same individual to whom the PIV card was issued.

- appropriately configure the password for a service account supporting an application.

Configuration Management

Configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point, and systematically controlling changes to that configuration during the system's life cycle. Appropriately designed and implemented configuration management controls provide reasonable assurance that systems are operating securely and as intended. They encompass 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.

We identified one deficiency in configuration management related to configuration settings. Specifically, IRS did not configure the use of a security mechanism to help protect the integrity of its systems.

Status of Prior Years' Recommendations Related to Internal Control over Financial Reporting

IRS has continued to address many of the control deficiencies and associated recommendations related to internal control over financial reporting from our prior years' reports. As of September 30, 2020, there were 10 transaction cycle recommendations, 96 information system recommendations, and 14 safeguarding recommendations from prior years' reports that we reported as open in our May 2021 reports.¹² During our fiscal year 2021 audit, we determined the following:

- IRS made progress in addressing seven of 10 transaction cycle recommendations from our prior years' reports; however, all 10 recommendations remained open. As a result, IRS needs to address 10 transaction cycle recommendations.
- IRS completed corrective actions to address 63 of the 96 information system recommendations from our prior years' reports. As a result, IRS needs to address 41 information system recommendations—33 from our prior years' reports and eight new recommendations that we are making in the LIMITED OFFICIAL USE ONLY report.
- IRS completed corrective actions to address five of the 14 safeguarding recommendations from our prior years' reports. As a result, IRS needs to address nine safeguarding recommendations.

See table 1 for a status of our open recommendations related to internal control over financial reporting and enclosure I for the detailed status of 30 open recommendations that are not sensitive in nature from our prior years' reports related to internal control over financial reporting and the status of IRS's corrective actions as of September 30, 2021. The LIMITED OFFICIAL USE ONLY report contains the status of each of the prior years' open recommendations that are sensitive and not sensitive in nature.

¹²[GAO-21-401R](#) and GAO-21-400RSU.

Table 1: Status of GAO Recommendations to IRS Related to Internal Control over Financial Reporting

Audit area	Open prior years' recommendations through the FY 2020 audit	Prior years' recommendations closed in the FY 2021 audit	New recommendations resulting from the FY 2021 audit	Total open recommendations resulting from the FY 2021 audit
Transaction cycles				
Unpaid assessments	1	—	—	1
Tax outlays				
Refunds	5	—	—	5
Tax credits	2	—	—	2
Total (tax outlays)	7	—	—	7
Property and equipment	1	—	—	1
Nonpayroll	1	—	—	1
Total (transaction cycles)	10	—	—	10
Information systems				
Access controls				
Boundary protection	5	5	1	1
Identification and authentication	21	16	2	7
Authorization	6	6	—	—
Sensitive system resources	24	8	—	16
Audit and monitoring	7	6	—	1
Total (access controls)	63	41	3	25
Configuration management				
Software updates	10	8	—	2
Configuration settings	15	9	5	11
Monitor configuration information	1	—	—	1
Total (configuration management)	26	17	5	14
Segregation of duties	1	1	—	—
Security management	6	4	—	2
Total (information systems)	96	63	8	41
Safeguarding	14	5	—	9
Total	120	68	8	60

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

Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-22-105559

Agency Comments

We provided a draft of this report to IRS for comment. In its comments, reproduced in enclosure II, IRS stated that it is committed to implementing improvements dedicated to promoting the highest standard of financial management, internal controls, and information technology security. Additionally, IRS provided comments on a draft of the separately issued LIMITED OFFICIAL USE ONLY report. In those comments, IRS agreed with our eight new recommendations and provided planned actions to address them. IRS also stated that it will continue its efforts to improve financial systems internal controls and information technology security by implementing initiatives that address the root causes. We plan to follow up to determine the status of corrective actions taken on the recommendations as part of our audit of IRS's fiscal year 2022 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 are sending copies of this report to Secretary of the Treasury, the Treasury Inspector General for Tax Administration, and members of Congress. In addition, this report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact Dawn B. Simpson at (202) 512-3406 or simpsondb@gao.gov or Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov. GAO staff members who made key contributions to this report include Mark Canter (Assistant Director), Sher'rie Bacon, Kisa Bushyeager, Stephen Duraiswamy, Sherwyn Hunte, Tyrone Hutchins, J. Andrew Long, Kevin Metcalfe, Koushik Nalluru, Eugene Stevens, and Anne Thomas.

Sincerely yours,



Dawn B. Simpson
Director, Financial Management and Assurance



Jennifer R. Franks
Director, Information Technology and Cybersecurity

Enclosures - 2

Enclosure I

Status of Prior Years' Recommendations Related to Internal Control over Financial Reporting

Our fiscal year 2021 audit included following up on the status of the Internal Revenue Service's (IRS) corrective actions to address recommendations from our prior years' reports related to internal control over financial reporting that remained open as of September 30, 2020. Table 2 summarizes the corrective actions taken to address 30 previously reported recommendations that are not sensitive in nature and indicates whether the recommendations were open or closed as of September 30, 2021. The LIMITED OFFICIAL USE ONLY report contains the previously reported sensitive and nonsensitive recommendations and indicates whether the recommendations were open or closed as of September 30, 2021. As part of our audit of IRS's fiscal year 2022 financial statements, we plan to follow up to determine the status of corrective actions taken on recommendations that remained open as of September 30, 2021. We define the abbreviations used in the legend at the end of the table.

Table 2: Status of Prior Years' Recommendations Related to Internal Control over Financial Reporting as of September 30, 2021

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
Transaction cycles			
Unpaid assessments			
1.	GAO-19-412R , #19-01	Implement the necessary actions to effectively address the two primary causes of the significant deficiency in IRS's internal control over unpaid assessments. These actions should (1) resolve the system limitations affecting the recording and maintenance of reliable and appropriately classified unpaid assessments and related taxpayer data to support timely and informed management decisions, and enable appropriate financial reporting of unpaid assessment balances throughout the year, and (2) identify the control deficiencies that result in significant errors in taxpayer accounts and implement control procedures to routinely and effectively prevent, or detect and correct, such errors. Actions taken: During fiscal year 2019, IRS documented the key management decisions in the design and use of the estimation process. However, IRS has placed its corrective actions on hold because of limited resources. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.	Open
Refunds			
2.	GAO-16-457R , #16-07	Determine the reason(s) why staff did not always comply with IRS's established policies and procedures related to initiating, monitoring, and reviewing the monitoring of manual refunds and, based on this determination, establish a process to better enforce compliance with these requirements.	Open

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
		<p>Actions taken:</p> <p>During fiscal year 2019, IRS determined that a fully automated process to perform monitoring of manual refunds is the optimal solution to address, at an enterprise level, deficiencies associated with relying on employees to monitor refunds in process and take appropriate action when they encounter potential duplicate or erroneous refund conditions. In addition, IRS plans to develop business requirements and request programming through the UWR process. However, IRS has placed its corrective actions on hold because of limited resources. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.</p>	
3.	GAO-16-457R , #16-10	<p>Identify the cause of and implement a solution for dealing with the periodic backlogs of ICO inventory that is hampering the performance of quality reviews.</p>	Open
		<p>Actions taken:</p> <p>During fiscal year 2020, IRS updated its IRM to remove the requirement to perform quality reviews of at least four cases per week for each employee. However, the updated IRM still requires a quality review of at least 260 cases for each employee during the year. In addition, IRS created plans for dealing with backlogs, which included using seasonal employees, overtime, cross-training, and transferring work to other SPCs. To determine whether IRS's corrective actions addressed the recommendation, we need to perform on-site testing of the controls, which we were unable to do during fiscal years 2020 and 2021 because of the COVID-19 pandemic. As a result, we determined that this recommendation remains open as of September 30, 2021.</p>	
4.	GAO-19-412R , #19-08	<p>Update and implement policies or procedures, or both, to clearly define the roles and responsibilities of second-level managers and IDRS security account administrators for validating the information on USR designation forms, including specifying how the information should be validated.</p>	Open
		<p>Actions taken:</p> <p>During fiscal year 2021, IRS updated the job aid for processing USR designation forms to include procedures for second-level managers and IDRS security account administrators to validate information on the USR designation forms. However, we identified instances where (1) active USRs did not have current designation forms on file and (2) the secondary reviews of USR designation forms were not performed timely. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.</p>	
5.	GAO-19-412R , #19-11	<p>Implement a validity check in the ISRP system to confirm that RSNs that Data Conversion key entry operators enter into the system have the required 14 digits.</p>	Open

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
Actions taken:			
IRS agrees that it needs to develop and implement a UWR for programming changes to systemically validate the RSNs input into the ISRP system. However, IRS has placed its corrective actions on hold because of limited resources. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.			
6.	GAO-20-480R , #20-02	Establish and implement manual refund procedures to direct (1) initiators to document (e.g., record on the taxpayers' accounts or annotate on the related manual refund forms) the justification for bypassing the IAT tool warning related to potential duplicate tax refunds on taxpayers' accounts and (2) managers to monitor whether such warnings were bypassed and review the justifications for reasonableness prior to approving manual refund forms.	Open
Actions taken:			
IRS agrees with the recommendation. However, IRS has placed its corrective actions on hold because of limited resources. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.			
Tax credits			
7.	GAO-19-412R , #19-12	Update and implement policies or procedures, or both, to require that reviewers follow up with tax examiners to verify the errors that tax examiners made in working on cases related to suspicious or questionable tax returns are corrected.	Open
Actions taken:			
In March 2020, IRS updated its IRM to require that reviewers follow up with tax examiners to verify that errors tax examiners made while working cases are corrected. The updated IRM includes policies and procedures for managers and leads to (1) document all cases that are reviewed; (2) track errors found in case reviews; and (3) follow up with tax examiners to ensure that the errors identified have been corrected. Given the sensitivity of the tax processing procedures, we need to perform on-site testing of the controls, which we were unable to do during fiscal years 2020 and 2021 because of the COVID-19 pandemic. As a result, we determined that this recommendation remains open as of September 30, 2021.			
Property and equipment			
8.	GAO-16-457R , #16-13	Establish and implement monitoring procedures designed to reasonably assure that the key detailed information for tangible capitalized P&E is properly recorded and updated in the KISAM system.	Open

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
Actions taken:			
IRS established the Asset Management Program Monitoring and Review procedure, effective October 1, 2016, for performing quarterly sample reviews of IT assets in KISAM. In September 2017, IRS also revised the IRM to require FMSS territory managers or section chiefs to review KISAM key data elements for non-IT assets to verify that they are correct and updated. To determine whether IRS's corrective actions addressed the recommendation, we need to perform on-site floor-to-book inventory testing, which we were unable to do during fiscal years 2020 and 2021 because of the COVID-19 pandemic. As a result, we determined that this recommendation remains open as of September 30, 2021.			
Nonpayroll			
9.	GAO-20-480R , #20-03	Establish and implement actions to provide reasonable assurance that business units record the acceptance of goods and services in a timely manner in accordance with IRS policies and procedures.	Open
Actions taken:			
In fiscal year 2021, IRS developed processes that (1) send earlier notification of invoices to receivers through system-generated emails; (2) improve invoice tracking, notifications, and management oversight related to timely R&A, (3) send executives an additional quarterly notice that addresses significant failures to perform timely recording of R&A; and (4) verify that staff have the proper system access when new commercial contracts are awarded. However, IRS officials indicated that these processes were in effect as of October 1, 2021. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.			
Information systems			
Authorization			
10.	GAO-18-391 , #02	Improve the implementation of IRS's information security program by documenting access authorizations for non-unique accounts.	Closed
Actions taken:			
During our fiscal year 2021 testing, we determined that IRS improved the implementation of its information security program by documenting access authorizations for non-unique accounts. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.			
11.	GAO-18-391 , #03	Improve the implementation of IRS's information security program by reviewing non-unique accounts at least annually, per IRS's policy.	Closed

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
Actions taken:			
During our fiscal year 2021 testing, we determined that IRS improved the implementation of IRS's information security program by reviewing non-unique accounts at least annually, per IRS's policy. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.			
Audit and monitoring			
12.	GAO-17-395 , #01	Implement the audit plans for the 12 systems and applications that we reviewed in the production computing environment.	Closed
Actions taken:			
During our fiscal year 2021 testing, we determined that IRS implemented the audit plans for seven of the 12 systems and applications that we reviewed in the production computing environment in accordance with its policy. The remaining five applications did not require an audit plan. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.			
13.	GAO-17-395 , #02	Ensure that system administrators and security operations analysts are alerted in the event of audit processing failures.	Closed
Actions taken:			
During our fiscal year 2021 testing, we determined that IRS ensured that system administrators and security operations analysts are alerted in the event of audit processing failures. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.			
Security management			
14.	GAO-17-395 , #07	Regularly update configuration standards and guidelines for network devices to incorporate recommendations from industry leaders, security agencies, and key practices from IRS partners to address known vulnerabilities applicable to IRS's environment.	Closed
Actions taken:			
During our fiscal year 2021 testing of network devices, we determined that IRS regularly updated configuration standards and guidelines for network devices to incorporate recommendations from industry leaders and security agencies and key practices from IRS partners to address known vulnerabilities applicable to its environment. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.			
15.	GAO-17-395 , #08	Implement a compliance verification application or other appropriate process to ensure that configuration policies are comprehensively tested on the mainframe.	Closed

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
		<p>Actions taken:</p> <p>During our fiscal year 2021 testing, we determined that IRS implemented a compliance verification application to ensure that configuration policies are comprehensively tested on the mainframe. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.</p>	
16.	GAO-21-401R, #01	Reasonably assure that reviews of external third parties' systems reference current documentation that supports IRS assessments of risk.	Open
		<p>Actions taken:</p> <p>During our fiscal year 2021 testing, IRS officials indicated that they plan to address this recommendation in the future. As a result, this recommendation remains open as of September 30, 2021.</p>	
Safeguarding			
Safeguarding			
17.	GAO-13-420R, #13-05	Perform a risk assessment to determine the appropriate level of IDRS access that should be granted to employee groups that handle hard-copy taxpayer receipts and related sensitive taxpayer information as part of their job responsibilities.	Open
		<p>Actions taken:</p> <p>During fiscal year 2020, the SB/SE organization completed risk assessments to determine the appropriate level of IDRS access granted to the employees who handle hard-copy taxpayer receipts and related sensitive taxpayer information as part of their job responsibilities. However, IRS officials indicated that the TAS organization will address this recommendation in the future. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.</p>	
18.	GAO-13-420R, #13-06	Based on the results of the risk assessment, update the IRM accordingly to specify the appropriate level of IDRS access that should be allowed for (1) remittance perfection technicians and (2) all other employee groups with IDRS access that handle hard-copy taxpayer receipts and related sensitive information as part of their job responsibilities.	Open
		<p>Actions taken:</p> <p>During fiscal year 2021, the SB/SE and TE/GE organizations updated applicable IRM sections to include policy changes on risk mitigation, including specifying the appropriate level of IDRS access allowed for employee groups who handle hard-copy taxpayer receipts and related sensitive information. However, IRS officials indicated that the TAS organization will address this recommendation in the future. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.</p>	

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
19.	GAO-13-420R , #13-07	Establish procedures to implement the updated IRM, including required steps to follow to prevent (1) remittance perfection technicians and (2) all other employee groups that handle hard-copy taxpayer receipts and related sensitive information as part of their job responsibilities from gaining access to command codes not required as part of their designated job duties.	Open
Actions taken:			
During fiscal year 2021, the SB/SE and TE/GE organizations established procedures in the applicable IRM sections to prevent employee groups who handle hard-copy taxpayer receipts and related sensitive information from gaining access to command codes not required as part of their designated job duties. However, IRS officials indicated that the TAS organization will address this recommendation in the future. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.			
20.	GAO-15-480R , #15-07	Establish procedures to monitor whether non-IRS contractors with unescorted physical access to IRS facilities are receiving unauthorized access awareness training.	Open
Actions taken:			
During fiscal year 2021, IRS developed an SOP to establish policies and procedures for monitoring and enforcing training requirements that allow contractors to maintain unescorted access to IRS facilities. However, during our testing of the implementation of the policies and procedures, we identified instances where the forms documenting the training of non-IRS contractors with unescorted access to IRS facilities were not complete. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.			
21.	GAO-15-480R , #15-08	Determine the reasons why staff did not consistently comply with IRS's existing requirements for the final candling of receipts at SCCs and lockbox banks, including logging remittances found during final candling on the final candling log at the time of discovery, safeguarding the remittances at the time of discovery, transferring the remittances to the deposit unit promptly, and passing one envelope at a time over the light source, and based on this determination, establish a process to better enforce compliance with these requirements.	Closed
Actions taken:			
In fiscal year 2021, IRS stated that it will rely on the Submission Processing internal control reviews in order to achieve better compliance and resolution of previously identified risks related to candling processes and procedures performed at the SCCs. These reviews include requirements for assessing whether SCC Candling Unit staff perform required procedures during final candling of receipts, including (1) logging remittances found during final candling on the final candling log at the time of discovery, (2) safeguarding the remittances at the time of discovery, (3) transferring the remittances to the deposit unit promptly, and (4) passing one envelope at a time over the light source. During our testing, we found no exceptions related to			

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
		this control. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.	
22.	GAO-17-454R , #17-03	Strengthen the process for reasonably assuring that the IRM is reviewed annually to align with the current control procedures and guidance being implemented by agency personnel. This should include a mechanism for reasonably assuring that program owner directors (1) review their respective program control activities and related guidance annually and timely update the IRM as needed, (2) document their reviews, and (3) utilize interim guidance and supplemental guidance correctly for their intended purposes.	Closed
		<p>Actions taken:</p> <p>In fiscal year 2018, IRS created an annual IRM review and certification requirement to reasonably assure that all IRM sections align with the current control procedures and guidance that IRS personnel are implementing. In addition, the IRS business units developed action plans to achieve substantial compliance with the IRM review and certification requirement. During fiscal year 2021, we confirmed that these organizations had completed their action plans. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.</p>	
23.	GAO-18-393R , #18-03	Develop and implement policies in the IRM for conducting and monitoring the Submission Processing internal control review. These policies should include or be accompanied by procedures to (1) assess and update the review questions and cited IRM criteria to reasonably assure they align with the controls under review; (2) periodically evaluate and document a review of the error threshold methodology to assess its current validity based on changes to the operating environment; (3) report findings identified in the Findings and Corrective Actions Report; and (4) assess and monitor (a) safeguarding of internal control activities across all work shifts, particularly during peak seasons, (b) safeguarding of internal control activities for the appropriate use and destruction of hard-copy taxpayer information, and (c) the results of relevant functional level reviews.	Open
		<p>Actions taken:</p> <p>In fiscal years 2019 and 2020, IRS established policies and procedures to address our recommendation. However, during our fiscal year 2021 testing of the implementation of the policies and procedures, we identified that the May 2021 and June 2021 Submission Processing internal control reviews performed at two SPCs were not complete and documented, as required. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.</p>	

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
24.	GAO-18-393R, #18-05	<p>Develop and implement policies in the IRM for conducting and monitoring the AEHR review. These policies should include or be accompanied by procedures for IRS management responsible for establishing policies related to safeguarding controls to (1) periodically monitor the results of the review and (2) reasonably assure that corrective actions for all identified deficiencies are tracked until fully implemented.</p> <p>Actions taken:</p> <p>During fiscal year 2021, IRS updated policies in the IRM and related procedures for completing the AEHR reviews within IRS's new automated tool. However, during our testing of the implementation of the policies and procedures, we identified that the May 2021 and June 2021 AEHR review certifications for one IRS facility did not include certifications by both the physical security specialist and the section chief, as required by the procedures. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.</p>	Open
25.	GAO-19-412R, #19-02	<p>Document and implement a formal comprehensive strategy to provide reasonable assurance concerning its nationwide coordination, consistency, and accountability for internal control over key areas of physical security. This strategy should include nationwide improvements for (1) coordinating among the functional areas involved in physical security; (2) implementing and monitoring the effectiveness of physical security policies, procedures, and internal controls; and (3) ongoing communication in identifying, documenting, and taking corrective action to resolve underlying control issues that affect IRS's facilities.</p> <p>Actions taken:</p> <p>In April 2020, IRS finished developing its nationwide physical security strategy. By March 2021, IRS finished establishing the framework to implement the strategy, which provided reasonable assurance concerning IRS's nationwide coordination, consistency, and accountability for internal control over key areas of physical security. For example, as part of its strategy, IRS implemented (1) a process to ensure that functional areas, such as policy and operations, coordinate to develop and update physical security policy; (2) a mechanism to track the completion of critical security deliverables across facilities to monitor compliance with policies and ensure the effectiveness of internal controls; and (3) a Quality Assurance office to ensure ongoing communication in identifying, documenting, and taking corrective action to resolve underlying control issues that affect the security of IRS's facilities. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.</p>	Closed
26.	GAO-19-412R, #19-04	<p>Establish and implement policies and procedures requiring that corrective actions be documented in the Alarm Maintenance and Testing Certification Report for malfunctioning alarms identified in the annual alarm tests.</p>	Open

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
		<p>Actions taken:</p> <p>During fiscal year 2021, IRS updated policies in the IRM and related procedures for completing the ACR (formerly Alarm Maintenance and Testing Certification Report) within IRS's new automated tool. However, during our testing of the implementation of the policies and procedures, we identified that in connection to the annual alarm testing and preventative maintenance conducted at the Martinsburg Computing Center, there was no evidence of corrective actions being documented on the fiscal year 2021 ACR to address identified alarm failures. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.</p>	
27.	GAO-19-412R , #19-05	<p>Establish and implement policies or procedures, or both, to provide reasonable assurance that the video surveillance systems at all IRS facilities record activity at the correct time and are properly secured. The policies or procedures should include periodic checks and adjustments, as needed, as part of the annual service and maintenance of security equipment and systems.</p> <p>Actions taken:</p> <p>In fiscal year 2020, IRS updated policies in the IRM and related procedures requiring the completion of annual maintenance of VSSs at IRS facilities to reasonably assure that (1) VSSs are operational, recording activity at the correct time, and properly secured and (2) any related corrective actions and completion dates are properly documented and monitored. In fiscal year 2021, IRS updated policies in the IRM and related procedures for completing annual maintenance of the VSSs within IRS's automated tool, to further ensure consistent and timely completion. During our testing, we reviewed documentation evidencing the annual maintenance of VSSs at three IRS facilities and found no exceptions related to this control. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.</p>	Closed
28.	GAO-19-412R , #19-06	<p>Update and implement policies or procedures, or both, to clarify (1) who is responsible for conducting the annual review of the visitor access logs, (2) the date by which the review is to be conducted, and (3) how the review should be documented.</p> <p>Actions taken:</p> <p>In March 2020, IRS updated procedures to clarify (1) who is responsible for reviewing the visitor access logs, (2) the date by which the reviews are to be conducted, and (3) how the reviews should be documented. However, during our fiscal year 2021 testing of the implementation of the procedures, we identified that visitor access logs for three computer rooms at three facilities did not include the digital signatures of the IT approving officials/computer room managers, certifying review of the forms, as required. As a result, we determined that IRS had not completed its corrective actions as of September 30, 2021, and that this recommendation remains open.</p>	Open

Enclosure I

No.	GAO source report and recommendation number	Recommendation and analysis of corrective actions taken	Recommendation status
29.	GAO-19-412R, #19-07	(1) Identify the reason IRS's policies and procedures related to the transmittal forms were not always followed and (2) design and implement actions to provide reasonable assurance that SB/SE units comply with these policies and procedures. Actions taken: In October 2019, the SB/SE Field Collection organization determined that the reasons the policies and procedures related to the transmittal forms were not always followed were either a lack of understanding of the requirements or a lack of consistency in adhering to them. In response, the SB/SE Field Collection organization distributed a memorandum to its area directors, territory managers, and group managers, reminding them of the required remittance processing procedures, emphasizing the importance of following the procedures, and requesting that they further distribute the information in the memorandum within their organizations. IRS officials stated that the memorandum will help assure that SB/SE Field Collection units comply with the policies and procedures related to the transmittal forms. In addition, in July 2020, the SB/SE Examination organization updated the IRM to clarify and supplement the service-wide guidance for the appropriate control, monitoring, and review of the transmittal forms. Given the sensitivity of the remittance processing procedures, we need to perform on-site testing of the controls, which we were unable to do during fiscal years 2020 and 2021 because of the COVID-19 pandemic. As a result, we determined that this recommendation remains open as of September 30, 2021.	Open
30.	GAO-20-480R, #20-01	Update and implement policies and procedures for developing a courier contingency plan to prohibit managers responsible for overseeing the preparation of taxpayer receipts for deposits from also transporting them to financial institutions. Actions taken: In fiscal year 2020, IRS updated the IRM to prohibit any management official listed in the courier contingency plan as being responsible for delivering taxpayer receipts for deposit from assisting or overseeing the preparation of the daily deposit package, when operating under the courier contingency plan. In fiscal year 2021, IRS updated the IRM to enhance the clarity of these requirements. During our testing, we reviewed the courier contingency plans for two SPCs and found no exceptions related to this control. As a result, we concluded that IRS's corrective actions as of September 30, 2021, were adequate to close this recommendation.	Closed

Legend:

ACR: Annual Maintenance and Testing Certification Report
 AEHR: All Events History Report
 FMSS: Facilities Management and Security Services
 IAT: Integrated Automation Technologies
 ICO: Input Correction Operation
 IDRS: Integrated Data Retrieval System
 IRM: *Internal Revenue Manual*
 IRS: Internal Revenue Service
 ISRP: Integrated Submission and Remittance Processing
 IT: information technology

Enclosure I

KISAM: Knowledge Incident/Problem Service Asset Management
P&E: property and equipment
R&A: receipt and acceptance
RSN: refund schedule number
SB/SE: Small Business/Self-Employed
SCC: service center campus
SOP: Standard Operating Procedure
SPC: Submission Processing Center
TAS: Taxpayer Advocate Service
TE/GE: Tax Exempt & Government Entities
USR: unit security representative
UWR: Unified Work Request
VSS: video surveillance system

Source: GAO. | GAO-22-105559

Enclosure II

Comments from the Internal Revenue Service



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

May 6, 2022

Ms. Dawn Simpson
Director, Financial Management and Assurance
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Simpson:

I am writing in response to the Government Accountability Office (GAO) draft report titled, Management Report: IRS Needs to Improve Financial Reporting and Information System Controls (GAO-22-105559). We are pleased that GAO acknowledged our progress in addressing our financial management challenges and agreed to close sixty-eight prior year financial management recommendations.

Notably, during fiscal year 2021, the IRS successfully implemented the Coronavirus Response and Relief Supplemental Appropriations Act of 2021, resulting in the issuance of a second round of Economic Impact Payments; the IRS issued most of these payments within two days following enactment of the legislation. While meeting the challenges presented by the pandemic, the IRS once again successfully completed the financial statement audit as scheduled.

We are committed to implementing improvements dedicated to promoting the highest standard of financial management, internal controls and information technology security. If you have any questions, please contact me, or a member of your staff may contact Teresa Hunter, Chief Financial Officer, at 202-317-6400.

Sincerely,

Charles P.
Rettig

Digitally signed by
Charles P. Rettig
Date: 2022.05.06
13:47:13 -04'00'

Charles P. Rettig

(105559)

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.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

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 [Email 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 FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

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



Please Print on Recycled Paper.