



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

May 13, 2020

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 2019 and 2018 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, 2019, 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 2019 audit, we identified new and continuing deficiencies in information system security controls 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 over financial reporting systems did not affect our opinion on IRS’s fiscal year 2019 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 2019 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 deficiencies in information system security controls and associated recommendations contained in our July 2019 report that remained open as of September 30, 2018.³

¹GAO, *Financial Audit: IRS’s FY 2019 and FY 2018 Financial Statements*, [GAO-20-159](#) (Washington, D.C.: Nov. 8, 2019).

²A 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.

³GAO, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service’s Information System Security Controls*, [GAO-19-473RSU](#) (Washington, D.C.: July 18, 2019).

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 deficiencies in information system security controls 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 2019 audit, we identified 11 new deficiencies in information system security controls related to access controls, configuration management, segregation of duties, and information security management program controls. Specifically, we identified five deficiencies related to access controls, three deficiencies related to configuration management, one deficiency related to segregation of duties, and two deficiencies related to information security management program controls. In the LIMITED OFFICIAL USE ONLY report, we are making 18 recommendations to address these control deficiencies.

In addition, we determined that as of September 30, 2019, IRS had completed corrective actions to address deficiencies associated with 13 of the 127 recommendations we reported as open in our July 2019 report.⁵ As a result, IRS has 132 open recommendations related to deficiencies in information system security controls identified during our audits, including 114 previously reported recommendations and 18 recommendations we are making in the LIMITED OFFICIAL USE ONLY report to address deficiencies identified during our fiscal year 2019 audit (see table 1). The specific recommendations from our prior audits and their status as of September 30, 2019, are presented in the LIMITED OFFICIAL USE ONLY report.

Table 1: Summary of GAO Recommendations to IRS for Addressing Deficiencies in Information System Security Controls

Information system security control area	Open recommendations from prior audits as of September 30, 2018	Prior recommendations closed as of September 30, 2019	New recommendations resulting from FY 2019 audit	Total remaining open recommendations
Access controls	93	8	7	92
Configuration management	26	3	7	30
Segregation of duties	1	—	1	2
Contingency planning	1	1	—	—
Information security management program	6	1	3	8
Total	127	13	18	132

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

Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-20-411R

While IRS continued to make progress in addressing deficiencies in information system security controls and successfully addressed a number of our prior recommendations, these new and

⁴GAO, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls*, GAO-20-410RSU (Washington, D.C.: May 13, 2020).

⁵GAO-19-473RSU.

continuing deficiencies that collectively represent a significant deficiency increase the risk of unauthorized access to, modification of, or disclosure of financial reporting and taxpayer data and disruption of critical operations.

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.

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 agency data, in fiscal year 2019, the agency collected about \$3.6 trillion in federal tax payments, processed about 255 million returns, and paid about \$452 billion in refunds and outlays.

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 it effectively secures its computer systems to protect the financial and federal taxpayer data it collects.

Federal law and implementing 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 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. FISMA states that 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.

FISMA requires the Secretary of Homeland Security, in consultation with the Director of the Office of Management and Budget (OMB), to develop and oversee the implementation of binding operational directives to agencies to implement the information security policies, principles, standards, and guidelines that OMB developed. Further, FISMA requires the Secretary of Homeland Security, in consultation with OMB, to coordinate government-wide efforts on information security policies and practices, including consultation with the National Institute of Standards and Technology (NIST) and the Chief Information Officers Council. Federal law requires that agencies comply with NIST information security standards. In addition, our *Standards for Internal Control in the Federal Government* provides the overall framework for establishing and maintaining an effective internal control system that provides reasonable

⁶Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), *codified at* 44 U.S.C. §§ 3551–3558, largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), which was 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 relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

assurance that the objectives (operations, reporting, and compliance) of an entity will be achieved.⁷

Information system security controls consist of 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 (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 reasonably assuring the confidentiality, integrity, and availability of financial reporting and federal taxpayer data and (2) determine the status of the agency's corrective actions as of September 30, 2019, to address deficiencies in information system security controls and associated recommendations contained in our prior years' reports for which actions were not complete as of September 30, 2018. We performed this work in connection with our audit of IRS's financial statements for the fiscal years ended September 30,

⁷GAO, *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).

⁸General 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 reasonably assure that backup and recovery plans are adequate and tested to reasonably assure 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.

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

¹⁰These 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 foreign governments that wish to do harm to an agency's systems.

2019, and 2018, to support our opinion on the agency's internal control over financial reporting.¹¹

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 deficiencies in information system security controls; 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 federal taxpayer data.

Our evaluation was based on the *Federal Information System Controls Audit Manual*,¹² *Standards for Internal Control in the Federal Government*,¹³ OMB memorandums, NIST publications, 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 fiscal year 2020 audit of IRS 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 2019 audit, we identified 11 new deficiencies in information system security controls: five deficiencies related to access controls, three deficiencies related to configuration management, one deficiency related to segregation of duties, and two deficiencies related to information security management program controls. We are making 18 recommendations in our separately issued LIMITED OFFICIAL USE ONLY report to address these deficiencies. The 11 deficiencies in information system security controls 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. An agency accomplishes this by designing and implementing controls to prevent, limit, and detect unauthorized access to programs, data,

¹¹An 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.

¹²GAO, *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](#).

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 five deficiencies in access controls we identified during our fiscal year 2019 audit 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 a system uses it to assign and recognize 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 using passwords and other identifiers, such as personal identity verification smart card credentials.¹⁴

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

- restrict employees from adding certificates that the Department of the Treasury had not approved to the Adobe Acrobat Trusted Identities list¹⁵ and
- use multifactor authentication for accessing a certain information system.

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 related to their assigned duties.

We identified one deficiency in access controls related to authorization. IRS did not update documentation supporting authorization and access for managing servers.

¹⁴A personal identity verification (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 had not been revoked, and that the holder of the credentials was the same individual to whom the PIV card was issued.

¹⁵The Adobe Acrobat Trusted Identities list provides a repository of trusted certificates. A certificate can be a trusted root or self-signed certificate used for signing or validating documents.

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 modules¹⁶ (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 in a file to determine whether any changes have been made, thus providing reasonable assurance of 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 can help prevent unauthorized access and disclosure of information (confidentiality) and detect changes to information (integrity).

We identified two deficiencies in access controls related to cryptography (i.e., encryption). IRS did not

- implement cryptographic mechanisms to secure certain data in a system environment that processes taxpayer data and
- enforce the use of NIST Federal Information Processing Standards 140-2-compliant encryption algorithms for certain operating systems.¹⁷

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 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 three deficiencies related to configuration management. IRS did not

- implement mandatory access control policies for Linux servers supporting certain applications,
- consistently install patches to a Windows server supporting a certain application, and
- consistently install patches to a hypervisor to support server virtualization across the IRS environment.¹⁸

¹⁶A 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.

¹⁷National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-2 (Gaithersburg, Md.: May 2001).

¹⁸A hypervisor provides virtualization of hardware that allows multiple guest operating systems to run on a single host computer. It enables shared computing resources, such as processors, memory, networking, and hard drives, between all of the guest operating systems.

Segregation of Duties

Segregating duties provides reasonable assurance 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 deficiency related to segregation of duties. IRS allowed incompatible user roles to be assigned to certain employees for one of its financial reporting systems.

Information Security Management Program

An information security management program is the foundation of a security control structure and reflects senior management's commitment to addressing security risks. An effective information security management program provides a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed information security management program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low risk resources.

We identified two deficiencies related to information security management program. IRS did not

- have properly authorized Authorization to Operate memos or applicable documents signed by appropriate officials for accepting risks of external systems (i.e., systems IRS does not own or operate)¹⁹ and
- always follow its Risk-Based Decision request procedures.²⁰

Status of Previously Identified Deficiencies in IRS's Information System Security Controls

IRS has continued to address many of the deficiencies in information system security controls identified in our prior financial audits. As of September 30, 2019, the agency informed us that it had implemented corrective actions to address deficiencies associated with 14 of the 127 recommendations resulting from our prior audits that we reported as open in our July 2019 report.²¹ However, during our fiscal year 2019 audit, we determined that IRS's actions had effectively addressed deficiencies associated with only 10 of these 14 recommendations as of September 30, 2019. We also found that IRS had adequately addressed three of the 113

¹⁹Authorization to Operate is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the United States based on the implementation of an agreed-upon set of security controls.

²⁰A Risk-Based Decision (RBD) request is the result of an analysis of risk to organizational operations (including mission, function, image, or reputation), organizational assets, individuals, other organizations, and the United States, and a determination that a requirement can be met (or not met) only with an RBD to an IRS information technology security policy, requirement, or standard.

²¹GAO-19-473RSU.

recommendations that it had not submitted to us for validation. As a result, we determined that 13 of our 127 previously reported recommendations were closed.

Although IRS made some progress in correcting or mitigating the previously reported deficiencies in information system security controls, additional corrective actions are needed to resolve deficiencies associated with 114 recommendations that remained open as of September 30, 2019.

When combined with the 18 new recommendations we are making in our separately issued LIMITED OFFICIAL USE ONLY report, a total of 132 recommendations to IRS for addressing deficiencies in information system security controls remain open as of September 30, 2019. See table 2 for a summary status of our recommendations to IRS for addressing these deficiencies.

Table 2: Status of GAO Recommendations to IRS for Addressing Deficiencies in Information System Security Controls

Information system security control area	Open recommendations from prior audits as of September 30, 2018	Prior recommendations closed as of September 30, 2019	New recommendations resulting from FY 2019 audit	Total remaining open recommendations
Access control				
Boundary protection	8	—	—	8
Identification and authentication	36	1	2	37
Authorization	16	4	1	13
Cryptography	22	2	4	24
Audit and monitoring	10	—	—	10
Physical security	1	1	—	—
Total (access controls)	93	8	7	92
Configuration management	26	3	7	30
Segregation of duties	1	—	1	2
Contingency planning	1	1	—	—
Information security management program				
Risk assessments	—	—	3	3
Policies and procedures	1	—	—	1
Security plans	1	1	—	—
Training	—	—	—	—
Testing and evaluation	3	—	—	3
Remedial actions	1	—	—	1
Total (information security management program)	6	1	3	8
Total	127	13	18	132

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

Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-20-411R

Conclusions

During fiscal year 2019, IRS continued to make progress in addressing deficiencies in its internal controls and successfully addressed a number of our prior recommendations concerning deficiencies in information system security controls. However, newly identified and continuing control deficiencies collectively represent a significant deficiency in IRS's internal control over financial reporting systems. Such deficiencies increase the risk of unauthorized access to, modification of, or disclosure of financial reporting and taxpayer data and disruption of critical operations. As a result, financial reporting and federal taxpayer data on IRS computer systems will remain vulnerable until the agency addresses the deficiencies for which we previously made 114 recommendations as well as the 18 new recommendations we are making in our separately issued LIMITED OFFICIAL USE ONLY report for deficiencies related to access controls, configuration management, segregation of duties, and information security management program that we identified during our fiscal year 2019 audit.

Recommendations for Executive Action

To help strengthen information system security controls over financial reporting systems and improve internal control over financial reporting, we recommend that the Commissioner of Internal Revenue, in addition to addressing previously issued recommendations from our prior reports, implement the 18 recommendations to address new deficiencies identified during our fiscal year 2019 audit that are discussed in our separately issued LIMITED OFFICIAL USE ONLY report. These recommendations address deficiencies in information system security controls related to access controls, configuration management, segregation of duties, and information security management program.

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. 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. We will evaluate the effectiveness of IRS's efforts during our audit of its fiscal year 2020 financial statements.

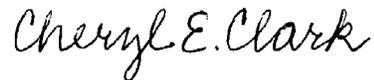
- - - - -

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 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 <https://www.gao.gov>.

We acknowledge and appreciate the cooperation and assistance from IRS officials and staff during our audit of IRS's fiscal years 2019 and 2018 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 Vijay A. D'Souza at (202) 512-6240 or dsouzav@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), Sher'rie Bacon, Larry Crosland, Nancy Glover, Tyrone Hutchins, J. Andrew Long, Vernetta Marquis, Kevin Metcalfe, Koushik Nalluru, Eugene Stevens, Shawn Ward, and Angela Wills.

Sincerely yours,



Cheryl E. Clark
Director, Financial Management and Assurance



Vijay A. D'Souza
Director, Information Technology and Cybersecurity

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/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

