

# TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



## Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021

December 14, 2021

Report Number: 2022-20-005

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

[TIGTACommunications@tigta.treas.gov](mailto:TIGTACommunications@tigta.treas.gov) | [www.treasury.gov/tigta](http://www.treasury.gov/tigta)

**Why TIGTA Did This Audit**

This audit was initiated because the IRS Restructuring and Reform Act of 1998 requires TIGTA to annually assess and report on an evaluation of the adequacy and security of IRS information technology. Our overall objective was to assess the adequacy and security of the IRS's information technology.

**Impact on Taxpayers**

In Fiscal Year 2021, the IRS collected approximately \$4.1 trillion in Federal tax payments, and processed 269 million tax returns and forms. In addition, Federal tax refund and outlay activities by the IRS were approximately \$1.1 trillion. This included approximately \$570 billion in Coronavirus Disease 2019 economic impact payments.

The IRS employs approximately 81,600 people in its Washington, D.C., Headquarters and 501 offices in all 50 States and U.S. territories.

The IRS relies extensively on computerized systems to support its financial and mission-related operations. Weaknesses within the IRS's computer operations could begin to adversely affect its ability to meet its mission of helping taxpayers comply with their tax responsibilities and enforcing the tax laws with integrity and fairness to all.

**What TIGTA Found**

The IRS continues to make progress in many information technology program areas. A review of systems security at the Information Sharing and Analysis Center found that the IRS and a contractor generally ensured that their actions complied with the law for sharing Federal tax information and included privacy controls to protect taxpayer information. Additional reviews found that most sampled laptops and desktops were sanitized prior to disposal, and most required baseline security controls were implemented for the Get My Payment application.

The Fiscal Year 2021 IRS Federal Information Security Modernization Act Evaluation found that three of the five Cybersecurity Framework function areas were rated as "effective." However, taxpayer data could be vulnerable to inappropriate and undetected use, modification, or disclosure until the IRS takes steps to improve its security program deficiencies and fully implement all security program components in compliance with the requirements.

Problems were also reported in the IRS's handling of the privacy of taxpayer data, access controls, system environment security, information system boundary components, network monitoring and audit logs, disaster recovery, roles and responsibilities, and separation of duties, as well as security policies, procedures, and documentation.

Reviews of systems development and information technology operations found that a roadmap was developed to include a framework to identify, classify, and group systems so that potential encryption solutions could be identified, and that the invoices provided for sampled information technology service contract payments met minimum Federal Acquisition Regulation standards. Reviews also found that the Chief Information Officer's roles and responsibilities are defined, and streamlined critical pay authority activities were compliant with the requirements of the Taxpayer First Act of 2019. Finally, the IRS deployed Release 1 of the Enterprise Case Management solution.

However, the Chief Information Officer is not notified of all significant information technology acquisitions. Problems were also reported with the IRS's information technology acquisitions, asset management, human capital, project management, risk management, implementation of corrective actions, modernizing operations, and the Coronavirus Disease 2019 response.

**What TIGTA Recommended**

Because this report was an assessment of the adequacy and security of the IRS's information technology based on previous TIGTA and Government Accountability Office reports issued during Fiscal Year 2021, TIGTA did not make any further recommendations.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

## U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

December 14, 2021

### MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

A handwritten signature in blue ink that reads "Michael E. McKenney".

**FROM:** Michael E. McKenney  
Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – Annual Assessment of the IRS’s Information  
Technology Program for Fiscal Year 2021 (Audit # 202120002)

This report presents the results of our assessment of the adequacy and security of the Internal Revenue Service’s (IRS) information technology. This review is required by the IRS Restructuring and Reform Act of 1998.<sup>1</sup> This audit was included in our Fiscal Year 2021 Annual Audit Plan and addresses the major management and performance challenges of *Responding to the COVID-19 [Coronavirus Disease 2019] Pandemic, Enhancing Security of Taxpayer Data and Protection of IRS Resources, Implementing Tax Law Changes, Modernizing IRS Operations, and Improving Tax Reporting and Payment Compliance*.

Copies of this report are also being sent to the IRS managers affected by the information in the report. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

---

<sup>1</sup> Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

# Table of Contents

<b><u>Background</u></b> .....	Page 1
<b><u>Results of Review</u></b> .....	Page 5
<u>Systems Security and Privacy of Taxpayer Data</u> .....	Page 6
<u>Systems Development and Information Technology Operations</u> .....	Page 40
<b>Appendices</b>	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u> .....	Page 73
<u>Appendix II – List of Treasury Inspector General for Tax Administration and Government Accountability Office Reports Reviewed</u> .....	Page 74
<u>Appendix III – Glossary of Terms</u> .....	Page 76
<u>Appendix IV – Abbreviations</u> .....	Page.87

## Background

The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998<sup>1</sup> requires the Treasury Inspector General for Tax Administration (TIGTA) to annually assess and report on an evaluation of the adequacy and security of the IRS's information technology.<sup>2</sup> TIGTA's Security and Information Technology Services business unit assesses the information technology of the IRS by evaluating cybersecurity, systems development, and information technology operations. This report provides our assessment for Fiscal Year 2021.

The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In Fiscal Year 2021, the IRS collected approximately \$4.1 trillion in Federal tax payments, and processed 269 million tax returns and forms. In addition, Federal tax refund and outlay activities<sup>3</sup> by the IRS were approximately \$1.1 trillion. This included approximately \$570 billion in

**The IRS collected approximately \$4.1 trillion in Federal tax payments and paid approximately \$1.1 trillion in refund and outlay activities.**

Coronavirus Disease 2019 (COVID-19) economic impact payments paid under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act);<sup>4</sup> the Coronavirus Response and Relief Supplemental Appropriations Act of 2021;<sup>5</sup> and the American Rescue Plan Act of 2021,<sup>6</sup> which included provisions to help stimulate the economy.

Further, the size and complexity of the IRS add unique operational challenges. The IRS employs approximately 81,600 people in its Washington, D.C., Headquarters and 501 offices in all 50 States and U.S. territories. The IRS relies extensively on computerized systems to support its operations in collecting taxes, processing tax returns, and enforcing Federal tax laws. As such, it is critical that its computer systems are effectively secured to protect sensitive financial and taxpayer data and are operating as intended. In addition, successful modernization of IRS systems, as well as the development and implementation of new technologies, is necessary to meet evolving business needs and to enhance the taxpayer experience.

In Fiscal Year 2021, the IRS's appropriations increased by \$409 million to \$11.9 billion, designated for taxpayer services, enforcement, operations support, and modernization. The Information Technology (IT) organization comprises a significant portion of the IRS's budget and plays a critical role to enable the IRS to carry out its mission and responsibilities. The IRS's Fiscal Year 2021 projected available funds included approximately \$4.5 billion for information technology investments, of which \$1.8 billion was received to fund recent legislative

---

<sup>1</sup> Pub. L. No. 105-206, 112 Stat. 685.

<sup>2</sup> See Appendix III for a glossary of terms.

<sup>3</sup> Federal tax refund and outlay activities include refunds of tax overpayments, payments for interest, and disbursements for refundable tax credits such as the Earned Income Tax Credit and the Additional Child Tax Credit.

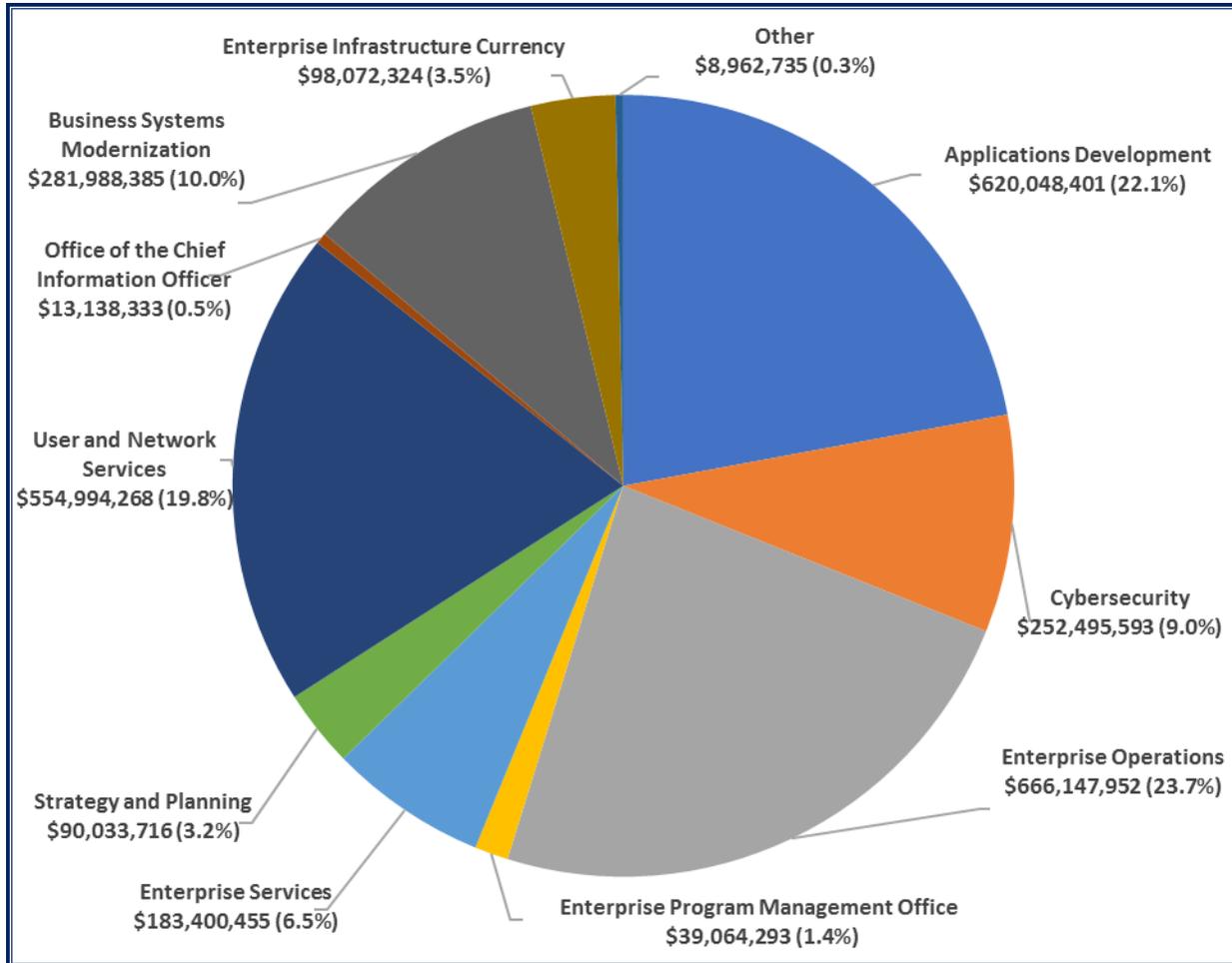
<sup>4</sup> Pub. L. No. 116-136, 134 Stat. 281.

<sup>5</sup> Pub. L. No. 116-260.

<sup>6</sup> Pub. L. No. 117-2.

requirements.<sup>7</sup> Figure 1 illustrates the IRS's Fiscal Year 2021 information technology projected available funding by IT organization function and major program.

**Figure 1: Fiscal Year 2021 Information Technology Projected Available Funding by IT Organization Function and Major Program**

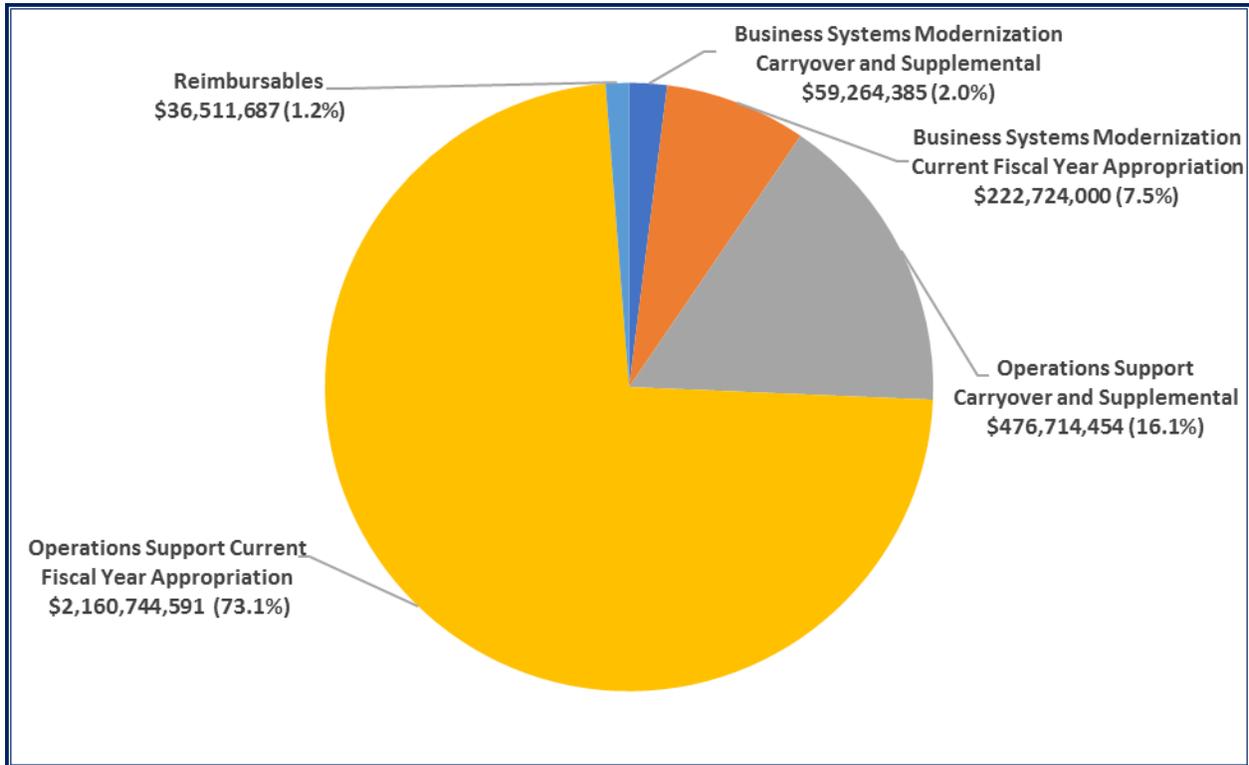


Source: IT organization budget data as of May 2021, based on information provided by the Strategy and Planning function's Office of Financial Management Services. The Other category includes Shared Support and other funds not yet distributed.

<sup>7</sup> The recent legislative requirements resulted from the American Rescue Plan Act; the CARES Act; the Families First Coronavirus Response Act; the Taxpayer First Act; and annual appropriations. Figure 3 provides further details on the funding for the recent legislative requirements.

Figure 2 shows the IT organization's actual available funding for Fiscal Year 2021 by funding source.

**Figure 2: Fiscal Year 2021 Total Actual Available Funding by Funding Source<sup>8</sup>**

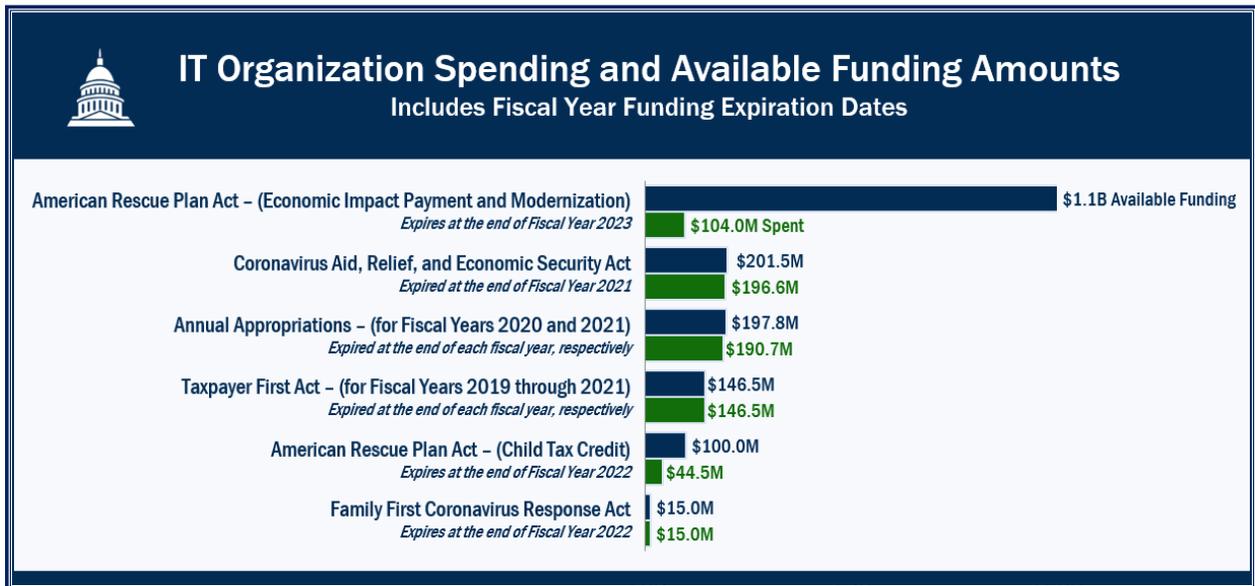


Source: IT organization budget data as of May 2021, based on information provided by the Strategy and Planning function's Office of Financial Management Services.

Figure 3 presents the IT organization's total spending and available funding, as of September 30, 2021, for recent legislative requirements by legislation.

<sup>8</sup> The percentages do not add up to 100 percent due to rounding. The difference of \$147,612,662 between Figures 1 and 2 is due to projected versus actual available funding.

**Figure 3: IT Organization Spending and Available Funding for Recent Legislative Requirements by Legislation (in Descending Available Funding Order)**



Source: IT organization budget and expense data as of September 30, 2021, based on information provided by the Office of the Chief Financial Officer's Financial Planning and Analysis office.

Figure 4 illustrates that, as of May 2021, the IRS had a total of 7,011 employees and 6,549 contractors working across eight different IT organization functions – 226 fewer employees and 436 more contractors than in Fiscal Year 2020.

**Figure 4: Number of Employees and Contractors by IT Organization Function (in Descending Employee Order)**

IT Organization Function/Office	Employees	Contractors
Applications Development	1,919	2,128
Enterprise Operations	1,905	477
User and Network Services	1,392	1,037
Enterprise Services	723	962
Cybersecurity	521	811
Strategy and Planning	311	171
Enterprise Program Management Office	228	948
Office of the Chief Information Officer	12	15
<b>Total</b>	<b>7,011</b>	<b>6,549</b>

Source: IRS Human Resources Reporting Center as of May 2021.

- The **Applications Development function** is responsible for building, unit testing, delivering, and maintaining integrated information applications to support modernized and legacy systems in production.
- The **Enterprise Operations function** facilitates information technology operational activities in the enterprise computing centers, campuses, and call sites.

- The **User and Network Services function** oversees a portfolio of technology and services that enable communication, collaboration, and business capabilities.
- The **Enterprise Services function** is responsible for strengthening the technology infrastructure across the enterprise by defining the current and target architectures, and developing a transition strategy to move towards the target environment.
- The **Cybersecurity function** ensures compliance with Federal statutory, legislative, and regulatory requirements to assure the confidentiality, integrity, and availability of electronic systems, services, and data.
- The **Strategy and Planning function** collaborates with IT organization leadership to provide policy, direction, and administration of essential programs, including strategy and capital planning; comprehensive and integrated modernization planning; strategic planning and performance measurement; financial management services; vendor and contract management; requirements and demand management; and risk management.
- The **Enterprise Program Management Office** delivers best practices in program management and leads programs to improve business processes and operations as well as the taxpayer experience.
- The **Office of the Chief Information Officer** includes the Chief Information Officer (CIO), two Deputy CIOs, and their employees. The CIO leads the IT organization and advises the IRS Commissioner. The CIO also manages all information system resources and is responsible for delivering and maintaining modernized systems. The Deputy CIO for Operations has oversight responsibility for the IT organization's planning and execution of filing season as well as the day-to-day operations of information systems and services. In addition, the Deputy CIO for Operations is focused on upgrading the IRS's infrastructure and improving service availability. The Deputy CIO for Strategy and Modernization provides executive oversight for large modernization programs in addition to providing guidance on investment planning and strategic decision-making supported by data and analysis.

## Results of Review

During this annual review, we summarize information from program efforts in cybersecurity, systems development, and information technology operations. During Fiscal Year 2021, TIGTA audits of the IRS's information technology program addressed the major management and performance challenges of *Responding to the COVID-19 Pandemic, Enhancing Security of Taxpayer Data and Protection of IRS Resources, Implementing Tax Law Changes, Modernizing IRS Operations, and Improving Tax Reporting and Payment Compliance*. This report presents a summary of TIGTA and Government Accountability Office (GAO) audit results previously reported for Fiscal Year 2021. It does not reflect any additional audit work or corrective actions that the IRS may have been taken since the initial reporting of the audit results.

Overall, the IRS needs to ensure that it continues to leverage viable technological advances as it modernizes its major business systems and improves its overall operational and security environments. While the IRS continues to make progress in many information technology areas, additional improvements are needed. Otherwise, weaknesses within the IRS's computer

operations could begin to adversely affect its ability to meet its mission of helping taxpayers comply with their tax responsibilities and enforcing the tax laws with integrity and fairness to all.

## Modernization

The reliance on legacy systems and aged hardware and software, and its use of outdated programming languages, pose significant risks to the IRS's ability to deliver its mission. Modernizing the IRS's computer systems has been a persistent challenge for many years and will likely remain a challenge for the foreseeable future. In response, the IRS developed the *IRS Integrated Modernization Business Plan*.<sup>9</sup> The plan provides a six-year roadmap for achieving the necessary modernization of IRS systems and taxpayer services in two, three-year phases that began in Fiscal Year 2019. The IRS organized the plan around four "Modernization Pillars" that are critical to its mission and future development: 1) *Taxpayer Experience*, 2) *Core Taxpayer Services and Enforcement*, 3) *Modernized IRS Operations*, and 4) *Cybersecurity and Data Protection*.

In addition, the IRS developed the *American Rescue Plan Modernization*.<sup>10</sup> According to the document, it is a portfolio of initiatives that "will transform foundational IRS technology to allow for future innovation and faster delivery of IT [information technology] capabilities, while making meaningful improvements in taxpayer service and compliance." The *American Rescue Plan Modernization* represents an evolution of the *IRS Integrated Modernization Business Plan* by accelerating existing initiatives identified to begin in Phase 2 of the *IRS Integrated Modernization Business Plan*, as well as introducing new initiatives based on emerging needs and technologies.

The *American Rescue Plan Modernization* was the result of additional funding provided to the IRS when the President signed the American Rescue Plan Act of 2021 into law. The legislation included additional funding of approximately \$1 billion available through September 30, 2023, for the continuation of integrating, modernizing, and securing information systems as well as for the Advance Child Tax Credit and a number of tax-related provisions. The additional funding will help accelerate modernization initiatives and address foundational information technology modernization that had previously been unfunded. The *American Rescue Plan Modernization* is also aligned with strategies resulting from the Taxpayer First Act of 2019 (TFA)<sup>11</sup> by continuing to provide the necessary technology foundation to reimagine the taxpayer experience. The TFA amended the Internal Revenue Code of 1986 to modernize and improve the IRS. It includes provisions related to cybersecurity and identity protection, development of information technology, expanded use of electronic systems, *etc.*

## Systems Security and Privacy of Taxpayer Data

Federal agencies are dependent on information systems and electronic data to carry out operations and to process, maintain, and report essential information. Virtually all Federal activities are supported by computer systems and electronic data. Agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without

---

<sup>9</sup> Dated April 2019.

<sup>10</sup> Dated June 16, 2021.

<sup>11</sup> Pub. L. No. 116-25.

these information technology assets. Therefore, the security of these systems and data is vital to public confidence and the Nation's safety, prosperity, and well-being. Ineffective security controls to protect these systems and data could have a significant effect on a broad array of Government operations and assets.

Without effective security controls, computer systems are vulnerable to human errors or actions committed with malicious intent. People acting with malicious intent can use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. These threats to computer systems and related critical infrastructure can come from sources that are internal or external to an organization. Internal threats include equipment failures, human errors, and fraudulent or malicious acts by employees or contractors. External threats include the ever-growing number of cyberattacks that can come from a variety of sources, such as individuals, groups, and countries that wish to do harm to an organization's systems or steal an organization's data.

In the previous 10 years, TIGTA designated *Enhancing Security of Taxpayer Data and Protection of IRS Resources* as the number one major management and performance challenge area, but it was succeeded by *Responding to the COVID-19 Pandemic* in Fiscal Year 2021. The IRS faces the daunting task of securing its computer systems against the growing threat of cyberattacks. In addition to TIGTA's annual Federal Information Security Modernization Act of 2014 (FISMA)<sup>12</sup> report that provides an overall assessment of the information security program, we performed several audits to assess the IRS's efforts to protect its information and taxpayer data. Our audits covered privacy of taxpayer data, access controls, system environment security, information system boundary components, network monitoring and audit logs, disaster recovery, roles and responsibilities, and separation of duties, as well as security policies, procedures, and documentation.

### **Overall assessment of the information security program**

The FISMA requires Federal agencies to develop, document, and implement an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by contractors. It assigns specific responsibilities to agency heads and Inspectors General in complying with the requirements of FISMA and is supported by the Office of Management and Budget, the Department of Homeland Security, agency security policy, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST) related to information security practices.

For example, the FISMA directs Federal agencies to report annually to the Director, Office of Management and Budget; the Comptroller General of the United States; and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices, as well as compliance with the FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to the Office of Management and Budget. These independent evaluations are to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General. TIGTA is responsible for oversight of the IRS while the Treasury Office of Inspector General is

---

<sup>12</sup> Pub. L. No. 113-283.

responsible for all other Department of the Treasury (hereafter referred to as the Treasury Department) bureaus.

The *Fiscal Year 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (hereafter referred to as the Inspector General FISMA Reporting Metrics),<sup>13</sup> developed as a collaborative effort among the Office of Management and Budget, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency, align with the five cybersecurity function areas in NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (hereafter referred to as the Cybersecurity Framework).<sup>14</sup> Figure 5 presents the five Cybersecurity Framework function areas and aligns each with the associated security program component(s) or reporting metric domain(s).

**Figure 5: Alignment of NIST Cybersecurity Framework Function Areas to the Fiscal Year 2021 Inspector General FISMA Reporting Metric Domains**

 IDENTIFY	 PROTECT	 DETECT	 RESPOND	 RECOVER
Develop the organizational understanding to manage cybersecurity risk to systems, assets, and capabilities.	Develop and implement the appropriate safeguards to ensure delivery of critical services.	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Fiscal Year 2021 Inspector General FISMA Reporting Metric Domains				
<ul style="list-style-type: none"> <li> Risk Management</li> <li> Supply Chain Risk Management</li> </ul>	<ul style="list-style-type: none"> <li> Configuration Management</li> <li> Identity and Access Management</li> <li> Data Protection and Privacy</li> <li> Security Training</li> </ul>	<ul style="list-style-type: none"> <li> Information Security</li> <li> Continuous Monitoring</li> </ul>	<ul style="list-style-type: none"> <li> Incident Response</li> </ul>	<ul style="list-style-type: none"> <li> Contingency Planning</li> </ul>

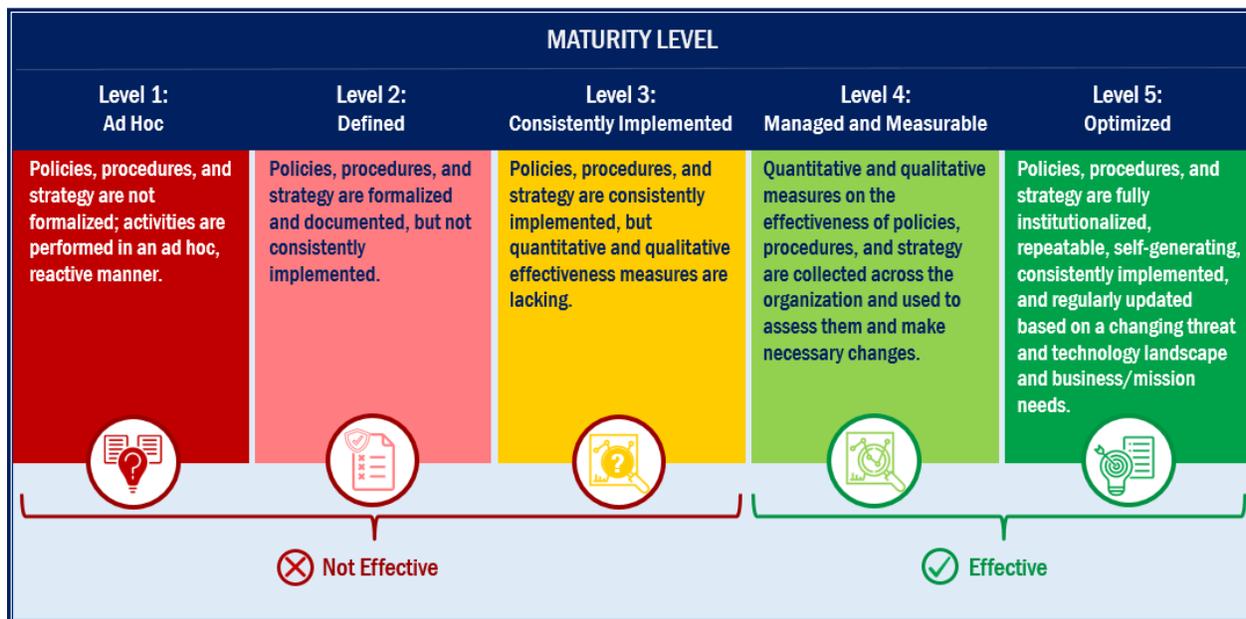
Source: *Fiscal Year 2021 Inspector General FISMA Reporting Metrics and NIST Cybersecurity Framework.*

The Inspectors General are required to assess the effectiveness of the information security programs based on a maturity model spectrum in which the reporting metric domains ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institute those policies and procedures. Maturity levels range from *Ad-Hoc* for not having formalized policies, procedures, and strategies to *Optimized* for fully institutionalizing sound policies, procedures, and strategies across the agency. Figure 6 details the five maturity levels: *Ad-Hoc*, *Defined*, *Consistently Implemented*, *Managed* and *Measurable*, and *Optimized*. The scoring methodology defines "effective" as being at a maturity level 4, *Managed and Measurable*, or above.

<sup>13</sup> Version 1.1, dated May 12, 2021.

<sup>14</sup> Version 1.1, dated April 2018.

Figure 6: Inspector General's Assessment Maturity Levels



Source: Fiscal Year 2021 Inspector General FISMA Reporting Metrics.

To determine the effectiveness of the cybersecurity program, we evaluated<sup>15</sup> the maturity level of the program metrics as specified in the Inspector General FISMA Reporting Metrics. Along with our review of pertinent documents and discussions with IRS subject matter experts, we based our evaluation on a representative subset of seven information systems and the implementation status of key security controls as well as considered the results of TIGTA and GAO audits. These audits, whose results were applicable to FISMA reporting metrics, were performed, completed, or contained recommendations that were still open during the FISMA evaluation period, July 1, 2020, to June 30, 2021. Figure 7 shows that TIGTA rated three Cybersecurity Framework function areas as “effective” and two as “not effective.”

<sup>15</sup> TIGTA, Report No. 2021-20-072, *Fiscal Year 2021 IRS Federal Information Security Modernization Act Evaluation* (Sept. 2021).

**Figure 7: Maturity Levels by Function Areas**

Overall Effectiveness of Each Function Area				
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Level 2: Defined <i>Not Effective</i>	Level 4: Managed and Measurable <i>Effective</i>	Level 2: Defined <i>Not Effective</i>	Level 4: Managed and Measurable <i>Effective</i>	Level 4: Managed and Measurable <i>Effective</i>
Assessed Maturity Levels for FY 2021 Inspector General FISMA Metric Domains				
Risk Management Level 2: Defined	Configuration Management Level 2: Defined	Information Security Continuous Monitoring Level 2: Defined	Incident Response Level 4: Managed and Measurable	Contingency Planning Level 4: Managed and Measurable
Supply Chain Risk Management <sup>1</sup> Level 1: Ad Hoc	Identity and Access Management Level 3: Consistently Implemented			
	Data Protection and Privacy Level 4: Managed and Measurable			
	Security Training Level 4: Managed and Measurable			

1 The Supply Chain Risk Management metric was not included in the overall rating for the IDENTIFY function rating.

Source: TIGTA evaluation of security program metrics that determined whether Cybersecurity Framework function areas were rated “effective” or “not effective.”

**The Cybersecurity Framework function areas of PROTECT, RESPOND and RECOVER were rated at a *Managed and Measurable* maturity level**

The Inspector General FISMA Reporting Metrics specify that, within the context of the maturity model evaluation process, maturity level 4, *Managed and Measurable*, represents an effective level of security. For the five Cybersecurity Framework function areas, we found that two function areas, RESPOND and RECOVER, and their respective security program components, Incident Response and Contingency Planning, achieved the *Managed and Measurable* maturity level 4 and were deemed as “effective.”

The PROTECT function area consists of four security program components: Configuration Management; Identity and Access Management; Data Protection and Privacy; and Security Training. We found that the performance metrics for Data Protection and Privacy, and Security Training achieved a *Managed and Measurable* maturity level 4, and we therefore considered them “effective.” However, we determined that the Identity and Access Management, and Configuration Management security program components were at a *Consistently Implemented* maturity level 3 and *Defined* maturity level 2, respectively. As such, we considered these program components “not effective.” The overall maturity level for the PROTECT function area is at a *Managed and Measurable* maturity level 4 in accordance with the Inspector General FISMA Reporting Metrics. As a result, we consider the function area “effective.”

While the PROTECT function area is at an effective level, the following examples are Configuration Management metrics that did not meet the *Managed and Measurable* maturity level 4.

- While the IRS has defined baseline configurations, it has not ensured that its information systems consistently maintain the baseline or component inventories are compliant with IRS policy.
- While the IRS has defined flaw remediation policies, including patching, it has not consistently implemented flaw remediation and patching on a timely basis.

### **The Cybersecurity Framework function areas of IDENTIFY and DETECT were rated at a *Defined* maturity level**

Based on the Inspector General FISMA Reporting Metrics, we found that the IDENTIFY and DETECT function areas and their respective security program components, Risk Management and Information Security Continuous Monitoring, met a *Defined* maturity level 2, which we considered "not effective." The following examples are metrics that did not meet the *Managed and Measurable* maturity level 4.

- Both the IRS and TIGTA have identified weaknesses in the IRS's ability to maintain a comprehensive and accurate inventory of its information systems. In addition, the IRS's FISMA system inventory and security artifact repository, the Treasury FISMA Inventory Management System, had an inaccurate inventory on cloud systems.
- The IRS has not implemented the Continuous Diagnostics and Mitigation, Phase 1, scanning tool necessary to perform checks for unauthorized hardware components/devices and software and to notify appropriate organizational officials. In addition, the IRS has open plans of action and milestones in a number of systems due to inaccurate hardware/software component inventories.
- The IRS has developed the *Information Security Continuous Monitoring* strategy, but it has not fully developed tools that support an accurate inventory.

Until the IRS takes steps to improve its security program deficiencies and fully implement all security program components in compliance with FISMA requirements, taxpayer data could be vulnerable to inappropriate and undetected use, modification, or disclosure.

### **Privacy of taxpayer data**

The trillions of dollars that flow through the IRS each year make it an attractive target for criminals who want to exploit the tax system in various ways for personal gain. The proliferation of stolen Personally Identifiable Information poses a significant threat to tax administration by making it difficult for the IRS to distinguish legitimate taxpayers from fraudsters. Tax-related scams, and the methods used to perpetrate them, are continually changing and require constant monitoring by the IRS. The IRS's ability to continuously monitor and improve its approach to taxpayer authentication is a critical step in defending the agency against evolving cyberthreats and fraud schemes and in protecting trillions of taxpayer dollars.

During Fiscal Year 2021, TIGTA performed four audits involving privacy of taxpayer data. We initiated an audit<sup>16</sup> to *evaluate IRS controls to validate transcript requests and implement TFA sections for the Income Verification Express Service (IVES) Program*. The IVES Program allows third-party participants, such as banks and financial institutions, to submit requests through the Transcript Delivery System, on behalf of clients, to obtain their tax transcripts. The transcripts cannot be obtained unless the third party successfully registers for e-Services and participates in electronic tax return filing or is a participant of the IVES Program. Once accepted, participants can submit an authorization Form 4506-T, *Request for Transcript of Tax Return*, to obtain tax transcripts for their clients. The TFA<sup>17</sup> requires that the IRS modernize the IVES Program and increase taxpayer protections, *e.g.*, develop an automated system to receive third-party income verification forms and comply with applicable security standards and guidelines.

Although the IVES Program can accept a taxpayer's electronic signature, the IRS cannot authenticate that the legitimate taxpayer electronically signed the Form 4506-T. As such, until the IRS deploys its online IVES Program transcript request system, it has no assurance that the legitimate taxpayer authorized release of their tax transcript. In the interim, the IRS relies on its current control that requires participants to undergo an independent audit of their electronic signature process and provide the IVES Program with an audit report by January 31 each year. However, IRS management does not ensure that IVES Program participants undergo the required independent audit. Our discussion with IVES Program management identified that processes have not been established to identify which participants are submitting electronically signed Forms 4506-T. As a result, management does not know which participants are required to provide an independent audit report of their electronic signature process. As of August 14, 2020, the IVES Program had 748 participants, but received an independent audit report from only five participants by January 31, 2020.

To participate in the electronic signature process, IVES Program participants must validate that signers are who they say they are, obtain consent from the signer to receive and sign documents electronically, and ensure that the electronic signature establishes a person's intent to sign the Form 4506-T. After the electronic signature is collected, the document must be made tamper proof to ensure its validity, and an audit log of the electronic signing must be retained by the IVES Program participant for two years.

On February 28, 2020, we issued an e-mail alert recommending that the IVES Program immediately require all participants inform the IRS whether they are submitting electronically signed Forms 4506-T and acknowledge their agreement to provide the independent audit report of their electronic signature process. On March 23, 2020, the IRS notified all IVES Program participants that they must certify whether they are submitting electronically signed transcript requests and, if so, provide the required audit report by April 30, 2020, subsequently postponed until August 7, 2020.

---

<sup>16</sup> TIGTA, Report No. 2021-45-017, *Additional Security Processes Are Needed to Prevent Unauthorized Release of Tax Information Through the Income Verification Express Service Program* (Feb. 2021).

<sup>17</sup> TFA § 2201, *Disclosure of Taxpayer Information for Third-Party Income Verification*; § 2202, *Limit Redislosures and Uses of Consent-Based Disclosures of Tax Return Information*; § 2302, *Uniform Standards for the Use of Electronic Signatures for Disclosure Authorizations to, and Other Authorizations of, Practitioners*; and § 2304, *Authentication of Users of Electronic Services Accounts*.

However, as of July 31, 2020, a majority of IVES Program participants did not respond to the IRS's March 23, 2020, mandate. Only 206 IVES Program participants responded to the request to certify whether they are submitting electronically signed Forms 4506-T. In addition, of the 53 participants who responded that they were using electronic signatures, 38 (72 percent) did not provide the required audit report. Only 15 participants submitted an audit report. The IVES Program's notice to participants stated that failure to submit the certification and independent audit report would result in suspension and potential removal from the program. However, as of September 9, 2020, management had not taken these actions.

In addition, independent audit reports submitted by participants did not address the IVES Program's electronic signature requirements. Our review of the 15 audit reports submitted identified that 10 (67 percent) did not address all key electronic signature requirements of the IVES Program. For example: six audit reports did not make Form 4506-T tamper proof to ensure its validity after the electronic signature was obtained; 10 audit reports did not address the requirement to retain all audit logs and transcript requests submitted to the IRS for two years; and two audit reports were not prepared by an independent party.

Also, transcript requests were processed erroneously for taxpayer accounts that contained identity theft markers. We identified 8,754 tax transcripts that the IVES Program improperly issued for 4,726 taxpayers during Processing Year 2019. Internal guidelines state that a transcript should not be provided if the taxpayer's account has an identity theft marker. IVES Program employees use an Integrated Automation Technologies tool to process Forms 4506-T. The tool automates research of the taxpayer's account for which the request was submitted and alerts the employee to reject the request if certain identity theft markers are on the account.

Our analysis of the 8,754 improperly issued transcripts found the following reasons for the errors:

- 5,207 (59 percent) improperly issued transcripts occurred because the Integrated Automation Technologies tool did not identify an identity theft marker on the taxpayer's account for a tax year other than the tax year on the Form 4506-T. This resulted from the Integrated Automation Technologies tool programming not notifying the clerk to reject the transcript request due to the presence of the identity theft marker on another tax year.
- 3,547 (41 percent) improperly issued transcripts occurred because some clerks did not follow procedures to reject requests when the Integrated Automation Technologies tool reported that an identity theft marker is on the taxpayer's account.

On June 10, 2020, we alerted IVES management to our concerns. In response, management noted that they are working with the Identity Protection Office and an Integrated Automation Technologies Team to correct the tool's programming. To address those transcripts improperly issued as a result of clerk error, management issued an alert to all Tax Processing Centers on June 26, 2020, reminding employees that all tax years requested on Form 4506-T must be researched to ensure that requests are rejected when accounts with an identity theft marker are identified.

In addition, we initiated an audit<sup>18</sup> to *determine whether policies, procedures, and controls have been effectively implemented to ensure that disclosed return information is protected as required at the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC)*. We found that the memorandum of understanding for sharing Federal tax information (FTI) between the IRS and the ISAC complied with TFA § 2003, *Information Sharing and Analysis Center*. The creation of the ISAC was a result of a Security Summit initiative to share refund schemes. According to the IRS, it is a [REDACTED] operated by the [REDACTED] (hereafter referred to as the trusted third party (TTP)) to detect, deter, and prevent tax-related identity theft. The Security Summit is composed of IRS officials with representatives from the State Departments of Revenue, the Chief Executive Officers of leading tax preparation firms, and software developers, as well as payroll and tax financial product processors.

The TFA gave the IRS authority to disclose certain return information for the purposes of cybersecurity and the prevention of identity theft tax refund fraud. It includes provisions that specify the return information that can be disclosed, restrictions on the use of the disclosed information, and data protections and safeguards.<sup>19</sup> Specifically, we identified 26 stipulations in the TFA. In 21 of the stipulations, there were little to no differences between the TFA and the memorandum of understanding. The stipulations included 12 related to specifying the return information that can be disclosed, seven related to restrictions on the use of the disclosed information, and two related to data protections and safeguards. The remaining five stipulations were not included in the memorandum of understanding because they were applicable to only the IRS and not the TTP. These included four relevant to return information that can be disclosed and one to data protection and safeguards.

We also reviewed the memorandum of understanding between the IRS and each of the 14 industry partners permitted to receive FTI for compliance with the law.<sup>20</sup> We identified similar compliance with 20 of the 26 stipulations. The remaining six stipulations were not applicable because industry partners included specifying return information that could be disclosed, and the IRS does not disclose return information directly to them. Instead, it is obtained from the TTP.

In addition, privacy controls included conducting an annual contractor site security assessment, having TTP employees take privacy awareness training, and having a privacy notification for users who access FTI on the ISAC Participant Area landing page. We observed the security assessment conducted in February 2020 and noted repeat issues for which we obtained an approved risk-based decision document and a flaw remediation issue for which the IRS provided a valid explanation. We also noted that the Cybersecurity function team's assessment of the privacy awareness training showed that the TTP met the requirement and that the contracting

---

<sup>18</sup> TIGTA, Report No. 2021-25-025, *Taxpayer First Act: Data Security in the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center* (May 2021).

<sup>19</sup> Specifically, TFA § 2003 provides that the Secretary of the Treasury (hereafter referred to as the Secretary) *may disclose specified return information to designated ISAC Participants to the extent that the Secretary determines such disclosure is in furtherance of effective Federal tax administration relating to the detection or prevention of identity theft tax refund fraud, validation of taxpayer identity, authentication of taxpayer returns, or detection or prevention of cybersecurity threats*.

<sup>20</sup> The States are governed under 26 U.S.C. § 6103(d), *Disclosure to State tax officials and State and local law enforcement agencies*, regarding the sharing of FTI and do not require a separate memorandum of understanding.

officer representative provided written documentation certifying that TTP employees completed the training. Further, the privacy notification included a warning that the system is for authorized use and the consequences, which included disciplinary, civil, and criminal actions, for unauthorized and improper use. The notification also warned that users should have no reasonable expectation of privacy regarding any communication, data transfers, or information stored on the system.

The IRS disclosed specified return information in accordance with the TFA. Our analysis of the April 24, 2020, [REDACTED] identity theft refund fraud file, the June 2020 [REDACTED] confirmed identity theft refund fraud file, and the Calendar Year 2019 [REDACTED] identity theft refund fraud file determined that the data fields shared with the ISAC contained only the specified data elements as outlined in the TFA.

In addition, the TTP securely received and stored FTI and monitored its use. Specifically, the TTP took measures to ensure the separation of FTI and non-FTI. [REDACTED]

[REDACTED]. We verified that the TTP maintains FTI on [REDACTED] by comparing a list of the files that we received from the IRS to the designated ISAC accounts. The stored and transmitted FTI also includes appropriate encryption to protect against unauthorized access and viewing. In addition, the TTP monitors ISAC activities by performing weekly automated and monthly manual reviews to ensure that only authorized users have accessed the ISAC.

Moreover, disclosure and redisclosure of FTI were properly captured and provided to the IRS. Transmitting FTI to the TTP is considered a permitted disclosure. [REDACTED]

[REDACTED] it is considered a redisclosure, which the memorandum of understanding between the IRS and the TTP permits. We also verified that the TTP is providing the IRS with a monthly accounting of the redisclosures. The TTP reported more [REDACTED]

Further, two-factor authentication is used to identify and authenticate individuals who access FTI. Two-factor authentication requires the use of something a user knows, *e.g.*, password, and something a user possesses, *e.g.*, token card, to access the contractor's system. We reviewed the latest updated version of the ISAC System Security Plan and found no security issues with the use of the two-factor authentication. We also confirmed that the TTP is using two-factor authentication when we independently accessed the ISAC portal.

We also initiated an audit<sup>22</sup> to *independently evaluate the performance of private collection agencies*. A direct debit payment option has been implemented for taxpayers working with private collection agencies, but protecting taxpayer information is a concern. In January 2020, members of Congress expressed concerns about the new preauthorized direct debit process being used by the private collection agencies because it requires taxpayers to disclose their bank account information, which is then used by the private collection agencies to draft the

---

<sup>21</sup> In [REDACTED] the IRS began sharing FTI with the TTP, one month after signing the memorandum of understanding with the TTP.

<sup>22</sup> TIGTA, Report No. 2021-30-010, *Fiscal Year 2021 Biannual Independent Assessment of Private Collection Agency Performance* (Dec. 2020).

preauthorized check made payable to the Treasury Department.<sup>23</sup> The concern was related to the potential fraudulent handling of a taxpayer's bank information by the private collection agencies and the fact that the Federal Trade Commission had previously banned telemarketing companies from using this direct debit paper check process.

The IRS responded to congressional concerns stating that it requires the private collection agencies to handle and protect all taxpayer information following the security guidelines detailed in Publication 4812, *Contractor Security & Privacy Controls*.<sup>24</sup> The IRS conducts contractor security assessments annually to ensure compliance with these guidelines and could terminate the contract if it finds a private collection agency to be noncompliant. In addition, the IRS stated that its oversight of the Private Debt Collection Program mitigates potential risks to taxpayers and includes measures to prevent potential violations of taxpayer rights or related identity theft. The IRS also stated that it holds the private collection agencies to the same standards as it holds itself, and any willful disclosure of taxpayer information could result in criminal and civil actions against the private collection agency employee.

After the IRS responded to the congressional inquiries, we requested from each private collection agency its process for handling preauthorized direct debit cases to make sure taxpayer information was safely secured during the process. We identified a concern with the controls for handling the verbal consent after a taxpayer acknowledges interest in the preauthorized direct debit. For example, one of the four private collection agencies selected for review discusses bank account information with the taxpayer during the verbal consent stage, stating that an assistor obtains the information and a senior collection specialist or management official verifies that the information is correct and obtains the verbal consent from the taxpayer.

However, Policy and Procedure Guide § 9.1, *Pre-Authorized Direct Debit*,<sup>25</sup> does not state that the private collection agencies should discuss or obtain bank account information from the taxpayer during the verbal consent stage, but rather should explain to the taxpayer that they must complete the bank and contact information on the written authorization form, sign, and return it to the private collection agency by mail or fax. The remaining three private collection agencies responded that bank account information is not requested during the verbal consent stage. After a signed preauthorized direct debit form is returned, each of the private collection agencies have designated employees responsible for inputting bank and routing account information. After input of the information, all four of the private collection agencies mask the data, which prohibits employees from accessing the full account information.

Further, we initiated an audit<sup>26</sup> to ***assess the effectiveness of the IT organization's hardware asset sanitization process***. The User and Network Services (UNS) function manages the Memphis Sanitization Site (MSS), which is responsible for receiving IRS end-user laptops, desktops, and smartphones for sanitization,<sup>27</sup> properly sanitizing them, and transferring them to the Facilities Management and Security Services function for disposal.

---

<sup>23</sup> January 8, 2020, letter from Senators Elizabeth Warren and Sherrod Brown to IRS Commissioner Charles Rettig.

<sup>24</sup> Revised October 2019. The Publication is designed to identify security requirements for contractors and any subcontractors supporting the primary contract.

<sup>25</sup> Dated August 30, 2019.

<sup>26</sup> TIGTA, Report No. 2021-20-056, *Laptop and Desktop Sanitization Practices Need Improvement* (Sept. 2021).

<sup>27</sup> A process that renders access to target data on the hardware asset unrecoverable.

In January 2016, the Associate CIO, UNS, issued a memorandum that mandated UNS function personnel refrain from sanitizing the data from any hard disk associated with an end-user. This applied to all end-user computers and smartphones, including those belonging to separating employees. In addition, personnel were instructed that hard disks were to remain intact with their respective computers. In July 2019, the Associate CIO, UNS, issued a memorandum lifting the sanitization moratorium, advising UNS function personnel that, effective August 5, 2019, they were to resume information technology equipment wiping and disposal operations. As of October 2020, the MSS had 61,809 unsanitized computers (28,370 laptops and 33,439 desktops) and 7,996 unsanitized smartphones.

The laptops and desktops were sanitized using an unapproved sanitization product. The UNS function was unable to provide sufficient evidence that the sanitization tool being used is properly approved by the Federal Government. The UNS function only provided:

- 1) A statement from the vendor's website that its product conformed to 1995 Department of Defense standards.
- 2) Internal guidance from a decade ago that stated, "The purging process is the removal of sensitive but unclassified data from computer media by using the approved [product name] overwriting process or degaussing the media."
- 3) A screenshot from the IRS's Enterprise Standards Profile mentioning that the sanitization software was an IRS-approved product.

We reviewed the list of sanitization software that the Common Criteria Recognition Arrangement<sup>28</sup> has certified using the Common Criteria for Information Technology Security Evaluation.<sup>29</sup> The Common Criteria Recognition Arrangement is comprised of 31 government agencies representing their respective member countries, with the Department of Defense representing the United States. While the Common Criteria Recognition Arrangement certified at least four sanitization software products between November 2017 and August 2020, the product that the UNS function is using is not on the list of certified products. Once certified, the products remain on the Certified Products List for five years.

In addition, the IRS has not tested the MSS's sanitization equipment and procedures to verify that the intended sanitization is being achieved, as required. Without using a currently approved sanitization product and annually testing the sanitization equipment and procedures, the risk exists that the sanitization product could fail to remove residual information from laptop and desktop hard disks. If not sanitized properly, release of the hard disks outside of the IRS could lead to unauthorized disclosure of confidential taxpayer information.

**Management Action:** In June 2021, UNS function management stated that they acquired and are now using a National Security Agency–approved degausser to purge data on hard disks at the MSS for laptops and desktops that will be disposed of outside of the IRS. If calibrated correctly, we believe that the degausser will effectively ensure complete erasure of the hard disks. For the remaining computers that the UNS function expects to reuse within the IRS, UNS function management is working to identify and implement a sanitization software

---

<sup>28</sup> It is composed of each signatory's country representatives, in which member countries recognize the products certified by the arrangement.

<sup>29</sup> An international standard (ISO/IEC 15408) for evaluating and certifying information security products.

solution. The UNS function is also in the process of acquiring a Solid State Drive Disintegrator, which is designed specifically for the destruction of solid state hard drives.

In addition, most sampled laptops and desktops were sanitized. To test the effectiveness of the computer sanitization process, we selected and tested a random statistical sample<sup>30</sup> of sanitized laptops and desktops to determine whether residual data remained on the computers' hard disks. Specifically, we randomly selected a statistical interval sample of 87 (2.24 percent) computers from a population of 3,882 computers that the MSS sanitized between January and March 2021. We used sanitization verification software from a different vendor to independently test if the sanitization was effective. Results of our sanitization verification testing include:

- 1 hard disk was not sanitized but encrypted.
- 2 hard disks were missing.
- 6 hard disks had "error accessing drive sectors" messages.
- 78 hard disks were effectively sanitized.

For the one unsanitized computer, we observed that the hard disk was encrypted. If encryption is properly enabled, the risk of inadvertent disclosure of confidential information is significantly reduced even if the hard disk was not sanitized. At our request, the IRS tried to locate the two computers with missing hard disks, but it ultimately was unable to do so. As a result, we were unable to test these two hard disks to determine if they had been sanitized and if the sanitization process was effective. Projecting our sample results to the total population of computers the MSS sanitized between January and March 2021, we estimate that 45 (1.16 percent)<sup>31</sup> of the 3,882 sanitized computers may not have been properly sanitized. Further, we estimate that 89 (2.30 percent)<sup>32</sup> of the 3,882 computers may have been missing hard disks that were not identified in the MSS's hardware asset inventory.

For the remaining six computers with bad sector error messages, we used a different vendor's data recovery software to retest the hard disks for the existence of residual data. Although our additional testing did not identify any residual data, NIST Special Publication 800-88, *Guidelines for Media Sanitization*,<sup>33</sup> states that overwriting cannot be used for media that are damaged or not rewriteable. However, degaussing or destruction are acceptable methods to purge damaged media containing sensitive information.

In addition to testing sanitized computers, we reviewed the process the IRS uses to wipe smartphones. MSS personnel enter an incorrect password several times to initiate the wipe. We

---

<sup>30</sup> Because the population of sanitized devices was constantly changing due to new assets being received and stockpiled assets being sanitized, we used interval attribute sampling, a form of random sampling that allowed for the selection of sample items from the sanitized population of devices as the sanitization occurred during our audit work.

<sup>31</sup> We selected this sample using a 95 percent confidence interval, 3 percent error rate, and  $\pm 3$  percent desired precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total number of unsanitized computers is between two and 239.

<sup>32</sup> We selected this sample using a 95 percent confidence interval, 3 percent error rate, and  $\pm 3$  percent desired precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total number of missing hard disks is between 12 and 310.

<sup>33</sup> Revision 1, dated December 2014.

observed this wiping process and also tested a judgmental sample<sup>34</sup> of eight smartphones and determined that the MSS had effectively sanitized them. To verify the success of the wipes, we observed that the smartphones booted up to the initial setup screens.

We also found that the process to independently verify the sanitization of laptops and desktops is ineffective. After computers are sanitized, the MSS transfers them to the Facilities Management and Security Services function for disposal. At the time of transfer, MSS and Facilities Management and Security Services function personnel together visually compare the description of the computers listed on the Standard Form 120, *Report of Excess Personal Property*, to the bar codes on the pallets of sanitized laptops and desktops. In addition, MSS personnel complete and sign an *Asset Sanitization Certification Form* to document that the MSS sanitized the computers prior to physical custody of the assets being transferred to the Facilities Management and Security Services function.<sup>35</sup>

The UNS function's asset sanitization certification process includes procedures for UNS function personnel to document the independent verification that each individual computer was effectively sanitized. While UNS function management stated that an individual conducting the verification process should boot up the computer to a command level prompt to demonstrate that the computer was sanitized, we did not see this procedure documented in the draft *MSS Standard Operating Procedures* or observe it being performed. Further, the UNS function's verification procedures for computers do not include an effective test of each computer using a verification software tool to verify that the sanitization was effective and that residual data cannot be read. NIST Special Publication 800-88 suggests that the verification process should be performed using a different verification software tool, that is, not simply booting up the computer or reusing the original sanitization tool to perform the verification.

UNS function management believed that the MSS met the intent of the sanitization verification guidance through 1) performing the visual inspection of the computers on the sanitized pallets and 2) having a person independent of the sanitization process boot up the computers to a command prompt. However, if the MSS had performed actual verification testing of its sanitized computers using a verification software tool, missing hard disks and hard disks with residual data or bad sector errors would have been identified.<sup>36</sup>

Because the MSS verification process is ineffective, the UNS function cannot ensure that residual taxpayer data or Personally Identifiable Information does not remain on those items disposed outside of the IRS. If an unauthorized disclosure of tax or Personally Identifiable Information occurred, it could result in substantial harm, embarrassment, and loss of public confidence in the IRS. An unauthorized disclosure could also harm an individual.

---

<sup>34</sup> A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

<sup>35</sup> The same process occurs for smartphones, but the visual examination compares the description of smartphones listed on the Form MI, *Miscellaneous Disposal*, to the bar codes of the smartphones in the boxes of sanitized smartphones. MSS personnel then complete and sign an *Asset Sanitization Certification Form*.

<sup>36</sup> Similar to a sanitized hard disk, bad sector errors can cause computer hard disks to not boot up properly. Without using a verification software tool, sanitized hard disks or ones with bad sector errors potentially containing taxpayer data would be indistinguishable.

## Access controls

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. This is accomplished by designing and implementing controls to prevent and limit unauthorized access to programs, data, facilities, and other computing resources. Access controls include both physical and system security access controls, *i.e.*, authentication and identity proofing, access management, and cryptography.

### Physical security access controls

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

In Fiscal Year 2021, TIGTA performed an audit involving physical security. We initiated this audit<sup>37</sup> to ***determine whether Criminal Investigation is implementing effective security controls over digital evidence and the e-Crimes labs.*** As part of our review, we tested six physical security and environmental controls, including automated fire suppression systems, stand-alone fire extinguishers, monthly extinguisher inspections, Limited Area designations, electronic cipher locks,<sup>38</sup> and cipher lock combination changes, at [REDACTED] e-Crimes labs. In total, we found nine physical security and environmental control weaknesses. Specifically, [REDACTED] sites were not having fire extinguishers inspected on a monthly basis, [REDACTED] sites did not have signs designating them as Limited Areas, [REDACTED] sites were not secured by electronic cipher locks with audit capability, and [REDACTED] sites were not changing the cipher lock combinations. [REDACTED]

### System security access controls

System security access controls is a policy that is uniformly enforced across all subjects and objects within the boundary of an information system. The access management process is responsible for allowing users to make use of information technology services, data, or other assets. Access management helps to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify them. Access management implements the policies of information security management.

### Authentication and identity proofing

Identification is the process of distinguishing one user from others as a prerequisite for granting access to resources in an information system. User identification is important because it is the means by which specific access privileges are assigned and recognized by the computer. However, the confidentiality of a user identification is typically not protected. For this reason, other means of authenticating users using knowledge-based information, *e.g.*, credit or tax return information, are typically implemented. Similarly, identity proofing is the process of verifying that a person who is attempting to interact with an organization, such as a Federal

---

<sup>37</sup> TIGTA, Report No. 2021-20-003, *Security Controls Over Electronic Crimes Labs Need Improvement* (Dec. 2020).

<sup>38</sup> A lock, opened with a programmable keypad, used to limit and control access to a highly sensitive area.

agency or a business, is the individual they claim to be. When remote identity proofing is used, there is no way to confirm an individual's identity through their physical presence. Instead, the individual provides information electronically or performs other electronically verifiable actions that demonstrate their identity. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators, *e.g.*, something an individual possesses and controls, such as a password, that is used to authenticate their identity.

In Fiscal Year 2021, TIGTA and the GAO performed three audits covering authentication and identity proofing. We initiated an audit<sup>39</sup> to ***review the effectiveness of IRS systems security and operations related to the CARES Act economic impact payment processing.*** Signed into law on March 27, 2020, the CARES Act is one of the largest economic rescue packages in U.S. history and will have a significant impact on the IRS and Federal tax administration.

On April 15, 2020, the IRS launched the Get My Payment application, a web-based tool that provides taxpayers with the ability to check the status of their economic impact payments and submit missing bank information for their accounts. The application is part of the Integrated Customer Communications Environment, which is comprised of numerous web and telephone applications. The functionality of these automated self-service applications supports the IRS mission by providing taxpayers with a variety of services, such as the ability to check tax refund status and establish payment agreements.

The IRS is required to perform a risk assessment on its web-based applications. The Digital Identity Acceptance Statement<sup>40</sup> must include the assessed and implemented assurance levels, rationale if the implemented assurance levels differ from the assessed assurance levels, comparability demonstration of compensating controls, and rationale if federated entities are not accepted. We reviewed the Digital Identity Acceptance Statement and all related documents for the Get My Payment application and found that the Digital Identity Acceptance Statement met both Federal and agency security requirements for the application. Although the IRS assessed the Get My Payment application's appropriate identity and authenticator assurance levels at Level 2, the IRS implemented the application's assurance levels at the less restrictive Level 1. The NIST defines the components of Level 1 and Level 2 identity assurance and authenticator assurance as follows:

- **Identity Assurance:** For Level 1, there is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such. For Level 2, evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. Level 2 also introduces the need for either remote or physically present identity proofing.
- **Authenticator Assurance:** For Level 1, it provides some assurance that the claimant controls an authenticator bound to the subscriber's account and requires either single-factor or multifactor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol. For Level 2, it

---

<sup>39</sup> TIGTA, Report No. 2021-26-006, *Systems Processing Economic Impact Payments Performed Well and the Get My Payment Application Security Vulnerabilities Are Being Remediated* (Dec. 2020).

<sup>40</sup> It documents a Federal agency's risk assessment; selected individual assurance levels for identity proofing, authentication, and federation (if applicable); and processes and technologies employed to meet each assurance level.

provides high confidence that the claimant controls authenticators bound to the subscriber's account and requires proof of possession and control of two distinct authentication factors through secure authentication protocols. Approved cryptographic techniques are required at Level 2 and above.

Although the IRS implemented identity and authenticator assurance levels that were below the assessed level, we found the Digital Identity Acceptance Statement met NIST and agency requirements by including a detailed implementation and rationale, compensating controls and risk mitigation factors, a description of risk acceptance, and a plan of action. Examples of the compensating controls and risk mitigation factors included masking taxpayer bank account information except for the last four digits, limiting the number of daily attempts per Social Security Number, and sending audit records to the Cybersecurity function's Cyber Fraud Analytics and Monitoring team for review and detection of potential fraudulent activity.

IRS officials reported that there were no confirmed cases of fraud in the Get My Payment application associated with users' bank account information. In addition, due to the identification of potential high-risk transactions, the Cyber Fraud Analytics and Monitoring team recommended that 159,739 economic impact payments be transitioned from direct deposit to paper check delivery. By ensuring that the application complies with all applicable NIST and agency security requirements related to digital identity services, the IRS properly implemented compensating controls to mitigate the risks from using inappropriate authentication controls, which could allow unauthorized access and activities, compromised taxpayer records, and lost revenue due to identity theft refund fraud.

We also initiated an audit<sup>41</sup> to ***determine whether the Endpoint Detection and Response (EDR) capability is effective to detect and provide information for the removal of any malicious activity deployed on or originating from endpoint devices, e.g., laptops, desktops, and other applicable devices.*** According to the IRS, it implemented the EDR solution to obtain a more complete picture of security incidents that occur on the IRS network by monitoring and obtaining detailed records of an incident from the affected workstation(s), which allows the IRS to conduct root cause analysis of identified threats. In addition, the Cybersecurity function determined that EDR solutions provide better detection and mitigation around advanced persistent threats through the analysis of indicators of compromise in real time.

However, Homeland Security Presidential Directive-12 credentials have not been implemented for access to the EDR solution. The credentials are required for all system accesses, privileged and nonprivileged. Homeland Security Presidential Directive-12 is designed to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Passwords are to be used (temporarily) only when the Public Key Infrastructure-based authentication via the Homeland Security Presidential Directive-12 credential is not capable. Specifically, the Public Key Infrastructure-based authentication via the Homeland Security Presidential Directive-12 credential had not been implemented for the EDR solution. A new release of the EDR solution had been implemented in May 2020, in which efforts toward meeting the directive were being reviewed. [REDACTED]

[REDACTED], which will also meet the requirements of

---

<sup>41</sup> TIGTA, Report No. 2021-20-065, *The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating As Intended, but Improvements Are Needed* (Sept. 2021).

the directive and will hopefully allow for more configuration granularity than what has been tested previously. A Cybersecurity function official stated that they are working toward a solution that they believe should be in place well before the end of Fiscal Year 2021. Until the IRS deploys Homeland Security Presidential Directive-12 credential access to the EDR solution, it cannot take advantage of two-factor authentication and enhanced protection for accessing the EDR solution.

The GAO initiated an audit<sup>42</sup> to ***evaluate the IRS's internal control over financial reporting and to determine the status of the agency's corrective actions as well as to address recommendations in prior years' reports for which actions were not complete as of September 30, 2019.*** The GAO reported that it found two deficiencies related to authentication and identity proofing. The IRS did not remove certain accounts in accordance with agency policy and did not consistently record the correct access revoke date for certain users to a system environment that processes taxpayer data.

### Access management

System access controls is a policy that is uniformly enforced across all subjects and objects within the boundary of an information system. The access management process is responsible for allowing users to make use of information technology services, data, or other assets. Access management helps to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify them. Access management implements the policies of information security management.

In Fiscal Year 2021, TIGTA performed three audits on access management. We initiated an audit<sup>43</sup> to ***determine the effectiveness of the [REDACTED] Platform's system security and operations.*** The [REDACTED] Platform provides the infrastructure that supports tax administration, including responsibilities associated with key provisions of the Patient Protection and Affordable Care Act legislation.<sup>44</sup> Operating systems of the [REDACTED] Platform include [REDACTED] and [REDACTED].

Some access controls are in place. We judgmentally sampled 30 servers running the [REDACTED] operating system and reviewed all user account information on each server. We verified that each of the 30 sampled servers had only one account with root-level access. The Internal Revenue Manual states that in the [REDACTED] operating system, the root account shall be implemented and used by the least number of staff possible without degrading system availability. In addition, we determined that of the over one million access log entries generated in January and February 2021, the IRS properly tracked modifications when users executed commands as a root user.

However, the [REDACTED] system recertification process for users and group owners needs improvement. We reviewed the [REDACTED] system reports of all [REDACTED] Platform's groups and found 21 unique groups, managed by 13 owners. [REDACTED]

---

<sup>42</sup> GAO, GAO-21-401R, *Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls* (May 4, 2021).

<sup>43</sup> TIGTA, Report No. 2021-20-063, [REDACTED] *Platform Management Needs Improvement* (Sept. 2021).

<sup>44</sup> Pub. L. No. 111-148, 124 Stat. 119 (2010).

[REDACTED]

We also selected a judgmental sample of 21 users, one user from every group, to evaluate access recertification. We received user recertification reports for all 21 users as of March 2021.

[REDACTED]

In addition, inactive users within the [REDACTED] tool retain privileges. The tool is a commercial off-the-shelf product that the IRS uses as an enterprise-wide solution for password management. We completed a detailed assessment of 272 users with access to the [REDACTED] Platform via the tool. The [REDACTED] tool history report from February 2021 indicated that [REDACTED]. The Internal Revenue Manual states that accounts that are inactive for a period of 60 and 365 days shall be disabled and removed, respectively. [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

The IRS lacks a process to review access to the [REDACTED]. As a result, these [REDACTED]

In our audit of the *Criminal Investigation e-Crimes labs*, we found that [REDACTED]

In addition, [REDACTED]

In our audit of the *EDR solution*, we found that EDR system administrator accounts were not timely disabled due to inactivity. Administrator accounts provide users with the authorization to override, or bypass, certain security restraints, and may include permissions to perform such actions as shutting down systems. In March 2021, [REDACTED]

[REDACTED]. The two accounts should have been disabled from logging in. We believe that poorly managed system administrator accounts leave organizations exposed to security breaches, such as accidental harm and malicious activity.

Also, there was no documented evidence that EDR system default passwords were timely changed. Factory default software configuration for embedded systems, devices, and appliances often include simple, publicly documented passwords. Default passwords for EDR solution appliances may not have been changed before or immediately after the solution was placed into production beginning May 7, 2020. During our review, we found the passwords for nine system administrator local accounts were last changed on December 1, 2020. Further interviews with a Cybersecurity official revealed that the nine local system accounts in question did not have their default password reset by the Cybersecurity EDR team after the installation of the appliances; however, they were disabled from being logged into as suggested by the vendor in June 2019 during the initial configuration set-up and when they had not yet started pulling the event logs into [REDACTED]. However, the official was unable to get the exact date and did not have documentation for when the passwords were disabled. Allowing default passwords and not disabling access to accounts unnecessarily exposes the EDR solution to unauthorized access, which may result in damage or data loss.

### Cryptography

Cryptography, *i.e.*, encryption, involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted or stored without unauthorized entities decoding it back into a readable format. The information cannot be read without a key to decrypt it.

In Fiscal Year 2021, TIGTA and the GAO each performed an audit covering cryptography. In our audit of the *CARES Act economic impact payment processing*, our review of the January 2020 scan report for the Get My Payment application found one medium-risk vulnerability due to the use of weak cryptographic ciphers. In addition, in the *Get My Payment Tier 2 Security Assessment Report*,<sup>45</sup> the Cybersecurity function's Security Risk Management office issued a finding to the Integrated Customer Communications Environment authorizing official stating that the web application scan had identified the use of weak cryptographic ciphers. The use of weak cryptographic ciphers could be exploited by a malicious attacker and potentially compromise the system's confidentiality, integrity, and availability.

**Management Action:** On June 18, 2020, the Applications Development function opened a plan of action and milestones with a planned completion date of July 1, 2021.

In its audit of the *IRS's internal control over financial reporting*, the GAO reported that it found a discrepancy related to cryptography. The IRS did not enforce cryptographic protocols used for authentication and data integrity in a system environment that processes taxpayer data in accordance with NIST guidance and agency policy.

---

<sup>45</sup> Dated June 10, 2020.

## System environment security

Management of the system security environment provides organizations the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate. It also contributes to information systems that are more resilient to cyberattacks and other threats. Security controls include, but are not limited to, system configuration management; system scanning, vulnerability remediation, and patching; information system boundary components; and network monitoring and audit logs.

## System configuration management

Configuration management administers security features for all hardware, software, and firmware components of an information system throughout its life cycle. Effective configuration management provides reasonable assurance that systems are operating securely and as intended. It encompasses policies, plans, and procedures that call for proper authorization, testing, approval, and tracking of all configuration changes and for timely software updates to protect against known vulnerabilities. Ineffective configuration management controls increase the risk that unauthorized changes could occur and that systems are not protected against known vulnerabilities.

In Fiscal Year 2021, TIGTA conducted two audits of system configuration management controls. We initiated an audit<sup>46</sup> to ***determine whether the virtual host infrastructure platform is effectively managed and secured***. We found that configuration management compliance for Windows and Linux servers is not effective. The IRS had implemented a new software configuration management compliance scanning application in April 2020 to replace the prior application, which was outdated. On December 15, 2020, we met with Cybersecurity and Enterprise Operations function officials for a demonstration of the new application. We observed that the new application scanned [REDACTED]

[REDACTED]. In addition, we reviewed monthly configuration management compliance reports of virtual host infrastructure platform servers running on Windows and Linux operating systems from August through November 2020 and [REDACTED]

[REDACTED]. According to Cybersecurity function officials, a server is noncompliant if it has one high-risk issue or the overall compliance score is below 90 percent. [REDACTED]

---

<sup>46</sup> TIGTA, Report No. 2021-20-024, *Improvements Are Needed to More [REDACTED] the Virtual Host Infrastructure Platform* (June 2021).

Figure 8: \*\*\*\*\*2\*\*\*\*\*

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

In addition,

<sup>47</sup>

[REDACTED]

<sup>48</sup>

In addition,

[REDACTED]

In our audit of the *Criminal Investigation e-Crimes labs*, we found that

[REDACTED]

<sup>47</sup>

<sup>48</sup> In Calendar Year 2013, the Department of Homeland Security established the Continuous Diagnostics and Mitigation Program as an implementation approach for continuously monitoring information systems. The program is designed to facilitate automated security control assessment and continuous monitoring consistent with established guidance by providing a robust, comprehensive set of monitoring tools, a continuous monitoring dashboard, and implementation assistance.

## System scanning, vulnerability remediation, and patching

One of the basic tenets of network security is the periodic monitoring and scanning for network vulnerabilities and timely remediation of identified vulnerabilities in order to reduce the exposure of exploitation. The information technology landscape is dynamic and always evolving in order to become more efficient and secure. Hardware and software vendors are constantly identifying errors and glitches within their components and issuing fixes to patch these weaknesses. Users must be diligent to identify weaknesses and take appropriate actions to minimize the chance of these weaknesses being exploited.

In Fiscal Year 2021, TIGTA performed five audits involving system scanning and vulnerability patching of IRS systems. In our audit of the *CARES Act economic impact payment processing*, we found that most required baseline security controls were implemented for the Get My Payment application. Specifically, 470 NIST and agency-specific security controls and control enhancements were applicable to the application. We found that 463 (99 percent) of the 470 security controls and control enhancements were fully implemented.<sup>49</sup> The remaining seven security controls and control enhancements identified as not implemented contained specific risk areas that need to be addressed.<sup>50</sup> The IRS documented an active plan of action and milestones for each risk area to reduce these risks, ensure system integrity, and maximize system availability for taxpayers.

While the IRS has successfully deployed the necessary tools and implemented procedures to detect software vulnerabilities for the Get My Payment application, it did not timely remediate critical and high-risk vulnerabilities. Based on our analysis of the May 2020 database vulnerability scan report for the Integrated Customer Communications Environment, which houses the application, we determined that 17 critical (four unique) vulnerabilities and 169 high-risk (five unique) vulnerabilities exceeded the IRS policy of 30 and 90 days for remediation, respectively. Nine (53 percent) of the critical vulnerabilities have existed for more than 180 days, of which four had a first-failed date of October 2, 2018, and 121 (72 percent) of the high-risk vulnerabilities have existed for nearly 590 days, of which 105 had a first-failed date of October 2, 2018. In addition, the IRS completed the required source code security review for the Get My Payment application on April 3, 2020. Our analysis of the source code security review report identified six security vulnerabilities (two medium-risk and four low-risk) related to input validation, injection, cross-site scripting, information leakage through log files, and improper resource shutdown due to using outdated software.

In the *Get My Payment Tier 2 Security Assessment Report*, the Cybersecurity function's Security Risk Management office issued a finding to the Integrated Customer Communications Environment authorizing official stating that the database vulnerability scan reports identified

---

<sup>49</sup> The control families associated with the security controls and control enhancements fully implemented include: Access Control; Audit and Accountability; Awareness and Training; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Personnel Security; Physical and Environmental Protection; Planning; Security Assessment and Authorization; and System and Services Acquisition.

<sup>50</sup> The control families associated with the security controls and control enhancements not fully implemented include: Configuration Management (3), Risk Assessment (1), System and Communication Protection (1), and System and Information Integrity (2).

17 critical and 169 high-risk vulnerabilities. The IRS assessed the likelihood of a threat and the impact of a threat exploiting these vulnerabilities as high and moderate, respectively, and assessed the overall risk level associated with these vulnerabilities as moderate. The Security Risk Management office also stated that medium and low-risk findings were identified in the *Static Source Code Analysis and the Dependency Check Report*.

Failing to timely remediate critical and high-risk vulnerabilities as well as all findings in the *Static Source Code Analysis and the Dependency Check Report* could compromise the security posture of the Get My Payment application's database. This could lead to unauthorized access, increased vulnerability to attacks, unauthorized data sharing, and known weaknesses being exploited by malicious bad actors.

**Management Action:** On June 18, 2020, the Applications Development function opened two plans of action and milestones with a planned completion date by July 2, 2021.

In our audit of the *Criminal Investigation e-Crimes labs*, we found that [REDACTED]

In our audit of the *virtual host infrastructure platform*, we found that [REDACTED]

[REDACTED]. Specifically, [REDACTED]

[REDACTED]. We initially reviewed vulnerability scan reports from January through May 2020 from the previous enterprise vulnerability scanning tool. During a meeting in September 2020, Enterprise Operations and Cybersecurity function officials confirmed the implementation of a new vulnerability scanning tool in August 2020. In addition, we reviewed monthly scanning reports from the new vulnerability scanning tool from September through November 2020. [REDACTED]

Figure 9: \*\*\*\*2\*\*\*\*

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED] <sup>51</sup>	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

In our audit of *protection of disclosed return information at the ISAC*, we found that FTI is transmitted through secure connections, using the [REDACTED] approved by the NIST, and no known protocol vulnerabilities were identified related to the connections. [REDACTED]

We reviewed for security vulnerabilities on the IRS servers housing FTI prior to transmission.<sup>52</sup> On August 31, 2020, the IRS switched vulnerability scanning tools from [REDACTED]. The IRS stated that it decided to use the [REDACTED] vulnerability scanning tool because it was able to increase network coverage, improve reporting times, and reduce the need to perform remote credentialed vulnerability scans by incorporating an agent. In addition, IRS personnel felt that the [REDACTED] tool was more robust and found it to be more accurate in reporting vulnerability findings. We were unable to verify the differences and effectiveness between the two vulnerability scanning tools. However, both [REDACTED] and [REDACTED] scan results throughout the audit continued to show the existence of [REDACTED].

\*\*\*\*2\*\*\*\* scan results

Our review of the IRS's [REDACTED] vulnerability scans from March through June 2020 identified [REDACTED]

<sup>51</sup> The May 2020 table entry represents our analysis of 19 weekly vulnerability scan reports from January through May 2020 from the previous vulnerability scanning tool. Some vulnerabilities appeared in more than one file, and we eliminated duplicated entries. We identified a unique set of records and their first and last reported dates so we could calculate the number of days between the two date entries.

<sup>52</sup> The IRS places FTI in folders on its servers for the TTP and is archived off after 10 days once the TTP picks up the data.

[REDACTED]

When we shared the analysis results with IRS personnel, they explained that some of the vulnerabilities were a result of the [REDACTED], *i.e.*, software installation was not complete. They stated that the [REDACTED] software was misconfigured for the two backup servers, but the [REDACTED]. However, we also identified vulnerabilities other than the [REDACTED] findings that resided on the servers, such as the [REDACTED]. IRS personnel further stated that they patch monthly and the [REDACTED].

To verify whether the identified vulnerabilities were resolved, we reviewed [REDACTED] scans dated August 17 through 20, 2020, and confirmed that the vulnerabilities attributed to the same [REDACTED] had been corrected for the two production servers. However, we found [REDACTED] were the same as the ones we found previously. The remaining [REDACTED] were identified in July 2020 on a [REDACTED].

\*\*\*\*2\*\*\*\* **scan results**

Our review of the IRS's [REDACTED] vulnerability scans from August 17 through September 18, 2020, identified [REDACTED].

Unresolved [REDACTED] that remain on [REDACTED] may unnecessarily expose the server to exploitation and compromise. By focusing remediation efforts on the highest scoring vulnerabilities, the IRS can achieve the greatest possible risk reduction to FTI stored on the servers for transmission to the TTP.

In our audit of the [REDACTED] *Platform*, we found that some servers were not scanned for vulnerabilities. The Enterprise Vulnerability Scanning process includes probes of communication services, operating systems, and applications to identify high-risk system weaknesses that could be exploited to gain unauthorized access to IRS networks and data. We compared the official inventory report dated February 18, 2021, to vulnerability scanning reports and found that [REDACTED].

Without complete scanning of all production servers, the IRS cannot adequately define its current security posture because some critical vulnerabilities may go undetected.

**Management Action:** The IRS started scanning 36 of the 41 production servers as of July 2021. Three of the unscanned servers are retired and the remaining two are under investigation.

We also found that configuration compliance controls are insufficient. Specifically, production servers are not compliant with configuration requirements, configuration vulnerability age is not tracked, and checklists used in the configuration compliance scanning tool are outdated and differences in requirements are not documented.

### **Production servers are not compliant with configuration requirements**

We met with the Director, Security Operations and Standards, and other Enterprise Operations function officials who provided documentation that stated between April 2020 and April 2021, they remediated approximately 19,000 [REDACTED] vulnerabilities. However, our review of the configuration compliance scanning tool dashboard output determined that

[REDACTED]

[REDACTED]. During the audit, the IRS provided a plan to replace 1,025 [REDACTED] servers and 781 [REDACTED] servers by December 2023. Configuration vulnerabilities that lack remediation can allow an attacker the opportunity to access and control servers.

### **Configuration vulnerability age is not tracked**

The configuration compliance scanning tool report provides limited historical information, such as client last seen dates. Our review of the scan report determined that the IRS does not keep track of when a vulnerability was first seen or remediated. According to the IRS, the client last seen date shows when the configuration compliance scanning tool last scanned the server. The IRS further stated the configuration compliance scanning tool

[REDACTED]

### **Checklists used in the configuration compliance scanning tool are outdated and differences in requirements are not documented**

The vendor-provided checklists in use by the configuration scanning tool had undergone adjudication reviews in [REDACTED] for [REDACTED] operating systems in production. However, the adjudicated vendor-provided checklists used in the configuration compliance scanning tool were not from the most current Defense Information Systems Agency security guide and did not align with IRS security requirements checklists. We determined that the vendor-provided [REDACTED] checklist used an outdated security guide released on [REDACTED]

[REDACTED]. We did not identify a Defense Information Systems Agency revision history for the vendor-provided [REDACTED] checklist; however, the IRS stated it is aware of needed improvements. When outdated Security Requirements Checklists are used in the configuration scanning tool, critical vulnerabilities that hackers can exploit may not be timely detected.

We also reviewed the IRS's adjudication of the vendor-provided checklists used in the configuration scanning tool and found that the IRS reviews the vendor-provided checklists and documents deviations from Internal Revenue Manual requirements. However, the review does

not document when a check required by the IRS's Security Requirements Checklists are not included in the vendor-provided checklists. The IRS lacks an adjudication process that would ensure that all security requirements are accounted for in the vendor-provided checklists used in the configuration compliance scanning tool. An official stated that the IRS is in the process of updating the vendor checklist adjudication process to account for security requirements that are not included in the vendor-provided checklists. Without ensuring that this process occurs, critical and unique security requirements may not be applied to IRS systems.

In our audit of the [REDACTED] Platform, we also found that vulnerability scanning and remediation are insufficient. Specifically, credentialed scans are not performed on all production servers, vulnerabilities are not timely remediated, and vulnerabilities open past remediation time frames are not effectively documented and tracked.

### **Credentialed scans are not performed on all production servers**

We reviewed two vulnerability scan reports from February 2021 and found [REDACTED].

**Management Action:** The IRS provided evidence that it is currently performing credentialed scans on [REDACTED].

### **Vulnerabilities are not timely remediated**

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

In addition, we identified an instance in which [REDACTED].  
[REDACTED] Unpatched

vulnerabilities allow bad actors to conduct attacks against the [REDACTED] Platform infrastructure. Unpatched vulnerabilities may also provide entry points into a network.

### **Vulnerabilities open past remediation time frames are not effectively documented and tracked**

We judgmentally sampled 12 and 36 servers with [REDACTED]. The IRS did not have a documented plan of action and milestones or risk-based decision to track the remediation of any of the [REDACTED] we sampled. Due to the lack of management oversight, the IRS is not ensuring that unremediated vulnerabilities are being tracked as required. Without tracking vulnerabilities, there is a possibility some vulnerabilities will not be remediated.

### **Information system boundary components**

The information system boundary controls the logical connectivity into and out of a network as well as to and from devices attached to the network. It should accurately reflect and include all components within the authorization boundary of the information system and be at a level of detail necessary for tracking and reporting.

In Fiscal Year 2021, TIGTA performed an audit involving information system boundary components. In our audit of the *CARES Act economic impact payment processing*, we found that there is no information system component inventory for the Get My Payment application. Specifically, our review of the *Get My Payment Continuous Monitoring Assessment Plan*<sup>53</sup> and the *Get My Payment Tier 2 Security Assessment Report* determined that the application does not develop, maintain, or update an inventory that is at the required level of granularity and contains all system components of the application. Failing to develop, maintain, or update a complete inventory could result in information system components not being included in vulnerability and compliance scanning as well as the contingency plan being inadequate should it be needed during an event.

### **Network monitoring and audit logs**

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Audit and monitoring controls can help information systems security professionals routinely assess computer security, recognize an ongoing attack, and perform investigations during and after an attack.

In Fiscal Year 2021, TIGTA performed two audits involving network monitoring and audit logging. In our audit of the *virtual host infrastructure platform*, we found that the IRS does not currently have automated mechanisms to integrate audit logging, monitoring, review, analysis, and reporting for VMware servers in the virtual host infrastructure platform. This status was reflected in the platform's June 2020 System Security Plan, which shows the IRS designated the "Audit Review, Analysis, and Reporting" control as "Not In Place" for VMware virtual host servers.

---

<sup>53</sup> Dated May 21, 2020.

The IRS created a plan of action and milestones in May 2017 that stated there was no evidence of review and analysis of information system audit records or reporting of findings to IRS officials for VMware servers. However, between August 2017 and April 2019, there were several requests, including management escalations, from the Cybersecurity function to the Virtual Host Infrastructure team asking for milestone updates. As a result of these unanswered requests, the planned completion date for the plan of action and milestones has been delayed, with a new target completion date of June 15, 2021. By not deploying automated monitoring, VMware virtual host server risk assessment and reviews are less timely and the servers are at a higher risk of exploitation from known vulnerabilities. Protecting critical assets and infrastructure helps reduce the risk of internal and external attacks on IRS assets.

In our audit of the *EDR solution*, we found that alert logs generated by the EDR solution are delivered through e-mail messages to the appropriate personnel and are forwarded to the [REDACTED]. Currently, Computer Security Incident Response Center analysts log all alerts issued from the EDR solution. However, prior to December 1, 2020, they did not have documentation to support logging actions. From January 1 through April 30, 2021, there were 735 alerts generated by the EDR solution, and there were 735 line items in the Computer Security Incident Response Center tracking log.

We also found that none of the alerts resulted in an incident and that the EDR solution is effectively generating alerts from the workstations. The alerts are being properly tracked and worked. The alerts were caused by either internal testing, legitimate processes or indicators of the appearance of a possible threat, *e.g.*, Powershell™, or potential credential theft attempts, which the EDR solution incorporates rules to identify as potential for concern. After the Computer Security Incident Response Center analysts conducted their reviews, they decided that none of the alerts qualified to be an incident.

## Disaster recovery

Disaster recovery is part of security planning and developed in conjunction with a business continuity plan. Disaster recovery is a set of policies and procedures that focus on protecting an organization from any significant effects in case of a negative event, which may include cyberattacks, natural disasters, or building or device failures. Disaster recovery helps in designing strategies that can restore hardware, applications, and data quickly for business continuity.

In Fiscal Year 2021, TIGTA provided coverage of disaster recovery in two audits. In our audit of the *Criminal Investigation e-Crimes labs*, we found that [REDACTED]

[REDACTED]

In our audit of *protection of disclosed return information at the ISAC*, we found that the ISAC alternate processing site does not meet the filing season maximum tolerable downtime.<sup>54</sup> We reviewed the October 1, 2019, draft plan to determine the resources needed to build an alternate ISAC processing site. According to the plan, the TTP determined that the ISAC classifies as a moderate-impact system based on Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.<sup>55</sup> The plan also included a detailed cost summary of [REDACTED] of the [REDACTED] as an alternate processing option based on the inventory of current resources required to operate. In response to the need for an alternate processing site identified during a review of the ISAC in February 2020, the TTP developed a strategy and implemented a "no cost" [REDACTED]. The TTP is committed to working with the IRS to incrementally "warm" the site.

However, our review of the current and future alternate processing site choices found that neither meets the maximum tolerable downtime needs for a filing season. The IRS responded that it is continuing ongoing discussions with the TTP, considering the costs and benefits associated with increasing resources and maintenance for a [REDACTED]. The ISAC is an important platform for the IRS and its partners' day-to-day operations to combat identity theft tax refund fraud and gain near-term data on emerging trends, and its continuity of operations is critical to ensure that fraud information is timely shared with its partners. The IRS found that the ISAC directly protected about \$3 million in fraudulent identity theft Federal refunds from being issued during Calendar Year 2018. Its importance will only continue to grow over time.

## Roles and responsibilities and separation of duties

As organizations continue to do more with less, the lines of communications, expectations, and alignment on achieving the vision of the organization are critical to its success. Defined roles and responsibilities provide clarity, alignment, and expectations to those executing the work and keeping the organization running. Separation of duties helps to ensure that no single individual has authorization to control all key aspects of a process or computer-related operation. Effective separation 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 separation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed.

In Fiscal Year 2021, we performed two audits involving roles and responsibilities and separation of duties. In our audit of the *EDR solution*, we found that not all EDR solution users were added to their assigned Active Directory domain groups. Specifically, we found four (10 percent) of 42 users who were not added to all of their assigned Active Directory domain groups, but were located in only their system administrator or investigator domain groups. There are four roles, *i.e.*, administrator, analyst, senior analyst, and investigator, in each of the three Active Directory domain groups, *i.e.*, production, test, and development, in the EDR management environment. For example, one user was not found in the investigator, production domain group, but was

---

<sup>54</sup> ISAC business process owners collaborated on the potential impact of a loss of the process/service and agreed that the maximum tolerable downtime the process owners and users are willing to accept is 72 hours for non-filing season and 24 hours for filing season because filing season is a critical time for the ISAC.

<sup>55</sup> Dated February 2004.

approved for that role and group. However, we did not find the user in the Active Directory production domain group. A Cybersecurity official stated that this user is a member of the analyst, production domain group, which has fewer rights than the investigator role.

For proper reporting and auditing moving forward, the IRS stated that the Cybersecurity function's EDR team will work to ensure that the Online 5081 system user assignments map correctly to the associated Active Directory groups for access to the environment for proper continuity. Until the role-mapping is corrected, we caution that if the IRS does not properly manage its role assignments, it will be unable to monitor the system administrator users' activity beyond the administrator and investigator role in the EDR management environment. Accuracy in role assignment management provides an independent check on the accounting for work performed and reduces the risk of inappropriate employee actions.

In our audit of the [REDACTED] *Platform*, we found that the Platform has one user who is both a member and an owner of a group, violating separation of duties. Without an effective review of the owners responsible for administering the group roles, accounts can be improperly managed and may violate separation of duty policies.

### **Security policies, procedures, and documentation**

The documentation of system security is an important element of information management for an organization. A system security policy identifies the rules and procedures that all individuals accessing and using an organization's information technology assets and resources must follow. The goal of security policies is to address security threats and implement strategies to mitigate information technology security vulnerabilities. Policies and procedures are also an essential component of any organization. Policies are important because they address pertinent issues, such as what constitutes acceptable behavior by employees. Procedures, on the other hand, clearly define a sequence of steps to be followed in a consistent manner.

During Fiscal Year 2021, TIGTA performed four audits involving security policies, procedures, and documentation. In our audit of the *IVES Program*, we found that the IRS completed actions to comply with the TFA to establish uniform standards and procedures for the acceptance of taxpayers' electronic signatures when requesting a taxpayer's return or return information. This guidance was published in the Internal Revenue Manual in December 2019 and addresses electronic signatures on forms used to request tax information, including Form 4506-T. However, we also found that internal guidelines were not updated with key IVES Program processes and procedures. This includes the administration of the electronic signature program, including the requirement for participants to submit the annual independent audit report on their electronic signature process, and the procedures IVES Program analysts should take for participants that do not meet the electronic signature requirements or submit the required independent audit report of their electronic signature process. Although IVES Program management stated that the procedures are documented in standard operating procedures, these procedures should be documented in the Internal Revenue Manual, which provides a single, authoritative compilation of the policies and procedures affecting IRS work.

In our audit of *protection of disclosed return information at the ISAC*, we found that while the IRS and the TTP established controls that complied with the TFA to secure FTI, the memorandum of understanding needs updating regarding incident reporting. Specifically, we found that incident reporting was not aligned with internal guidance to include the Computer

Security Incident Response Center as one of the primary points of contact, and that the incident response tabletop exercise<sup>56</sup> neither tested nor reported all aspects of responding to an incident.

The Computer Security Incident Response Center serves as the primary coordination point and oversees all incident responses at the IRS. It also serves as the liaison between the IRS and the Treasury Department's Government Security Operations Center for all communications and follow-up activities in response to an activity. The IRS is required to report breaches or incidents, whether confirmed or suspected, to the Government Security Operations Center as quickly as possible after discovery, but no more than one business day.

We reviewed the tabletop exercise that the TTP performed in July 2019 and July 2020. The primary objectives of the exercise were to validate the [REDACTED] the incident response handling and reporting procedures; and identify areas of the incident response plan that need to be revised. We confirmed that the TTP reported the security incident to TIGTA, the contracting officer representative, and the Office of Safeguards as part of the simulation activity, but was not reported to the Computer Security Incident Response Center. Because the Computer Security Incident Response Center is the primary IRS function to respond to security incidents and coordinate reactive and preventative actions from incidents across the enterprise, it is imperative that it is aware of all incidents directed at IRS assets, including those at IRS third-party systems to ensure that appropriate actions are taken.

In addition, our review of the tabletop exercise documents determined that they did not support that the TTP generated a simulated report with the required data fields, *e.g.*, the data and potential number of FTI records involved. A TTP official confirmed that they did not test whether the necessary data could be produced as required. The IRS stated that a report can be generated for the Fiscal Year 2021 Incident Response exercise and will be available for review. We requested that the TTP provide a limited report showing FTI filename, date, and file type, *i.e.*, potential or confirmed identity theft tax refund fraud, that ISAC users downloaded during March to July 2020. The TTP provided a report listing the date and file type, but not the filename. The TTP stated that providing the filename would require a manual review of each FTI file and the removal of some identifying information. We believe that using a manual process to identify the filename of the files that the users download could create a delay in reporting this information to the IRS and TIGTA, which could subsequently delay the reporting and investigation into possible unauthorized disclosure incidents.

Our review of the requested information showed that 31 industry partner users downloaded 155 files<sup>57</sup> from the ISAC. Of the files downloaded, 137 files were the IRS's FTI files consisting of 102 potential and 35 confirmed identity theft tax refund fraud files. The confirmed files contained Personally Identifiable Information. Because the TTP did not provide the filenames that were downloaded, we could not determine whether a [REDACTED] or [REDACTED] identity theft refund fraud file was downloaded. Without the filenames, we could not calculate the precise number of taxpayer records in the files.

---

<sup>56</sup> The title of the exercise, *i.e.*, test, is [REDACTED] Incidence Response Test and Exercise, but it is referred to as the tabletop exercise.

<sup>57</sup> Each file contains more than one taxpayer account.

In our audit of *protection of disclosed return information at the ISAC*, we also found that the privacy notification was not fully completed for all privacy aspects. The IRS requires system owners to update the Privacy and Civil Liberties Impact Assessment every three years or sooner if there are major changes to the system. The existing ISAC assessment was dated December 18, 2019, and was not updated after Congress' July 2019 approval to permit the sharing of FTI. However, during our audit work, the IRS's Privacy, Governmental Liaison, and Disclosure office and the Wage and Investment Division's Return Integrity and Compliance Services function worked with the TTP to update the Privacy and Civil Liberties Impact Assessment, which was approved on May 12, 2020. Our review of the latest assessment found that the IRS appropriately completed all but two of the 31 questions in the Privacy and Civil Liberties Impact Assessment.

- Question 6.c asked: *Does this system contain sensitive but unclassified information that is not Personally Identifiable Information, it uses, collects, receives, displays, stores, maintains, or disseminates?* The IRS answered "no" for "Proprietary data," which is defined as *Business information that does not belong to the IRS*. We found the ISAC [REDACTED].
- Question 21 asked: *The following people have access to the system with the specified rights: IRS Employees?* The IRS answered "no." In addition, the table indicating the access levels (read only, read-write, or administrator) for each type of IRS employee, *i.e.*, user, manager, administrator, or system developer, was left blank. We found that IRS employees do have access to the ISAC with various access levels. As of December 2020, 87 IRS employees were users, and 31 had access to FTI, including TIGTA employees (Office of Audit and Office of Investigations) who are provided access to the ISAC as IRS users.

The IRS states on its website that it recognizes the importance of protecting the privacy and civil liberties of taxpayers and uses the Privacy and Civil Liberties Impact Assessment as the vehicle to address privacy and civil liberty issues in a system. The assessment demonstrates that program/project managers, system owners, and developers have consciously incorporated privacy and civil liberty protections throughout the entire system. When the Privacy and Civil Liberties Impact Assessment is inaccurate and incomplete, it weakens the assurances that it was designed to promote.

In our audit of the *Criminal Investigation e-Crimes labs*, we found that [REDACTED]

In our audit of the *hardware asset sanitization process*, we found that the draft *MSS Standard Operating Procedures* need to be clarified concerning accounting for damaged or missing hard

disks. During our review, two sampled computers with missing hard disks were incorrectly stored on a pallet with sanitized devices and incorrectly recorded as accounted for in the MSS's hardware asset inventory. The Internal Revenue Manual states that the IT organization is "responsible for the accounting and recording of IT [information technology] property in the inventory system.... This process supports the integrity of the data by ensuring accurate and complete asset records are maintained." However, the draft *MSS Standard Operating Procedures* state that personnel should remove the computer's damaged hard disk and give it to the tape library at the Enterprise Computing Center – Memphis but does not clearly define under what circumstances to do so, any time frame for doing so, or how to account for the hard disks in the MSS's hardware asset inventory. In addition, these procedures do not explain how to account for computer shells sent to the MSS with missing hard disks. This lack of detailed guidance resulted in the IRS misplacing hard disks most likely containing taxpayer data and errors in the hardware asset inventory records.

## **Systems Development and Information Technology Operations**

In carrying out its responsibilities of administering the tax laws, the IRS relies extensively on information technology investments to support its mission-related operations. The IRS's ability to provide high-quality taxpayer service and maintain the integrity of the tax system requires modern, secure, and nimble operations, as well as a sustained and talented workforce. Many emerging trends offer challenges and opportunities for the IRS, including changes in the taxpaying public and its expectations, technological disruptions, shifts in the workforce, and an increasingly globalized and interconnected world.

TIGTA and the GAO performed several audits that assessed systems development and information technology operations at the IRS. These audits covered information technology acquisitions, asset management, human capital, project management, risk management, implementation of corrective actions, modernizing operations, and COVID-19 response.

### **Information technology acquisitions**

The mission of the Office of the Chief Procurement Officer is to deliver top-quality acquisition services to ensure that the IRS can meet its mission of effective tax administration. Within the Office of the Chief Procurement Officer, the Office of Information Technology Acquisitions is primarily responsible for managing the procurement of information technology products and services, and ensuring that the IRS acquires them for the best value, within budget, and in a timely manner. It is also responsible for ensuring that the information technology acquisition process is managed properly and efficiently, and is conducted with integrity, fairness, and openness. As stewards of taxpayer dollars, the IRS must ensure that it only pays for the procured products or services as authorized and delivered under contract.

During Fiscal Year 2021, TIGTA performed two audits covering information technology acquisitions. We initiated an audit<sup>58</sup> to ***assess the effectiveness of select post-award activities of information technology service contracts***. We selected and reviewed a stratified statistical sample of 190 payments from a population of 12,109 invoice payments totaling

---

<sup>58</sup> TIGTA, Report No. 2021-20-046, *Select Post-Award Financial Management and Documentation Controls for Information Technology Service Contracts Need Improvement* (Aug. 2021).

approximately \$2.82 billion, made between October 1, 2018, and June 30, 2020. Some of these invoice payments came from a population of information technology service contracts<sup>59</sup> in which the material group and Federal supply code combinations were valid<sup>60</sup> and invalid.<sup>61</sup> We initially selected 96 and 94 payments, respectively, for review. However, upon further review of the expense(s) on each invoice, we determined that six of the valid and 67 of the invalid code combinations were not from one of the 10 information technology service subcategories we selected for review. As a result, our sample was reduced to 90 and 27 invoice payments, respectively. Collectively, we reviewed 117 invoice payments.

All the invoices provided for the 117 sampled information technology service contract payments met minimum Federal Acquisition Regulation<sup>62</sup> standards, *e.g.*, included information on contract or other authorization number for the services performed, including the order and line item numbers, payment terms. However, we also found invoice payments that could not be fully verified due to insufficient receipt and acceptance documentation.<sup>63</sup> Of the documentation provided for our sample, we determined that the invoices were appropriately verified and supported for 44 payments. For 73 invoice payments, we could not make this determination because the IRS was unable to provide all of the necessary supporting documentation requested. Projecting our sample results to the total population of information technology service contracts, we estimate that the IRS may not have properly maintained sufficient receipt and acceptance documentation to support 6,502 invoice payments.<sup>64</sup>

For our analysis, we initially accessed the Folders Management module of the Procurement for Public Sector application to obtain the respective contract, modification(s), and supporting receipt and acceptance documentation to determine whether post-award activities ensured that invoices for information technology service contracts were appropriately verified prior to being paid. However, we were unable to locate any of these documents because they are not organized in a manner that can easily be identified by either using file naming conventions or specific folders as an organizational tool. Consequently, on September 24, 2020, we sent an initial request to the IRS asking for documentation supporting a portion of the sampled invoice payments. From our initial request, the IRS provided some documents for 19 of 46 invoice payments, of which only three payments included receipt and acceptance documentation.

---

<sup>59</sup> Our review included the following 10 information technology service subcategories: 1) Acquisition – Tier III Support; 2) Indirect – Category II; 3) Indirect – Category III; 4) Install – Hardware and Software; 5) Install – Other; 6) Install – Tier III; 7) Maintenance – Operations and Automatic Data Processing; 8) Management Consulting; 9) Technical Services – Automatic Data Processing; and 10) Telecommunication.

<sup>60</sup> Document 12353, *Financial Management* (April 2020), provides a comprehensive list of valid financial codes as well as material group and Federal supply code combinations for use. This document is updated quarterly.

<sup>61</sup> Invalid combinations could include an incorrect material group code, an incorrect Federal supply code, or both. They could also include combinations that were once valid, but are no longer listed in the current Document 12353 and are now considered inactive.

<sup>62</sup> 48 C.F.R. § 32.905, *Payment Documentation and Process* (Aug. 2018).

<sup>63</sup> Receipt and acceptance documentation can include a *COR [Contracting Officer's Representative] and Technical Point of Contact Checklist*, an e-mail, or other documentation acknowledging the service or product provided was received and meets the requirements as specified in the contract.

<sup>64</sup> Our sample was selected using a 95 percent confidence level, a 5 percent error rate, and ±5 percent precision factor. When projecting the results of our stratified statistical sample, we are 95 percent confident that the actual total number is between 5,549 and 7,454 invoice payments that were not supported by adequate receipt and acceptance documentation.

On October 22, 2020, we became concerned with the pace and the limited number of documents the IRS had provided. As a result, we met with Office of Information Technology Acquisitions and IT organization personnel to clarify and explain the specific documents we had requested. We subsequently requested the remaining invoice payment documents on November 2 and 12, 2020, followed by additional meetings to further clarify and explain our documentation requests. Despite these efforts, we continued to experience delays. In total, we gave the IRS more than three months after our initial request to provide the supporting documentation for our sampled invoice payments. Office of Information Technology Acquisitions and IT organization personnel estimated that they spent more than 490 hours trying to locate the requested documentation.

**Management Action:** Recognizing that insufficient documentation was a concern, Office of the Chief Financial Officer management stated that they implemented a receipt and acceptance Supporting Documentation Upload Tool on February 24, 2021. According to an announcement, the Upload Tool provides an automated upload and transfer of supporting receipt and acceptance documentation with the proper file naming conventions into the appropriate folder in the Folders Management module. Use of the Upload Tool is required for every receipt and acceptance transaction, and the Procurement for Public Sector application will display an error message when supporting documents are not attached. The Upload Tool is expected to improve the timeliness of receipt and acceptance documentation uploads and subsequent searches for supporting documents.

For our analysis of financial management controls over invoice and interest payments, we obtained the IRS's *Fiscal Year 2020 Third Quarter Award Line Item*<sup>65</sup> table and identified 2,812 contracts containing information technology services. Upon further review, we excluded 709 contracts because the IRS had not made any payments on them as of November 3, 2020, or the Treasury Department was the requestor of the services and outside the scope of this review. We analyzed the remaining 2,103 contracts, totaling a combined award amount of approximately \$5.18 billion.

We determined that contract and modification dollar amounts were not always accurately captured and reported, resulting in the total payment for some contracts exceeding their award amounts. The IRS misreported \$7,469,962 for information technology service contracts from five base awards and 30 modifications in the Federal Procurement Data System, which the Federal Government, *e.g.*, the President, Congress, Federal executive agencies, uses to assess how to most effectively and efficiently expend its resources. In addition, the IRS potentially spent \$893,804 more than the total award amount of approximately \$139.05 million for 11 information technology service contracts due to incorrect information in the Integrated Financial System. As a result, IRS management does not have important information for effective financial management.

In our audit of *select post-award activities of information technology service contracts*, we also determined that late payment interest penalties were not always identified or correctly calculated. For our analysis, we used the 2,103 contracts containing information technology services. We reviewed all the invoices for the contracts that were paid on or before

---

<sup>65</sup> An electronic file obtained from the Procurement for Public Sector application that contains 10,718 IRS contracts as of June 30, 2020.

August 20, 2020,<sup>66</sup> and the IRS was the requester of the service. Of the 27,075 invoices reviewed, 1,176 invoices totaling approximately \$151.45 million were subject to interest penalties for late payments. We determined that the IRS correctly calculated the late payment interest penalties totaling \$141,443 for 1,008 (85.71 percent) invoices, but also miscalculated or did not identify that late payment interest penalties were due for 168 (14.29 percent) invoices. Specifically, the IRS underpaid late payment interest penalties of \$26,200 for 148 of the 168 invoices<sup>67</sup> and overpaid late payment interest penalties of \$1,664 for the remaining 20 invoices.

The Office of the Chief Financial Officer's Program and Process Review group has a review process that examines all interest penalties for invoice payments made from the previous business day. A financial management analyst reviews the calculations of the penalty amounts to determine if the Integrated Financial System properly calculated the interest. According to Program and Process Review group personnel, they already identified and took the necessary steps to make supplemental payments for the underpayments in interest penalties totaling \$15,217 for 90 of the 148 invoices we identified. They also offset against a current or future payment or created an account receivable to collect the interest penalty overpayments totaling \$1,610 for 12 of the 20 invoices prior to our review. We randomly selected 24 of these interest penalty miscalculations and were able to verify that the IRS took the necessary steps to correct them as stated. In addition, Program and Process Review group personnel confirmed our results that interest penalties were miscalculated with information obtained from the Integrated Financial System and the Procurement for Public Sector application, and agreed that they had not identified the miscalculations for 58 invoices with interest underpayments totaling \$10,984 and eight invoices with interest overpayments totaling \$53, respectively.

Further, some contracts were not charged to valid expense categories. The IRS charged some contracts to material group and Federal supply code combinations that are invalid as well as combinations that are no longer active when the Office of the Chief Financial Officer updated the codes. As a result, IRS expenses totaling approximately \$726 million reported in the Federal Procurement Data System were miscategorized.

In addition, we initiated an audit<sup>68</sup> to ***assess the IRS's implementation of the CIO's duties and responsibilities in relation to TFA § 2101, Management of Internal Revenue Service Information Technology***. We found that policies were established regarding the consulting and notification processes as required by the TFA. In July 2020, the Chief of Staff, the Deputy Commissioner for Services and Enforcement, and the Deputy Commissioner for Operations Support issued a memorandum to define the CIO's roles and responsibilities. Specifically, the memorandum addresses the planned IRS coordination efforts to comply with TFA § 2101, including that: 1) the CIO should regularly consult with the Chief Procurement Officer concerning information technology products and services acquired for the IRS and 2) the Chief Procurement Officer should notify the CIO of all significant information technology purchases prior to their acquisition. The memorandum further requires the Chief Procurement Officer to ensure that any procurement requests for information technology products and services reflect

---

<sup>66</sup> We used August 20, 2020, for this test rather than the November 3, 2020, date in the previous finding in which total payments exceeded the award amount because the IRS provided two separate financial data updates that were necessary to conduct each test.

<sup>67</sup> Additional interest does not accrue on interest penalties that are underpaid.

<sup>68</sup> TIGTA, Report No. 2021-25-058, *Efforts to Implement Taxpayer First Act Section 2101 Have Been Mostly Successful* (Sept. 2021).

engagement with the IT organization, and if they do not, the Chief Procurement Officer should cease the procurement activities and inform the requesting business units that they must engage the IT organization. To satisfy the notification requirement of TFA § 2101, the IRS relies on two processes: 1) the *Greater Than \$1 Million Report* and 2) monthly meetings between the Chief Procurement Officer and the CIO in which they discuss significant planned and in-process information technology acquisitions.

However, the CIO is not notified of all significant information technology acquisitions. Initially, the *Greater Than \$1 Million Report* showed only acquisitions for the IT organization and did not include the information technology product and service acquisitions for non-information technology business units, e.g., the Wage and Investment Division, Criminal Investigation. While the report did contain a way to filter the data to include all non-information technology business unit acquisitions, it did not have the ability to identify which acquisitions were for information technology products and services.

In November 2020, the Office of the Chief Procurement Officer modified the *Greater Than \$1 Million Report* to incorporate logic to identify information technology product and service acquisitions initiated by non-information technology business units. To test the accuracy of the report, we analyzed and compared current Procurement for Public Sector application data to the *Fiscal Year 2021 Greater Than \$1 Million Report* as of May 2021. Using some of the more general material group codes that could be applicable to information technology acquisitions, we initially identified 100 potential information technology shopping carts<sup>69</sup> not on the report. Upon further research and discussions with the IRS, we determined that, in our initial group of 100 acquisitions, there were 25 shopping carts, each in excess of \$1 million<sup>70</sup> that included information technology products and services. These 25 shopping carts, totaling approximately \$57.8 million, were initiated by non-information technology business units and contained material group codes that were not listed in the selection criteria used to create the *Greater Than \$1 Million Report*.<sup>71</sup>

To determine if the IT organization properly approved shopping carts containing significant information technology acquisitions for non-information technology business units, we analyzed the approvals for the 25 shopping carts in the Procurement for Public Sector application that were not identified on the *Fiscal Year 2021 Greater Than \$1 Million Report* as of May 2021. None of these shopping carts for information technology products and services were properly approved by the IT organization.

The second process the IRS relies upon to comply with the notification requirements of TFA § 2101 is the monthly meetings between the Chief Procurement Officer and the CIO to discuss upcoming and in-process information technology acquisitions. The Chief Procurement Officer uses the *Greater Than \$1 Million Report* to communicate and discuss significant information technology acquisitions with the CIO.

---

<sup>69</sup> IRS business units use shopping carts in the Procurement for Public Sector application to request external products and services, and to secure the necessary approval and funding for those products and services prior to their acquisition.

<sup>70</sup> The shopping carts ranged from \$1 million to \$7.5 million.

<sup>71</sup> These material group codes included: 1) 2512 – Management Consulting Services, 2) 2357 – Communications Enforcement, and 3) 252H – Other Indirect Services Non-Federal.

The *Greater Than \$1 Million Report* and the monthly meetings are the primary tools used to notify the CIO of significant information technology acquisitions. However, by not accounting for all significant information technology shopping carts for non-information technology business units, the usefulness of these tools is limited and compliance with the TFA § 2101 notification requirements cannot be achieved.

## Asset management

Asset management controls are key to: 1) timely detecting loss, theft, or misuse of Government property; 2) helping to mitigate unauthorized access to taxpayer or other sensitive information; 3) ensuring accurate financial statement reporting; and 4) helping management make sound operating decisions and manage operations. Asset management includes asset inventory management and information technology architecture.

## Asset inventory management

Asset inventory is the way an organization lists and provides details of the assets it owns. Asset inventory management is the means by which an organization monitors its assets, such as physical location, maintenance requirements, depreciation, performance, and eventual disposition of the asset. Implementing robust procedures for managing asset inventory is a critical part of the organization's accounting processes. It also helps to ensure that the organization has a clear understanding of the assets it owns and that the assets are being utilized in the most efficient and cost-effective manner.

In Fiscal Year 2021, TIGTA performed four audits covering the management of hardware inventory. In our audit of the *Criminal Investigation e-Crimes labs*, we found that the hardware inventory of [REDACTED] is inaccurate. We reviewed two hardware inventories [REDACTED] assets dated June 4 and July 6, 2020.<sup>72</sup> The inventories included information, such as the asset's brand, model, barcode number, serial number, user, location, and last verified date and time. Based on the information to be captured in the inventory, Criminal Investigation should have sufficient information to track and report assets accurately.

During our site visits, we observed [REDACTED]. To assess the accuracy of the June 4, 2020, inventory, we compared each [REDACTED] barcode, location, and user assigned to the hardware inventory. We found that [REDACTED] (86 percent) of the [REDACTED] were accurately accounted for. However, [REDACTED] (14 percent) of the [REDACTED] were missing from the inventory. We requested another inventory dated July 6, 2020, and found no changes from the June 4, 2020, inventory.

At one [REDACTED], we found one [REDACTED] without an IRS barcode number. The CIS e-mailed us the barcode information and we compared the barcode information provided to the inventory dated June 4, 2020, and found that the location and user information did not match the [REDACTED] observed during the site visit. We also tried to verify the [REDACTED] serial number and found no corresponding asset. In addition, the [REDACTED] information provided was not located in the July 6, 2020, inventory. We notified Criminal Investigation personnel and they confirmed that the [REDACTED] from that

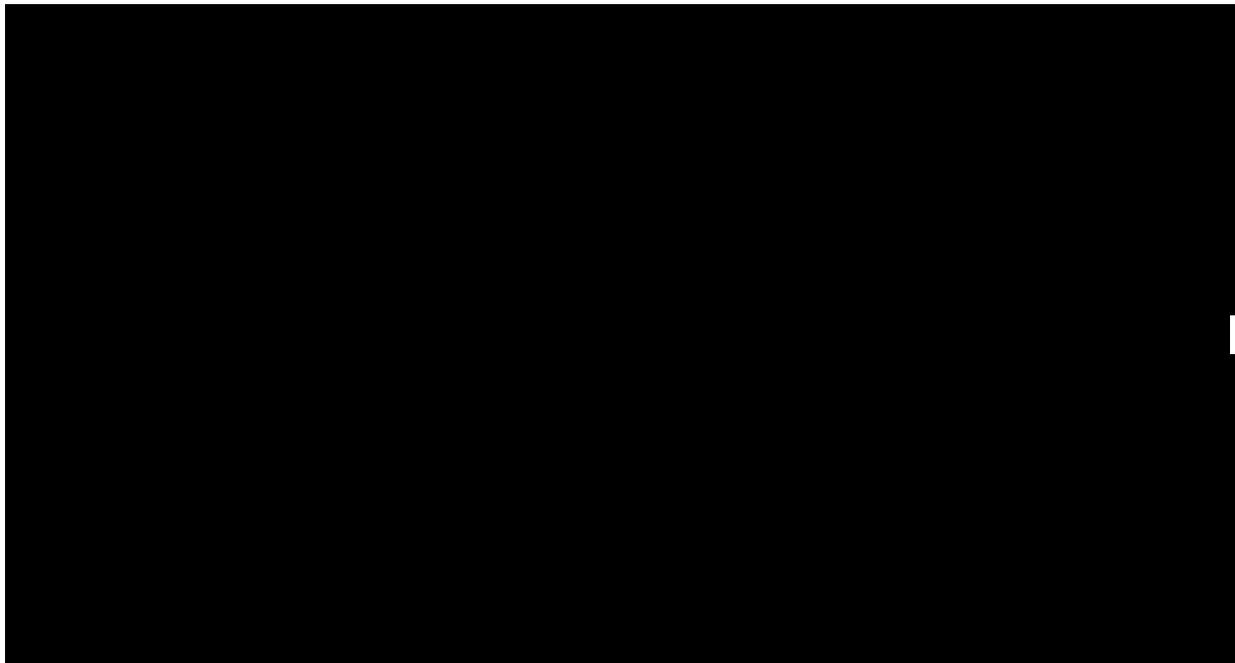
---

<sup>72</sup> Hardware inventory is maintained in the Knowledge, Incident/Problem, Service Asset Management database, which is the asset management tool used to track information technology and non-information technology equipment.



In our audit of the [REDACTED] Platform, we found that the platform inventory reconciliation process needs improvement. We reviewed the inventories from the Information System Contingency Plan, the vulnerability scanning tool, and the configuration compliance scanning tool to reconcile with the official inventory. We also reviewed the most recent annual security control assessment performed from March through April 2020 and found that the IRS failed to reconcile the official inventory to the Information System Contingency Plan inventory. To assess the accuracy and completeness of the [REDACTED] Platform inventory, we reconciled the January and February 2021 official inventory reports to the Information System Contingency Plan reports and identified variances between the inventories. Figure 10 provides the results of our review.

**Figure 10:** [REDACTED] 2 [REDACTED]  
[REDACTED] 2 [REDACTED]



Source: TIGTA analysis of data from the Information System Contingency Plan and official inventories. ISCP – Information System Contingency Plan.

In addition, we reviewed the February 2021 official inventory and found production servers with the following missing inventory data elements: 1) *Asset Location* field was blank for 286 servers, 2) *Serial Number* field was blank for seven physical servers, and 3) *Building Code* field was blank for two servers. An inaccurate inventory can hinder the agency's ability to manage systems and negatively affects systems that rely on the information within the official inventory, such as configuration and vulnerability scanning tool inventories.

We also found that nine servers in the official inventory are classified as being in production; however, according to the configuration compliance scanning tool, these servers are in the testing or development environments. The IRS stated that the Server Signature File is used to set the *Environment*, the *General Support System*, and the *Project* fields in the official inventory. The IRS stated that this discrepancy is due to an incorrect Server Signature File or the original file data were not populated correctly. Server misclassification can lead to vulnerabilities being excluded from prioritization and remediation efforts.

In our audit of the *EDR solution*, we found that it was neither fully accounted for nor deployed to all required workstations enterprise-wide. We requested the UNS function provide a list of workstations that were in use enterprise-wide from May 7 through December 31, 2020,<sup>74</sup> and that the Cybersecurity function provide a list of all workstations with the deployed EDR solution from the same time period. The UNS function also provided the January 31, 2021, status of workstations that were in use as of December 31, 2020, which totaled 111,283 workstations. However, UNS function personnel explained that in use was historically set as a financial qualification to indicate an asset was being used in some capacity by the IRS and not as an indication of it being on the network. In addition, UNS function personnel stated that their list could include duplicates, as some assets were taken in and out of use multiple times.

The Cybersecurity function's list totaled 96,441 workstations with the deployed EDR solution. When we compared the host name of the workstations from both lists, we identified 25,245 workstations that were on the UNS function's list but not on the Cybersecurity function's list. Further review of the data allowed us to remove 16,288 workstations from the list, which comprised of 14,931 workstations that were in stock, 1,329 workstations that were missing, and 28 workstations that were retired. We also removed 1,631 workstations that were duplicates and those that either received the in-depth defense capability<sup>75</sup> or the EDR solution after our cutoff date, which yielded a difference of 7,326 workstations that potentially did not have the EDR solution.

In April 2021, we provided a list of the 7,326 workstations to the IRS for review. The IRS stated that 10 workstations were not eligible for the EDR solution. A Cybersecurity function official conducted analysis and found that 61 workstations had the EDR solution but not the in-depth defense capability, and 256 workstations had the in-depth defense capability of which 203 had and 53 workstations did not have the EDR solution. For the remaining 6,999 workstations, which had neither the in-depth defense capability nor the EDR solution, Enterprise Services function personnel were unable to provide specific reasons why the EDR solution was not installed and stated it could take a month or more to research because it is a manual process. However, UNS function personnel provided possible explanations for the workstations that were in use but did not have the EDR solution. Possible explanations include the asset in use may have a bad security software agent and therefore, it does not show up on the network; the asset was in use, but an inventory transaction occurred that took the asset off the network, without the inventory transactional update being reported, *etc.*

In addition, we determined in a separate analysis with a Cybersecurity function official's assistance, that there were 144 workstations shown as connected to the network as of April 9, 2021, without the EDR solution. For the 144 workstations, five were not currently eligible for the EDR solution because they were Apple™ devices; three were blacklisted as they were not approved to be on the network; and 33 were found to be in stock but not in use. For the remaining 103 workstations, the IRS confirmed that 38 workstations appeared on the IRS's network between May 21 and June 2, 2021, and did not have the EDR solution deployed. For the remaining 65 workstations, 32 either had both the EDR solution and the in-depth defense capability or only the EDR solution, and 33 were not identified on the network when a

---

<sup>74</sup> The UNS function list of workstations is from the Asset Manager module in the Knowledge Incident/Problem Service Asset Management System.

<sup>75</sup> The official used the workstations that appear online by checking in through the in-depth defense capability to determine whether the workstations did or did not have the EDR solution.

Cybersecurity function official conducted a subsequent analysis, and as such, the current inventory status of those devices is unknown.

In total, we are concerned with the 91 confirmed workstations<sup>76</sup> without the EDR solution and 7,032 workstations<sup>77</sup> without a known explanation for why the EDR solution has not been deployed to them. These workstations will require further investigation to determine whether they are valid workstations and should have the solution installed. The unreliability of the status of the workstations impacts the Cybersecurity function's proactive approach of identifying cyberthreats and potential attacks before they occur, so they can be immediately remediated. The Cybersecurity function is making attempts to verify that the installation of the EDR solution is working correctly on each system, although Cybersecurity personnel admitted that challenges exist on how to best obtain missing/misconfigured installations and how to best rectify them as quickly as possible.

By not ensuring that all eligible workstations have the EDR solution installed, the IRS will be unable to monitor and obtain detailed records of incidents on all workstations and conduct root cause analyses of identified threats. These gaps of EDR deployments may also give a false sense of security, possibly missing opportunities to quickly mitigate incoming cyberattacks at the workstation.

### Information technology architecture

Information technology architecture is the fundamental underlying design of computer hardware, software, or both. An effective information technology architecture plan improves efficiencies. When the architecture program includes consolidation and centralization of information technology resources, complexity can be reduced and resource use can improve.

In Fiscal Year 2021, TIGTA performed an audit covering information technology architecture. In our audit of the *Criminal Investigation e-Crimes labs*, we found that [REDACTED]

[REDACTED]. To address the workspace requirements, e-Crimes section management proposed a consolidation of the number of e-Crimes labs using the existing regional area infrastructure and leaving two to three labs in each of the eight regions. The e-Crimes section does not have a definitive completion date because it is seeking to reduce the number of lab locations through employee attrition. An e-Crimes official stated that the consolidation would take at least five years to complete. We reviewed the December 2019 proposal for the nationwide reduction and consolidation of e-Crimes labs. The proposal states the desired lab locations for the consolidation and that the unconsolidated labs will be eliminated as opportunities arise.

The e-Crimes section proposal states that the consolidation would reduce overhead costs, such as utilities, equipment, and facility rental fees, but it did not quantify the costs or any potential savings from the consolidation effort. The estimated project costs are \$7 million and the annual rent is \$2.6 million. These estimates projected costs for incorporating locations into existing space acquisitions, but Facilities Management and Security Services organization personnel

---

<sup>76</sup> Thirty-eight plus 53 equals 91 confirmed workstations without the EDR solution.

<sup>77</sup> Thirty-three plus 6,999 equals 7,032 workstations without a known explanation for why the EDR solution is not deployed.

stated those estimates might increase or decrease once the acquisition is finalized. Further, they had not identified any potential cost savings because it had not fully estimated the costs for all of the physical and environmental requirements for the new e-Crimes labs.

## Human capital

Mission-critical skill gaps across the Federal workforce pose a high risk to the Nation because they impede the Government from cost-effectively serving the public and achieving results. Implementing effective information technology workforce planning practices can better position the IRS to address human capital risks. Accordingly, the GAO identified four key information technology workforce planning practices and supporting activities detailed in various laws enacted and guidance issued over the past 20 years that call for agencies to perform workforce planning activities. These key practices include: 1) setting the strategic direction for workforce planning, 2) analyzing the workforce to identify skill gaps, 3) developing strategies to address skill gaps, and 4) monitoring and reporting on progress in addressing skill gaps.

During Fiscal Year 2021, TIGTA performed two audits covering human capital. We initiated an audit<sup>78</sup> to ***determine whether the IRS's implementation of streamlined critical pay authority in the IT organization conforms to established laws, policies, and regulations.*** The ongoing streamlined critical pay authority activities were compliant with the requirements of TFA § 2103, *Streamlined Critical Pay Authority for Information Technology Positions*, related policies, and regulations. As of February 22, 2021, the IRS had filled seven vacant positions, *e.g.*, Enterprise Operations Associate CIO, Senior Data Architect, and is in the process of filling three more positions, *e.g.*, Chief Technology Officer, Technical Integration Director, under its current authority. Specifically, the IRS Commissioner approved the streamlined critical pay candidate packages for all seven appointees in Calendar Year 2020 and each package contained the required information, *e.g.*, a position description, a resume, an appointment justification (including a rationale for compensation and incentives), and an organizational chart.<sup>79</sup>

The streamlined critical pay position descriptions created (new or updated from existing positions) generally reflected the need for more advanced technical skills and experience. According to the IRS, nine of these positions already existed and required their positions to be updated to reflect new technical skills and skill experience requirements. The remaining position, Senior Data Architect, was newly created to fill an identified organizational need, which required the development of a new position description.

In addition, the four-year appointment terms were clearly stipulated in the Final Offer letters and compensation limits were followed. We reviewed the Final Offer letters for all seven streamlined critical pay appointees and found that each letter stated that the appointment term limits would be no longer than four years. In addition, each appointee's initial annual salary offerings appear to be appropriate, and the total compensation (including salary, plus any recruitment incentive, potential performance bonus, *etc.*) was under the \$253,300 limit for Calendar Year 2020.

---

<sup>78</sup> TIGTA, Report No. 2021-25-032, *Streamlined Critical Pay Authority for Information Technology Positions Is Being Successfully Implemented* (May 2021).

<sup>79</sup> Although the streamlined critical pay candidate packages did not include an organizational chart, each of them included a description of the position's location in the IT organization and to whom they would report.

None of the seven appointees were previously employed at the IRS, and the preliminary background and tax compliance checks were completed prior to hiring them. We reviewed the resumes and searched the Separated IRS Employee File and did not identify the appointees having any prior IRS employment. We also validated the tax compliance check results by using the Integrated Data Retrieval System to examine the Individual Master File tax module information for Tax Years 2015 through 2019. The overall tax compliance ratings for all seven appointees were accurate at the time the tax compliance results were generated.

In addition, we initiated an audit<sup>80</sup> to ***evaluate the IRS's efforts to hire and retain skilled IT organization personnel***. We found that hundreds of skilled employees are nearing retirement eligibility. Specifically, we identified 619 employees who are eligible for retirement within the next three years and there are no other employees with these same skill levels in the IT organization. Collectively, the employees account for 13,520 expert-level skills. The Human Capital Office provided a November 2020 report with recommendations to the IT organization for consideration, including focusing on training and the transfer of knowledge, especially in the area of legacy system programming, to mitigate the risk of losing retirement-eligible employees with expert skills.

We also found that skill gap report reviews and mitigation are not required. The Human Capital Office identifies technical skills of IT organization employees by performing skills assessment surveys. The skill gap reports summarize the skills captured in the skills assessment surveys. While the surveys include both mission-critical and nonessential skill questions<sup>81</sup> as defined by each IT organization function, the skill gap reports only include the mission-critical skills from the skills assessment surveys. The IT organization has identified 14 mission-critical skills,<sup>82</sup> which vary based on the specific needs of each function. Each mission-critical skill is made up of multiple competencies, and each competency is made up of multiple questions. The skill gap reports compare an individual's skill level in a particular area to the industry's standard and identifies strengths as well as deficiencies.

The Human Capital Office shares the skill gap reports with IT organization management, which is accessible by front-line managers. However, the IT organization does not require managers to review all employees' skill gaps in the reports. We judgmentally sampled 12 (33 percent) of 36 managers to evaluate whether the managers review the skill gap reports. Of the 10 responses we received, only two managers said that they track and review all skill gaps related to each employee's job duties, and eight said they did not. In addition, we analyzed the skill gap reports for 335 employees hired during Fiscal Year 2020 to determine whether the IT organization hired qualified individuals to perform their job duties based on mission-critical skills.<sup>83</sup> As of August 21, 2020, 281 (84 percent) employees have deficiencies in one or more mission-critical skills, and 54 (16 percent) employees have no deficiencies. Of the 335 employees, 82 (24 percent) have deficiencies in all mission-critical skills for their IT organization functions. If managers do not address skill gaps, their employees may not

---

<sup>80</sup> TIGTA, Report No. 2021-20-028, *Opportunities Exist to Improve Hiring and Retaining Employees With Information Technology Expertise* (June 2021).

<sup>81</sup> The term mission-critical skills is interchangeable with technical parts.

<sup>82</sup> The 14 mission-critical skills are: Acquisition, Architecture, Cybersecurity, Data Analysis, Finance, Information Systems, Policy and Law, Process Improvement, Project Management, Software, Strategic Planning, System Development, Technical Services, and Technical Support. Software is not included in the skill gap reports.

<sup>83</sup> We did not validate the accuracy and reliability of the data within the skill gap reports.

meet job requirements or further develop the skills needed for their positions to enable the IT organization to effectively and efficiently meet its mission.

According to Human Capital Office management, they work with IT organization management to develop skill gap mitigation reports. The reports summarize skill gaps at the function level and outline how the functions need to address their deficiencies, *e.g.*, through training, by level of importance. However, the IT organization does not require all functions to participate in skill gap mitigations. As a result, one of the functions did not participate in the skill gap mitigations and has yet to agree to participate. According to Human Capital Office management, instead of participating in the mitigations, the function identified its own workforce concerns. If there is no requirement for complete mitigation participation across the IT organization, each function may create its own solution, or not have any solution, which would reduce the impact of collaboration efforts between the Human Capital Office and the IT organization.

In addition, Career Connector templates (hereafter referred to as job announcement templates) are detailed and reviewed timely. We selected a judgmental sample of 10 job announcement templates from an inventory of 360 templates in active status as of July 2020 to determine whether the content in the templates is specific enough to ensure that applicants meet the general qualifications. We also evaluated whether the IRS regularly reviews the job announcement templates to account for any changes, such as changes in occupation, to ensure that the templates are still relevant to the IT organization. We reviewed a job announcement template report with an active status of templates between January 2015 and December 2020 (which included eight templates from our judgmental sample). We determined that the templates were sufficiently detailed to target the job skills necessary for the positions and that the Human Capital Office is timely reviewing and updating job announcement templates.

In our audit of *skilled IT organization personnel*, we also found assessments that may assist in hiring qualified employees are not performed. Specifically, we determined that interviews are not conducted. According to IRS management, the IT organization primarily used surge hiring as a strategy along with direct-hire authority<sup>84</sup> to target filling 2,427 positions from Fiscal Years 2017 through 2019. Human Capital Office management stated that surge hiring was created by the IT organization in Fiscal Year 2017 to fill critical information technology and Cybersecurity function positions as well as to support tax reform legislation.<sup>85</sup> Surge hiring entails submitting a small number of job announcements for a large number of positions across multiple IT organization functions. The first surge hiring process occurred between December 2016 and January 2017. In March 2018, the IT organization initiated a nearly two-year-long surge hiring process, which included direct-hire authorization to streamline hiring external employees to support changes needed for tax reform legislation. The last stage of the hiring surge began in August 2019 to fill the remaining positions for Fiscal Year 2019. Figure 11 summarizes the timeline of significant IT organization hiring initiatives.

---

<sup>84</sup> It allows Federal agencies to fill vacancies in specific occupations, grade levels, and locations when there is a proven critical hiring need or a severe shortage of candidates. It also allows for an abbreviation of the normal hiring process.

<sup>85</sup> Tax Cuts and Jobs Act of 2017. Pub. L. No. 115-97. Officially known as "*An act to provide for reconciliation pursuant to titles II and V of the concurrent resolution on the budget for Fiscal Year 2018.*"

**Figure 11: Timeline of IT Organization Hiring Initiatives**

Date	Hiring Process	Targeted Positions to Fill	Purpose
December 2016 – January 2017	Surge	981	Hiring in anticipation of potential freeze on Federal hiring in Fiscal Year 2017.
March 2018 – December 2019	Surge	1,446	Multipurpose, including hiring of critical information technology and Cybersecurity function positions and to support tax reform.
August 2018 – December 2019	Direct Hire	426 (subset of the 1,446)	Support for tax reform.
August 2019 – September 2019	Surge	200 (subset of the 1,446)	Accelerated push to complete the hiring surge before the end of Fiscal Year 2019.

Source: TIGTA analysis of IT organization hiring initiatives.

Human Capital Office management stated that the IT organization did not perform interviews during these hiring surges. The IRS decided to omit interviews in these cases and focus on assessing the written materials submitted by each applicant. The IRS accepted the risk of having limited information to assess applicants to mitigate the risk of having critical positions left vacant. We interviewed six of 11 IT organization managers who were assigned new employees hired in Fiscal Year 2020 who no longer work at the IRS to discuss their experience with the hiring process and whether or not these departed employees were qualified for the positions. Three of the managers stated that the employee was not interviewed, one manager considered a telephone discussion with the employee an interview, and two managers did not know whether an interview was performed. All the managers we interviewed stated that these new employees were qualified for their positions.

Also, the IT organization does not administer pre-employment skills assessments (hereafter referred to as hiring assessments as defined by the IRS) whereby an applicant must demonstrate job qualifications, although the IRS requires hiring assessments for some positions in other business units. These assessments allow for the demonstration of skills and experience based on actual simulations and could help determine job applicant skillsets prior to hiring. Currently, IT organization job applicants respond to multiple choice questions related to their qualifications and experience to help determine their qualifications. Management stated that they do not need to use hiring assessments to verify an applicant's qualifications because the IT organization is meeting its business needs.

The lack of interviews and hiring assessments may have contributed to employees being hired with mission-critical skill gap deficiencies. For example, project management is one of the mission-critical skills identified in all IT organization functions. If the IT organization interviewed applicants and administered hiring assessments, the hiring managers could consider whether an individual has project management skills prior to being hired. While it is unlikely that all skill gap deficiencies can be eliminated, interviews and hiring assessments may allow the IRS the opportunity to hire individuals who possess more of the mission-critical skills required.

Further, the retention strategy focuses on employee engagement. One way to effectively use limited resources is to retain those employees who possess the necessary skills and expertise the agency requires to meet its mission. The IRS implemented a Service-wide engagement strategy,

*FY [Fiscal Year] 2019-2021 Leadership Engagement Action Plan*,<sup>86</sup> which provides meaningful engagement actions that all business units should accomplish. The plan focuses on the Office of Personnel Management's recommended engagement themes of recognition and empowerment, motivation, diversity and inclusion as well as communication. As a result of the plan, the IT organization developed its *FY [Fiscal Year] 2020 Employee Engagement Action Plan*, which is updated annually based on the Federal Employee Viewpoint Survey results.

The IRS may consider a retention incentive if the unusually high or unique qualifications of the employee or a special need for the employee's services makes it essential to retain the employee, and the employee would be likely to leave the Federal service in the absence of a retention incentive. The IRS has several factors it must consider before authorizing a retention incentive, including special or unique competencies required for the position and the extent to which the employee's departure would affect the IRS's ability to carry out an activity, perform a function, or complete a project that the IRS deems essential to its mission. In the last six years, the IRS approved use of its retention incentive policy for two IT organization employees; the first request was in December 2014, and the second request was in August 2020 (both for a one-year period). We reviewed the retention incentive request forms and verified that the IRS documented the factors it believed warranted the authorization of the retention incentives.

According to Human Capital Office management, the retention incentive policy has not been used frequently in recent years due to budget constraints. A loss of employees with expert-level skills could negatively affect the IT organization's ability to meet its mission. It could lead to insufficient staff to address system security issues and perform necessary system maintenance and upgrades as well as develop modernized tools and systems to enhance tax administration.

## Project management

Project management is the discipline of using established principles, procedures, and policies to manage a project from conception through completion. It is the application of knowledge, skills, tools, and techniques to activities to meet the project requirements. It is also the process of defining and achieving goals while optimizing the use of resources, such as people, time, and money during the course of a project.

In Fiscal Year 2021, TIGTA provided coverage of information technology project management in four audits. We initiated an audit<sup>87</sup> to ***evaluate the implementation of the Data at Rest Encryption (DARE) Program***.<sup>88</sup> We found that progress has been made to identify and test encryption and key management solutions. The DARE Program developed a roadmap, which is a five-year plan (Fiscal Years 2019 through 2023), for establishing encryption solution standards and an enterprise key management solution. The roadmap included a framework to identify, classify, and group systems so that potential encryption solutions could be identified. We determined that the DARE Program used this framework to identify system attributes, such as platform technology, programming language, and data format, and created natural groupings of systems, called technology clusters. As a result, these technology clusters could be potentially addressed by a single encryption solution.

---

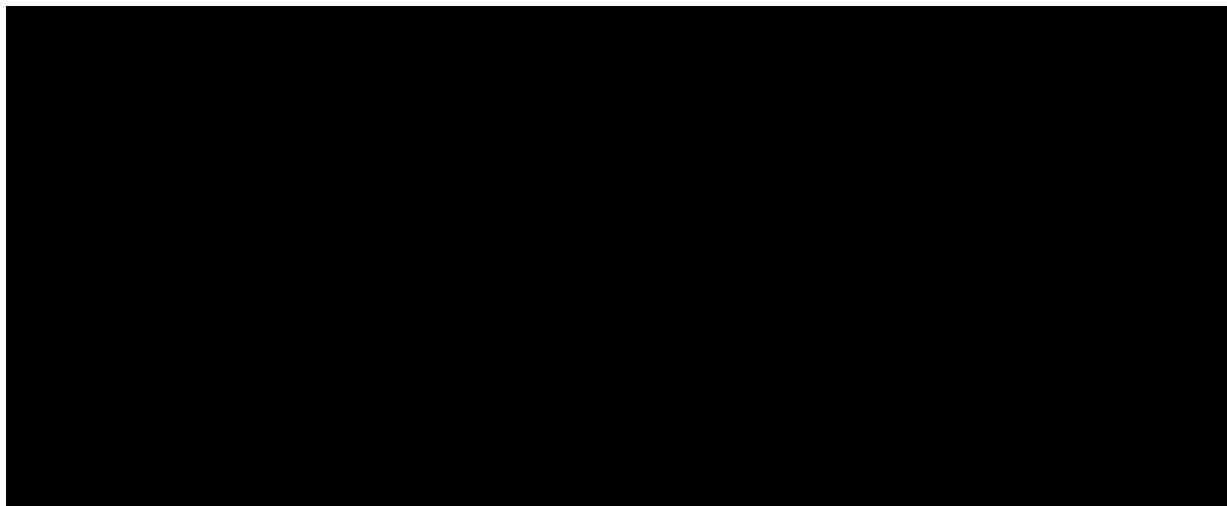
<sup>86</sup> Dated October 1, 2018.

<sup>87</sup> TIGTA, Report No. 2021-20-066, *The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement* (Sept. 2021).

<sup>88</sup> The DARE Program was created to address the need for encryption to protect data across the IRS enterprise.

The creation of technology clusters enabled identification and categorization of the diverse types of databases/platforms in use across the enterprise. The DARE Program used the technology cluster information to identify potential encryption solutions by performing market research and identifying potential commercially available encryption and key management solutions for each cluster. Figure 12 shows the four primary groupings of systems requiring encryption identified by the DARE Program as well as the identified key management solutions and technology clusters that could utilize similar encryption agents.

**Figure 12: DARE Key Management Solutions and Technology Clusters**



*Source: DARE Strategy Chief Information Officer Brief, dated March 9, 2021. AWS – Amazon Web Services, COTS – Commercial-Off-The-Shelf, EKMF – Enterprise Key Management Foundation, HVA – High Value Asset, IBM – International Business Machines, and KMS – Key Management System.*

The DARE Program identified 15 technology clusters and related encryption and key management solutions to select systems for testing. It then conducted an Analysis of Alternatives<sup>89</sup> to select a key management solution, *i.e.*, the Oracle Transparent Data Encryption solution with integration to the Thales key management system, which was tested during the proof-of-concept process.

In our audit of the **DARE Program**, we also found that encryption plans have been delayed. By the summer of Calendar Year 2020, the DARE Program was in the process of planning for the *IRS Integrated Modernization Business Plan* activity of deploying a DARE Full Operating Capability by September 30, 2021. To meet this commitment, the DARE Program has to deploy an encryption solution and key management solution into production, and then use them to successfully support [REDACTED]. However, in the summer of Calendar Year 2020, the DARE Program was also tasked with a new priority to encrypt data on High Value Assets along with the work already in progress to deploy the DARE Full Operating Capability. The requirement to encrypt High Value Assets came from the Treasury Department as one of its initiatives to focus on cybersecurity across the Department. The IRS has [REDACTED]

---

<sup>89</sup> An analytical comparison or evaluation of proposed approaches to meet an objective. The formal or informal process involves identifying key decision factors, such as life cycle operations, support, training, and sustaining costs, risks, effectiveness, and assessing each alternative with respect to these factors.

██████████. The IRS informed the Treasury Department that it would encrypt all High Value Assets by September 2026, and subsequently, the decision was made to encrypt the ██████████ by ██████████.

We identified specific program issues that have affected the DARE Program's ability to meet its goals. Specifically, the DARE Project did not follow various enterprise life cycle requirements. These include combining milestone exit reviews for multiple phases instead of conducting the reviews separately as required, and not timely updating significant artifacts as required. The enterprise life cycle is used to ensure consistency and compliance with Government and industry best practices by information technology projects. There are various enterprise life cycle paths available for information technology projects, which are to be agreed upon at the start of new projects and documented in a Project Tailoring Plan. Figure 13 shows the descriptions of the phases, along with their related milestone numbers.

**Figure 13: Enterprise Life Cycle Phases**

Phase Name	Description	Milestone
Vision and Strategy/Enterprise Architecture	High-level direction setting.	Milestone 0
Project Initiation	Define project scope, form project teams, and begin many enterprise life cycle artifacts.	Milestone 1
Domain Architecture	Gather, develop, and approve solution concept, requirements, and architecture.	Milestone 2
Preliminary Design	Development of logical design.	Milestone 3
Detailed Design	Development of physical design.	Milestone 4a
System Development	Coding, integration, testing, and certification of solution/system.	Milestone 4b
System Deployment	Expand availability of solution to all target environments and users.	Milestone 5

*Source: Internal Revenue Manual 2.16.1, Enterprise Life Cycle, dated July 10, 2017.*

The commercial-off-the-shelf path was chosen for the DARE Project. This path provides guidance when pre-packaged, vendor-supplied software is to be used with little or no modification to provide all or part of a solution. While there are multiple sequential phases in this enterprise life cycle path, it is common practice to combine the first two phases (Project Initiation and Domain Architecture) with a single milestone exit for both. In addition, because it is based on using commercial software, both design phases (Preliminary and Detailed Design) typically can be combined with a single milestone exit. However, during the tailoring process, it was agreed that the DARE Program would have a single milestone exit for Milestones 1 through 4a. This has the practical effect of deferring reviews of the milestone exit requirements until the project is at the end of the development phase. This could cause unnecessary delays if there were any adjustments or decisions about the design or scope of the project that needed to be addressed earlier. Subsequent to our discussions with DARE Program management and the Enterprise Life Cycle Office, this approach was revised and an updated Project Tailoring Plan was issued in March 2021 requiring milestone exit reviews at Milestone 1/2 and Milestone 3/4a.

In addition, significant enterprise life cycle artifacts were not updated as required. For example, the Project Charter, Project Management Plan, and Project Tailoring Plan were not updated to reflect the inclusion of High Value Asset-related work in the project scope. Artifacts are used by a project to document how it plans to meet standards and requirements, and are usually in the form of documents based on pre-established templates. In addition, a revision of the original Project Management Plan did not contain information related to the change in scope. Further, the DARE Business System Report was not completed and approved.<sup>90</sup>

All of these artifacts were prepared in June and July 2020 when the project entered into the enterprise life cycle process. However, they reflect the original project scope prior to High Value Asset encryption-related work being prioritized. These artifacts were still not updated by the end of April 2021. We believe that proceeding to the development phase prior to completing the design or architecture phases could create confusion and uncertainty if the artifacts do not accurately reflect the current project scope, thus reducing their effectiveness and usefulness for project management and resulting in unnecessary delays.

In our audit of the *DARE Program*, we also identified that development of the Integrated Master Schedule was delayed. It took approximately eight months to create the initial baseline, *i.e.*, approved version. While the schedule was being approved through the governance process, the project used the un-baselined schedule to track and manage program activities. The baseline Integrated Master Schedule is meant to be the starting point from which all project activities are managed.

In June 2020, the IRS entered into the enterprise life cycle process when it started the development of the Integrated Master Schedule based on the scope of the DARE Program at that time. The baseline schedule was not initially approved until February 2021, and the IRS used various ad hoc methods to manage the DARE Program until it was approved. In May 2021, DARE Program management informed us that there were issues with gaps between dependencies and tasks that needed to be addressed, and that the schedule would have to be re-baselined. According to the IRS, the Integrated Master Schedule reviews and revisions were completed in June 2021, and the schedule was formally approved through the governance process on July 29, 2021.

Project management issues contributed to the Integrated Master Schedule delays, including difficulties in obtaining timely, useful feedback from delivery partners as well as having to work with feedback comments based on various versions of the schedule. Based on the extended time taken for this process, we are concerned that the DARE Program has been working on implementing an encryption solution at the same time as developing the related schedule that includes necessary information to effectively manage and measure program progress. Without a baseline Integrated Master Schedule, the DARE Program has no reliable schedule with which to gauge progress or to allocate resources. This increases the difficulty of effectively managing such a large project with multiple interdependencies and could further contribute to delays.

In addition, prior encryption recommendations were not prioritized and could impact the DARE Program's ability to meet deadlines. Prior to March 2021, the priority was to deploy the DARE

---

<sup>90</sup> The report serves as the primary reference for all project requirements for the project and is supposed to be completed and approved prior to exiting the Architecture phase (Milestone 2). Subsequent phases, such as Design (Milestones 3/4a), Development (Milestone 4b), and Deployment (Milestone 5), are based on the requirements and scope information in the approved Business System Report.

Full Operating Capability by September 30, 2021. However, in March 2021 the DARE Program was also tasked with additional work unrelated to meeting this priority. Specifically, the decision was made to include addressing prior GAO audit recommendations for encryption of certain systems. Further, Treasury-designated High Value Assets were to be encrypted by [REDACTED].

A GAO report issued in July 2017<sup>91</sup> recommended data on certain systems be encrypted. IRS management neither agreed nor disagreed with the recommendations, but stated they would review each of the recommendations and ensure that corrective actions include sustainable fixes that implement appropriate security controls. The due date for the planned corrective actions was originally May 15, 2020, but was extended to May 15, 2022. According to the IRS, initial DARE planning in Calendar Year 2018 for proof-of-concept testing specifically indicated that the focus should be on the systems mentioned in the GAO report, and one system had proof-of-concept testing in November 2019. However, the work to address the planned corrective actions was not made a priority until March 2021.

Although the IRS prepared a briefing for the GAO about DARE Program progress in March 2020, this briefing did not include information about addressing the GAO recommendations during Calendar Years 2020 or 2021. [REDACTED]

[REDACTED]. However, significant additional work is also needed to ensure that the encryption of the systems in question is accomplished timely. Prior to March 2021, that work was not included as a DARE Program goal or in the Integrated Master Schedule that was in the process of being baselined.

The DARE Program's work on Full Operating Capability and Treasury-designated High Value Assets involves significant planning, testing, and procurement activities in order to meet the associated deadlines. In addition, other activities are in progress concurrently with those efforts, including the creation of an IRS-designated High Value Asset encryption implementation plan and the continuation of testing and development of technology cluster solutions. The DARE Program was aware of the need to address the GAO recommendations as early as Calendar Year 2018, but did not make it a priority until March 2021, when the deadline for closing the corrective actions was approaching. The notional schedule to address the GAO recommendations is very aggressive and could directly impact the DARE Full Operating Capability deployment and High Value Asset encryption plans. Therefore, delays with determining the priority of work related to the GAO recommendations could have significant negative impacts on these efforts.

We also initiated an audit<sup>92</sup> to ***review the Enterprise Case Management (ECM) Program<sup>93</sup> migration efforts***. The ECM Program developed a formal sequencing plan, which provides a documented, repeatable method to select business processes for migration prioritization, through Fiscal Year 2022. The selected processes are intended to balance near-term business

---

<sup>91</sup> GAO, GAO-17-394SU, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).

<sup>92</sup> TIGTA, Report No. 2021-20-059, *Enterprise Case Management Deployed Its Initial Release, but Process Improvements Are Needed for Future Releases* (Sept. 2021).

<sup>93</sup> For this report, the ECM Program includes the Enterprise Digitization and Case Management Office, the ECM Initiative, and the IT organization's ECM Program Management Office.

value, leadership priorities, and long-term scalability, while working to establish operational footprints within IRS organizations.

In September 2020, the ECM Program made its first partial product deployment with Release 1.0 to the Tax-Exempt and Government Entities Division's Exempt Organizations Correspondence Unit and full deployment in December 2020 with Release 1.1. As of April 2021, the ECM Program has deployed two updates providing additional functionality and software patches, and is on schedule to deploy Release 2.0 to the Wage and Investment Division's Grants Management process. The releases and updates spanned the ECM Program's Release 1.0 and 2.0 plans. In April 2021, the Release 3.0 plan received approval and includes 10 areas, *e.g.*, the Human Capital Office's Labor Relations processes, Taxpayer Advocate Service's Grants Management process, for development. In addition, the ECM Program identified six processes, *e.g.*, Taxpayer Advocate Service's Case Advocacy, Wage and Investment Division's Linguistics Policy, Tools, and Services, for migration into the ECM solution. The proposed processes were approved for analysis and exploration and will be worked throughout Fiscal Year 2022 as ECM Program capacity allows.

However, the ECM Program has not finalized its scaled agile framework configuration. The IRS's *Reference Guide: ECM Enterprise Life Cycle/SAFe [Scaled Agile Framework®]<sup>94</sup> Delivery Optimization<sup>95</sup>* states that ECM Program management obtained approval to move from a waterfall delivery method to the scaled agile framework for software development. The framework provides four configuration options<sup>96</sup> allowing organizations to adapt the framework to meet their business needs. Each configuration option incorporates parts of seven core competencies required for business agility.

The ECM Program stated that it is implementing a combination of two scaled agile framework configurations, trying to strike a balance between implementing the recommended roles and configurations while minimizing unnecessary overhead. Performing assessments could help determine which of the four framework configuration options to use. Failure to identify and implement the appropriate scaled agile framework elements could result in delays in product delivery and reduced productivity, product quality, and customer satisfaction. In January 2021, an ECM Program team with contractor support began reporting quarterly results on their evaluation of how the program aligns with agile best practices. The quarterly reports, along with internal reviews, are being used to evaluate the current scaled agile framework configuration.

Also, while some best practices are in place, there are areas for improvement. In July 2020, the contractor issued its final report, *Independent Verification and Validation of the ECM Program*, and stated that the ECM Program has yet to finalize a roadmap to achieve its goals between Calendar Years 2020 and 2022. Specifically, the team has not created a roadmap to achieve its goals that can guide prioritization, plan for resourcing, encourage team collaboration, or help with features/functionality to include in Release 1.0 to prevent rework. In addition, the report did not provide an in-depth validation of the ECM Program cost estimates, but stated that costs have historically and on average been approximately 10 percent under budget. The report also stated that the ECM Program has a high-level, independent cost estimate through

---

<sup>94</sup> Scaled Agile Framework and SAFe are registered trademarks of Scaled Agile, Inc.

<sup>95</sup> Dated November 2020.

<sup>96</sup> The Essential configuration is the simplest version with basic core competencies. The Portfolio configuration incorporates lean portfolio management. The Large Solution configuration includes multiple simultaneous teams for complex solutions. The Full configuration is comprehensive for multiple large, integrated solutions.

Fiscal Year 2024 and expects the ECM Program commercial off-the-shelf platform to be established with all core case management capabilities and data integration enabled.

The contractor also evaluated 10 factors across multiple areas of the ECM Program based on detailed criteria to develop a scorecard. The contractor conducted assessments from April through June 2020 via a series of interviews with all levels of staff, surveys, and a review of documentation. The Independent Verification and Validation report stated that the ECM Program had met or exceeded all relevant best practices in six of the 10 areas examined and met many of the best practices in the remaining categories. The best practices met include a clear articulation of the vision and high-level objectives in program material, *e.g.*, ECM long-term strategy, program charter; development of roles for the in-house management of the overall program and the product expertise from an experienced system integrator; and careful delineation of which aspects of the case management system could be moved into the cloud or remain on premise. In addition, the report specifically identified areas for improvement: program benefits are defined only in broad terms and lack specificity and the ECM Program has yet to implement all necessary characteristics of a high-performing agile program or finalize a roadmap to achieve its goals between Calendar Years 2020 and 2022.

The Independent Verification and Validation report also stated that ECM Program benefits defined in broad terms lack granular, quantified benefits and will make it difficult for leadership to manage continuous implementation of processes over a long period of time, identify tradeoffs in competing priorities, and evaluate success. In addition, the report identified significant needs in the areas of making project benefits and the functionality required to enable them to be more widely understood, prioritizing the most valuable functionality, and quantifying benefit drivers financially or with metrics.

To address the findings from the Independent Verification and Validation report, the ECM Program conducted self-assessments of the best practices identified in the report in January and March 2021 and compared the results to the original independent verification and validation assessment. In the first quarterly report in February 2021, the ECM Program identified improvement in two of the best practice areas. It prioritized establishing a minimum viable product prior to beginning configuration work, identified the project scope for the next 12 months, including Releases 2.0 and 3.0, and started a process to identify outcomes aligned to benefits at the business process level.

In the April 2021 quarterly report, the ECM Program highlighted the addition of a weighted-shortest-job-first score to prioritize work based on business benefits and job size; development of a long-term strategy with objectives, measures, and metrics aligned to each program strategic goal; and development of a decommissioning process that will quantify financial benefits related to system retirement. Gaps that still need to be addressed include quantifying benefits with a return on investment; identifying benefits from new functionality; and aligning the ECM Program life cycle cost estimate to program benefits or metrics.

In our audit of the *ECM Program*, we found that the Program identified lessons learned from the Release 1.0 deployment. Specifically, end users were not fully integrated into the development process. In April 2019, the ECM Program had Tax-Exempt and Government Entities Division end users take part in a Blue-Sky Program<sup>97</sup> to help determine and prioritize

---

<sup>97</sup> A design session held by the ECM Program with Tax-Exempt and Government Entities Division personnel to identify opportunities for improvement in the Correspondence Unit process.

operational requirements. The end users came away with the expectation that the initial release of the ECM tool would include the ability to access, read, and update datasets. However, that functionality was not included with the December 2020 release, and was partially incorporated into the ECM solution with Release 1.2 in January 2021.

During our interviews with end users, they expressed frustrations with the ECM deployment. These frustrations were due to two primary issues: poor communication regarding changes in expected functionality between the Blue-Sky Program and the release as well as inadequate training. Release 1.1 functionality could not read or edit data as originally expected and the change in functionality was not communicated to end users prior to the release. Despite multiple updates, as of April 2021, the system still requires end users to use workarounds for retrieving and updating data. The workaround requires end users to capture screenshots from the legacy database and record the activity in the ECM tool. The ECM Program identified the potential risks of not providing access to legacy data through the ECM solution as reduced work efficiency, minimal process improvement, and undermining end users' perception of the program.

In response to lessons learned during Release 1.0 and because different teams play lead roles in different stages of the process, the ECM Program created the role of a Customer Journey Advocate. This individual provides hands-on support and guides customers through the process from preparing for migration to the new ECM tool to the decommissioning of legacy systems. The ECM Program has also worked to incorporate the end user earlier in the process. For example, during the ECM Program's implementation of the Expedited Delivery Process, end users were provided a test environment in which they are able to use development versions of the software. The ECM Program found this process so beneficial that it incorporated the process into ECM Release 2.0.

Another lesson learned resulted from the ECM Program identifying significant Section 508 defects when it deployed Release 1.1. Section 508 of the Rehabilitation Act of 1973<sup>98</sup> requires Federal agencies to make their electronic and information technology accessible to people with disabilities. On December 9, 2020, just prior to deployment of Release 1.1, ECM Program reports identified 153 total internal defects, of which 76 (50 percent) were for Section 508 compliance.<sup>99</sup> In April 2021, 184 Section 508 compliance internal defects were reported.

The ECM Program stated that IRS development programs traditionally address Section 508 compliance during the testing phase, but it is trying to address compliance earlier in the development process for future releases. The ECM Program identified a lesson learned to allocate sufficient time during program increments to configure, test, and fix defects to avoid a significant number of defects in the backlog going into production. To reach this goal, it is attempting to allocate sufficient resources to complete all defect testing, provide time during program increments for defect remediation, and provide time during the iteration for simultaneous configuration and testing. The ECM Program also implemented additional steps to develop software with Section 508 compliance for Release 2.0. As of February 2021, these

---

<sup>98</sup> 29 U.S.C § 794 (d).

<sup>99</sup> The ECM delivery team can address internal defects by implementing fixes. External defects require the solution provider to release a new version or upgrade of the software to fix the defect. In addition to the internal defects, there were 81 external defects identified in December 2020 and 107 external defects identified in April 2021.

steps included utilizing Section 508 checklists by developers during development and unit testing, and adding a rule to warn developers if a label is missing on any user interface elements.

In addition, the ECM Program introduced an Accessibility Advocate function. The ECM Program stated that this team will work together with the IT organization's Information Resources Accessibility Program, which provides centralized leadership of Section 508 defect analysis and remediation, expertise in configuration, tailored training, and coordination of user groups. The Accessibility Advocate is expected to assist the Information Resources Accessibility Program in reducing the number of Section 508 defects in future releases; improve the user experience; reduce downtime with resulting increases in productivity; and reduce or avoid settlements, grievances, and lawsuits.

The ECM Program is making progress towards its decommissioning strategy. It has completed an initial inventory of legacy case management systems and tools that includes functional needs, systems dependencies, and other relevant information which will drive prioritization; deep dive discussions; and recommendations for sequencing, migrating, and ultimately decommissioning. In April 2021, the ECM Program completed a *Draft Enterprise Case Management Decommissioning Strategy*<sup>100</sup> to enable and expedite the retirement of legacy case management systems. The strategy lays out a repeatable process for planning and executing decommissioning, while mitigating the risks associated with system shutdowns.

The ECM Program also developed a Decommissioning Prioritization Tool that works to identify early decommissioning opportunities and align them with the sequencing plan. The tool evaluates legacy case management systems data to determine the estimated level of effort to decommission the system and the value it will bring to the IRS. The results are plotted on a graph for a clear visual representation. The input data include several variables that can be adjusted to meet changing priorities. A technical analysis of the results is performed and a Decommissioning Recommendation Package is provided to the sequencing team. A Decommissioning Cost Funding Model, Business Process Heat Map, and Decommissioning Roadmap are all in various stages of development. The ECM Program expects to decommission three components of a major case management system this calendar year.

In our audit of the *IRS's implementation of the CIO's duties and responsibilities*, we found that the IT organization arranged for an independent verification and validation assessment for the Customer Account Data Engine 2 and the ECM implementation plans as required. We reviewed the Independent Verification and Validation reports for the Customer Account Data Engine 2 and the ECM applications and were able to confirm that the IRS engaged a contractor to perform an independent verification and validation of both implementation plans, and that it received the contractor's reports prior to the deadline of July 2020 as established in the TFA. The contractor concluded that, if the IRS uses the opportunities presented in its reports, the IRS would be on track to complete both projects on time and on budget. According to the CIO, the IT organization has presented the independent verification and validation results to the IRS Senior Leadership Team and the Treasury Department.

In our audit of the *IVES Program*, we found that the IRS is in the early stages of developing an online system to replace the current manual IVES Program transcript request process. The system will replace the IRS's current partially automated system, which requires employees to

---

<sup>100</sup> Dated April 26, 2021.

manually process transcript requests received from IVES Program participants. Under the current system, clerks in the IVES Program units receive Forms 4506-T on dedicated fax machines, print and batch the forms, and input information from the forms into the Transcript Delivery System. The transcripts are then systemically delivered to IVES Program participants' secure electronic mailboxes. Once implemented, this new system will eliminate the manual processes that require clerks to print and manually input each form in the Transcript Delivery System.

The TFA requires the IRS to modernize its IVES Program for disclosure of taxpayer information for third-party income verification by January 1, 2023, and the IRS expects to meet this deadline. For example, the IRS has developed a high-level solution concept for the new system detailing the business process flow and system requirements. In October 2020, the IRS began the architecture and engineering design phase of its project development cycle and prepared a high-level system development and implementation schedule. However, the cost to develop the online system has not been finalized and a significant shortfall already exists in the estimated user fees to be collected to cover the development costs.

TFA § 2201, authorizes the IRS to charge a separate user fee over a two-year period (Calendar Years 2020 and 2021) to fund the development of the new system. The fee can be charged for any qualified transcript request, *i.e.*, a request used to verify the income or creditworthiness of a taxpayer that is a borrower in the process of a loan application. Once the new system design is finalized, the IRS will produce the final cost estimate. However, without knowing the final cost, the IRS cannot accurately calculate a user fee and must rely on estimates.

To establish the user fee amount, the IRS developed a preliminary cost estimate of \$75.3 million to develop and deploy the new IVES Program system. The IRS also analyzed IVES Program historical transcript request volumes and worked with the IVES Program Participant Working Group to estimate that 12 million Forms 4506-T would be submitted to the IVES Program in Fiscal Year 2020. Based on these estimates, the IRS increased its transcript request fee from \$2 to \$5 starting on March 1, 2020. The fee increase was expected to raise \$36 million in the first year, which is nearly one-half the \$75.3 million estimated cost to develop the new system. However, as of July 31, 2020, the IRS spent more than \$9.3 million developing the new system and collected approximately \$6 million in fees. This amount is well below the estimated fee revenue of \$36 million expected for the first year. The significant shortfall is a direct result of the COVID-19 pandemic. For example, the IVES Program was shut down from March 27 until May 18, 2020, and operated at a reduced capacity until returning to normal operations on July 14, 2020. This disruption significantly reduced transcript request processing volumes and fees collected.

## Risk management

Risk management is the process of identifying, monitoring, and mitigating project and program risks. Effective risk management emphasizes the need to integrate risk management into existing business activities of an agency. It can help the IRS, including its IT organization, more securely and effectively administer the Federal tax system by identifying and mitigating emerging risks before they affect performance.

During Fiscal Year 2021, the GAO performed an audit covering risk management. In its audit of the *IRS's internal control over financial reporting*, the GAO identified one deficiency in risk

management related to external system risk assessments. The IRS did not conduct an adequate assessment of risks and controls of an external system.

### Implementation of corrective actions

Internal controls are a major part of managing an organization and provide reasonable assurance that organizational objectives are being achieved. Internal controls protect assets, detect errors, and prevent fraud. Internal controls help Government program managers achieve desired results through effective stewardship of public resources. Systems of internal control provide reasonable assurance that the following objectives are being met: 1) effectiveness and efficiency of operations, 2) reliability of financial reporting, and 3) compliance with applicable laws and regulations.

In Fiscal Year 2021, TIGTA and the GAO performed four audits with coverage on the status of closed planned corrective actions. In our audit of the *IVES Program*, we found that the IRS implemented planned corrective actions to address our prior recommendations. In March 2018, we reported<sup>101</sup> that IVES Program certification requirements are not effective in addressing risks associated with the unauthorized release of tax transcripts to IVES Program clients, and that the IRS does not have processes and procedures to ensure that the legitimate taxpayers signed the Form 4506-T to authorize the release of their tax transcripts. Since our last review, the IRS implemented some security controls to protect taxpayer information from unauthorized disclosure. The IRS:

- Implemented the Secure Access for e-Services, on December 10, 2017, to prevent unauthorized access to taxpayer data. This multifactor authentication process improves security and helps ensure that tax transcripts can only be accessed by authorized IVES Program participants.
- Implemented masking of Personally Identifiable Information from tax transcripts beginning September 23, 2018, to better protect and prevent unauthorized disclosure of taxpayer data. In addition, the IRS created a new customer file number, which is reflected on the redacted transcript that third parties can use as an identifying number instead of the taxpayer's Social Security Number.

In our audit of the *DARE Program*, we found that corrective action to address a previously identified encryption security weakness was not fully implemented. In July 2018, TIGTA reported<sup>102</sup> that end-to-end encryption was not enforced for the transferring of taxpayer data to and from private collection agencies.<sup>103</sup> Specifically, TIGTA identified that taxpayer information used by the private collection agencies was not encrypted by either the IRS or the private collection agencies prior to being transferred. This information is supplied electronically to the private collection agencies so they can attempt the collection of tax debts and the information

---

<sup>101</sup> TIGTA, Report No. 2018-40-014, *Transcript Delivery System Authentication and Authorization Processes Do Not Adequately Protect Against Unauthorized Release of Tax Information* (Mar. 2018).

<sup>102</sup> TIGTA, Report No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018).

<sup>103</sup> On December 4, 2015, the President signed into law the Fixing America's Surface Transportation Act,<sup>1</sup> which included provisions amending Internal Revenue Code §§ 6306 and 6307 pertaining to the use of qualified tax collection contractors to collect inactive tax receivables. To address this legislative mandate, the IRS established a Private Debt Collection Program and selected four private collection agencies. The IRS enabled these designated contractors to collect outstanding inactive tax receivables on the Government's behalf.

about the amounts collected is then returned to the IRS. This taxpayer information is considered data at rest prior to being transferred and is required to be encrypted by both the IRS and the private collection agencies. TIGTA recommended that the CIO ensure that the data at rest be encrypted by the IRS and by the private collection agencies. In July 2019, the IRS closed this recommendation as completed.

Prior to closing the recommendation, the IRS verified the taxpayer information was being encrypted through e-mail verification with the private collection agencies. In addition, the IRS verified encryption of the private collection agencies' data through annual testing established by Publication 4812. The publication defines basic security and privacy control requirements and standards required of contractors and its employees when the contract involves access to, development, hosting, or maintaining of sensitive but unclassified information. Based on this testing, the IRS determined that the private collection agencies were encrypting the taxpayer information as required.

In addition, the IRS completed a feasibility study to determine how it could implement DARE for taxpayer information prior to it being transferred to the private collection agencies. This feasibility study concluded that IRS-based options would require further testing to ensure compatibility. It also concluded that access to necessary resources would need to be obtained to develop and implement any strategy for the encryption of taxpayer data prior to being transferred to the private collection agencies. Based on the feasibility study, the IRS conducted a pilot and determined that it was able to encrypt the data in both the development and test environments. Based on the results of the pilot, the IRS indicated it was planning to encrypt the private collection agency information after it had completed encrypting two other systems. The IRS also stated that the encryption of data was resolved; however, we determined that the private collection agency information residing at the IRS had not been encrypted in production. Until DARE is employed for these sensitive data, it will remain at risk of exposure or unauthorized access.

The GAO initiated an audit<sup>104</sup> to ***determine whether the IRS's financial statements are fairly presented and IRS management maintained effective internal control over financial reporting.*** The GAO reported that while the IRS made progress addressing previously reported control deficiencies, it found continuing and newly identified deficiencies that contributed to the significant deficiency in the IRS's internal control over financial reporting systems. Specifically, deficiencies continue to exist concerning 1) unnecessary access rights granted to accounts, 2) inconsistent monitoring of systems and accounts, 3) inadequately enforced encryption to protect systems and data, 4) out-of-date and unsupported hardware and software, and 5) insufficient implementation and enforcement of effective policies and procedures as part of IRS's security management program.

The GAO also reported that the IRS mitigated the potential effect of these continuing and newly identified deficiencies primarily through compensating controls that management has designed to detect potential misstatements on the financial statements. Nevertheless, these application and general control deficiencies increase the risk of unauthorized access to, modification of, or disclosure of sensitive financial and taxpayer data and disruption of critical operations, which are important enough to merit attention. Continued and consistent management commitment and

---

<sup>104</sup> GAO, GAO-21-162, *Financial Audit: IRS's FY 2020 and FY 2019 Financial Statements* (Nov. 10, 2020). FY = Fiscal Year.

attention will be essential to addressing existing system deficiencies and continually improving the IRS's financial reporting system controls.

In its audit of the *IRS's internal control over financial reporting*, the GAO followed up on the status of the IRS's corrective actions to address control deficiencies in information system and associated recommendations that remained open as of September 30, 2019. The GAO determined that the IRS had completed corrective actions to close 41 of 132 recommendations from its prior audits related to information systems as of September 30, 2020. Closed corrective actions include: audit and monitoring, authorization, boundary protection, configuration management, cryptography, identification and authentication, security management, and separation of duties. Combined with the GAO's five new recommendations, a total of 96 recommendations addressing control deficiencies in information systems remain open as of September 30, 2020.

### Modernizing operations

Successful modernization of systems and the development and implementation of new information technology applications are critical to meeting the IRS's evolving business needs and enhancing services provided to taxpayers. Modernization is necessary to deliver efficient taxpayer services and enforcement with enhanced user experiences.

In Fiscal Year 2021, TIGTA performed two audits covering the modernization of the IRS's operations. In our audit of *private collection agencies*, we found that the IRS implemented programming on January 24, 2020, to systemically exclude accounts of Social Security Disability Insurance recipients from being assigned to a private collection agency, as required starting in January 2021. The IRS informed TIGTA that the new programming reads the annual Social Security Disability Insurance recipient file provided by the Social Security Administration on a weekly basis (annually reported on Form SSA-1099, *Social Security Benefit Statement*). If any Individual Master File taxpayer or their spouse in the IRS's Unpaid Assessments database is receiving Social Security Disability Insurance income, the case is excluded from the Private Debt Collection Program. TIGTA also inquired as to how the IRS would conduct reviews of the inventory to ensure that no Social Security Disability Insurance cases are being assigned to private collection agency inventory. The IRS responded that it created unique reason codes to allow for tracking the recalled or excluded cases and verified that the system is programmed to monitor the private collection agency inventory on a weekly basis using the unique codes to ensure that the Social Security Disability Insurance accounts are not present.

In our audit of the *IRS's implementation of the CIO's duties and responsibilities*, we found that most provisions of TFA § 2101 have been implemented. This includes: 1) the CIO's roles and responsibilities have been defined; 2) the IRS Commissioner appointed a permanent CIO; 3) the CIO oversees the development, implementation, and maintenance of information technology enterprise-wide; and 4) the IT organization developed an *Information Technology Strategic Plan*.<sup>105</sup>

TFA § 2101 specifies that the IRS Commissioner and the Secretary of the Treasury will act through the CIO with respect to the development, implementation, and maintenance of the

---

<sup>105</sup> Dated November 2020.

IRS's information technology. It also defines the general duties and responsibilities of the CIO, requiring the CIO to:

- 1) Oversee the development, implementation, and maintenance of information technology throughout the IRS, including the Taxpayer Advocate Service, Criminal Investigation, and the Office of Chief Counsel.
- 2) Ensure that the information technology is secure and integrated.
- 3) Maintain operational control over the information technology.
- 4) Act as the principal advocate for the IRS's information technology needs.
- 5) Consult with the Chief Procurement Officer on significant information technology acquired.

Although many of these activities were already under the CIO's purview in one form or another, the IRS has taken some steps to further define and implement the CIO's roles and responsibilities. For example, the memorandum issued defining the CIO's roles and responsibilities states that the CIO is responsible for developing, implementing, and maintaining the IRS's information technology, ensuring that the information technology is secure and integrated, maintaining operational control of all information technology, and being the principal advocate for information technology needs. In addition, the IRS Commissioner appointed a permanent CIO in February 2021.

TFA § 2101 requires the CIO to be responsible for the development, implementation, and maintenance of information technology enterprise-wide. For most business units, the IT organization maintains the operational information technology environment and provides information technology services. According to the CIO, some business units may have contracts for software and other information technology, but the CIO oversees the information technology budgets of these business units. This provides the CIO awareness of the information technology products and services that are acquired.

In addition, the IT organization provides oversight of IRS information technology efforts through several governance boards. The IT organization has governance boards over Associate CIO areas of responsibility, such as UNS, Cybersecurity and Privacy, and Enterprise Services. There are also IRS enterprise governance boards, *e.g.*, Executive Risk Committee, Strategic Development Executive Steering Committee, to which the CIO is either a member or co-chair. Further, there are dedicated program governance boards, *e.g.*, the Web Applications Governance Board and the Financial Services Governance Board. The program governance boards govern selected investments and their systems, programs, and projects to ensure that investment, program, and project objectives are met, risks are managed appropriately, and enterprise expenditures are fiscally sound.

The IT organization is also involved in functional governance boards, such as the Criminal Investigation Governance Board. Criminal Investigation chairs this board, and voting IT organization members include representatives from the Cybersecurity, Enterprise Services, and Applications Development functions. The Criminal Investigation Governance Board reports to the Sustaining Operations Executive Steering Committee, which is co-chaired by the Deputy CIO for Operations.

While some business units maintain their own information technology staff, in September 2020, the then acting CIO issued a memorandum to all heads of office that describes the process for business units to fill select information technology positions outside of the IT organization. Specifically, the memorandum sets forth policy that work related to the determination of information technology solutions and investments, cybersecurity, and technology products inherently used in the IT organization should not be staffed from within business units, outside of the IT organization. Further, the memorandum established an annual reporting requirement for business units to report their information technology staffing needs, describing their existing, vacant, and any proposed new information technology positions to the IT organization.

However, Criminal Investigation is an exception to the other business units as it operates its own information technology environment as well as maintains its own information technology staff. In Fiscal Year 2016, the Deputy Commissioner for Services and Enforcement and the Deputy Commissioner for Operations Support signed a memorandum of understanding to outline the operation and management of a consolidated information technology environment between Criminal Investigation and the IT organization. The IT organization began to update the memorandum of understanding with Criminal Investigation to reflect the roles and responsibilities outlined in TFA § 2101; however, this effort remains on an “indefinite pause” as IRS leadership considers broader options. The indefinite pause of updating the memorandum of understanding means that the working relationship between the CIO and Criminal Investigation does not reflect TFA requirements.

According to the CIO, the IT organization engages monthly with Criminal Investigation leadership to ensure that Criminal Investigation remains strategically aligned with the IT organization. The CIO maintains oversight of Criminal Investigation's [REDACTED] information technology budget. While the budget does not include the \$15 million that Criminal Investigation received through the Consolidated Appropriations Act of 2020<sup>106</sup> for investigative technology, the IT organization retains oversight of these funds through the Work Request Management System.<sup>107</sup> In addition, the Office of the CIO has approval authority over Criminal Investigation's acquisition of information technology products and services except for information technology acquisitions required for sensitive law enforcement activities related to covert and law enforcement needs that do not affect the IRS network.

The IT organization also developed an *Information Technology Strategic Plan*. According to the CIO, the IRS Commissioner and the Treasury Department have approved the plan. The *Information Technology Strategic Plan* addresses multiple years and contains performance measurements that allow the IRS to assess its progress towards reaching the desired end state as set out in the plan. The plan identifies nine performance measurements. Five measurements are in place and actively tracked with baseline and target performance goals, including reduction of selected legacy code, aged infrastructure, service availability at the appropriate level of redundancy, application at the assessed level of risk or mitigated with compensating controls, and operations and maintenance cost stabilization. In addition, the plan identifies

---

<sup>106</sup> Pub. L. No. 116-93, 133 Stat. 2317.

<sup>107</sup> The authoritative, centralized database and repository for information technology-related work requests. The system maintains, distributes, and tracks work requests and their associated documentation, attachments, and responses.

four new performance measurements, including security compliance, workforce mobility, data, and new hire retention.

The *Information Technology Strategic Plan* refers to other companion documents, such as the *Target Enterprise Architecture*, the *Enterprise Technology Blueprint*, the *Annual Key Insights Report*, the *Information Technology Integrated Modernization Business Plan*, and the *Taxpayer Experience Strategy* for further information on how the multiyear plan will be implemented. The *Target Enterprise Architecture* and the *Enterprise Technology Blueprint* discuss the integrated enterprise architecture by taking into consideration the present, short-term, and long-term integrated architecture for the IRS. The *Annual Key Insights Report* considers resources that are required to accomplish the *Information Technology Strategic Plan* by discussing budgets and resources of information technology projects and initiatives for the coming year. The *Information Technology Integrated Modernization Business Plan* and the *Taxpayer Experience Strategy* describe specific projects and when the capabilities will be implemented and delivered.

The *Information Technology Strategic Plan* aligns with the *IRS Strategic Plan*.<sup>108</sup> Specifically, the plan states that it “builds on enterprise-wide strategic goals outlined in the *IRS Strategic Plan* and provides specifics around the mission, vision, and goals set forth for the technology landscape.” The *Information Technology Strategic Plan* takes the overall objectives from the *IRS Strategic Plan* and links them to the information technology environment.

## COVID-2019 response

COVID-19 is a virus that causes respiratory illness in people and can spread from person-to-person. The first case of the COVID-19 pandemic in the United States was confirmed on January 21, 2020. On March 13, 2020, the President of the United States officially declared a national emergency due to the outbreak of the COVID-19 pandemic. The pandemic caused by COVID-19 impacted how we live and work across the country, and around the world.

In Fiscal Year 2021, TIGTA and the GAO performed three audits covering the IRS's response to the COVID-19 pandemic. We initiated an audit<sup>109</sup> to ***determine whether the IRS effectively used its telework program to reduce the impact of the COVID-19 pandemic on IRS operations.*** Telework is a work flexibility arrangement under which employees perform their duties and responsibilities from an approved worksite other than the location from which employees would otherwise work. A robust telework program and ensuring as many employees as possible are prepared to telework are critical components of a plan to allow employees to work effectively from alternative sites and continue tax administration and mission-critical operations.

The IRS leveraged its telework program to continue operations during the pandemic. On March 27, 2020, the IRS issued an evacuation order directing all employees, except for those individuals performing mission-critical functions that could not be performed remotely, to vacate the work site by March 30 and work from home or an alternate location. The IRS had to respond quickly to safely evacuate employees from IRS facilities and provide nontelework-ready employees with the required information technology equipment needed to effectively work

---

<sup>108</sup> Dated April 2018.

<sup>109</sup> TIGTA, Report No. 2021-IE-R002, *Interim Report: The IRS Leveraged Its Telework Program to Continue Operations During the COVID-19 Pandemic* (Mar. 2021).

from alternate locations. Since the start of the pandemic, the telework program has been critical to maintaining IRS operations during the pandemic.

At the beginning of Fiscal Year 2020, prior to the pandemic, the IRS identified approximately 39,000 employees as telework eligible.<sup>110</sup> We analyzed weekly time reports before and after the COVID-19 pandemic began to assess the pandemic's impact on IRS operations.<sup>111</sup> Between March 14 and 28, 2020, the number of employees who reported any time worked at IRS facilities decreased from approximately 70,700 to 19,400 employees. The number of employees who reported any time to telework increased from approximately 27,500 to 41,000 employees.

Prior to the pandemic, between October 2019 and early March 2020, an average of 26,000 employees teleworked for approximately 22 hours each week.<sup>112</sup> By March 21, 2020, more than 36,500 employees teleworked an average of nearly 33 hours per week. After March 21, 2020, the number of teleworkers continued to increase. By September 26, 2020, nearly 60,700 employees teleworked at least some time during the week, a 134 percent increase from the weekly average before the pandemic. These 60,700 employees teleworked an average of 36 hours a week, a 64 percent increase in the weekly average before the pandemic.

A limiting factor to the growth of employee telework participation was the IRS's ability to identify, prioritize, and issue laptop computers and other information technology equipment to employees who previously had not participated in the telework program. The IRS indicated that it converted employees from desktops or shared workstations to individually assigned laptops through a set of information technology initiatives designed to make previously nontelework-ready employees ready to work remotely. Although the IRS was unable to distribute many laptops in March 2020, it had issued more than 12,600 laptops to employees by May 2020. As of October 2020, nearly 18,600 laptops had been distributed. As of September 30, 2020, the IRS indicated that it is continuing to work with the business units to identify additional users who require laptops to be telework enabled; however, it believes it has enough inventory to support additional needs.

Although the IRS issued more than 18,000 laptops to expand its employees' ability to telework, we found other technology-related concerns affected teleworking employees. For example, we conducted a series of site visits at four tax processing sites. Managers in these sites noted several information technology-related concerns affecting teleworking employees including: delays at the helpdesk, issues logging in through the virtual private network, issues with equipment, and issues with the SharePoint sites not working.

We identified several time codes used to capture downtime related to information technology issues. Between late January and April 2020, across the IRS, total downtime hours were typically below 10,000 hours per week. However, between May and September 2020, total information

---

<sup>110</sup> Telework-eligible employees are those employees who are authorized to apply for telework.

<sup>111</sup> We obtained weekly time reports from the IRS management information system, the Treasury Integrated Management Information System, and its time and attendance reporting system, the Single Entry Time Reporting system. The Treasury Integrated Management Information System is the official automated personnel and payroll system for storing and tracking all employee personnel and payroll data. The Single Entry Time Reporting system is an online payroll system that enables the timely input of time and attendance data to the National Finance Center for the generation of the employee's paycheck every pay period.

<sup>112</sup> The October 2019 through March 2020 period excludes the pay period including the Christmas and New Year Federal holidays (pay period 26-2019) because the number of employees reporting time to telework hours is skewed as a result of employees reporting time to holiday and annual leave categories.

technology downtime increased significantly, ranging from 20,000 to 30,000 hours per week. The total information technology downtime consists of downtime charged by employees during system, computer, and information technology helpdesk downtime.<sup>113</sup> During the pandemic, all three types of downtime increased as the IRS expanded the use of telework.

In our audit of the *CARES Act economic impact payment processing*, we found that the tax systems involved in delivering the economic impact payments to individuals generally performed well. The CARES Act contains numerous tax-related provisions that include the issuance of recovery rebates of \$1,200 per eligible individual (\$2,400 in the case of eligible individuals filing a joint return) and \$500 for each qualifying child. The IRS began issuing economic impact payments on April 10, 2020, just 14 days after the passage of the CARES Act; at the same time, the IRS was closing its facilities in response to the COVID-19 pandemic. To support these efforts, the IRS completed extensive computer programming and testing that was necessary to begin issuing the economic impact payments. This included developing computer programming requirements to identify eligible individuals and computing their economic impact payment amounts as well as modifying the Individual Master File to capture information related to the issuance of the economic impact payment in each individual's tax account. In total, 16 IRS tax systems were involved in the processing and delivery of the economic impact payments to individual taxpayers.

Of these 16 IRS tax systems, only the Individual Master File experienced a performance problem due to a coding issue in the software developed to process the payments. The IRS fully restored the system within approximately 24 hours and the economic impact payments scheduled to be delivered during the outage were processed the following business day. By quickly restoring the Individual Master File functionality, the IRS was able to continue to timely issue the economic impact payments to individual taxpayers in accordance with the CARES Act.

In addition, the IRS educated taxpayers on the economic impact payments. In order to complete this task, the IRS established a dedicated web page on IRS.gov to provide updated information related to the issuance of economic impact payments, including a continually evolving list of frequently asked questions.

The GAO initiated an audit<sup>114</sup> to *determine selected agencies' initial experiences in providing the information technology needed to support remote access for maximum telework and the extent to which selected agencies followed Federal information security guidance for their information technology systems that provide remote access*. The GAO reported that it found the IRS had information technology in place to support remote access for telework during the COVID-19 pandemic. For example, the IRS used a virtual private network to enable employees to connect remotely to its resources. Although the IRS initially experienced information technology challenges in supporting remote access for maximum telework, it generally overcame them. While the increased number of remote connections brings additional

---

<sup>113</sup> System downtime includes idle time when enterprise-wide systems/applications are down preventing the accomplishment of work. Computer downtime includes idle time when an employee's individual computer is unavailable due to computer-related issues preventing the accomplishment of work. Information technology helpdesk downtime includes idle time when an employee is waiting for information technology helpdesk assistance, including idle time while the IT organization is resolving the issue.

<sup>114</sup> GAO, GAO-21-583, *COVID-19: Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls* (Sept. 30, 2021).

<sup>115</sup> The IRS was selected for the Treasury Department.

cybersecurity risks, the IRS reported that it continued activities intended to help ensure the security of the information and systems. In addition, the GAO reported that the IRS generally followed Federal information security guidance for its information technology that supports remote access for telework, including elements of a telework security policy.

## Appendix I

### Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the adequacy and security of the IRS's information technology. This review is required by the IRS Restructuring and Reform Act of 1998. To accomplish our objective, we:

- Obtained information on the IRS's budget and staffing of employees and contractors to provide context on the size of the IT organization.
- Reviewed the Security and Information Technology Services business unit's Systems Security, Systems Development, and Systems Operations Directorates' audit reports issued during Fiscal Year 2021. We also analyzed and prepared summaries of the information technology security, systems development, and operations issues.
- Identified and summarized other relevant TIGTA and external oversight assessments dealing with information technology security, systems development, and operations.
- Assessed the security, systems development, and operations issues and determined which are at high risk for failing to deliver IRS program objectives and protect tax administration data.

#### **Performance of This Review**

The compilation of information for this report was performed at various TIGTA offices during the period of April through September 2021. The information presented was derived from TIGTA and GAO reports issued during Fiscal Year 2021 as well as IRS documents related to its information technology plans and issues. TIGTA audits and our analyses were conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Bryce Kisler, Director; Louis Lee, Audit Manager; Natalie Russell, Lead Auditor; and Paula Benjamin-Grant, Auditor.

#### **Internal Controls Methodology**

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. This report presents an overall assessment of the IRS's information technology program based on a compilation of the audit results reported during Fiscal Year 2021. Therefore, we did not evaluate internal controls as part of this review.

## Appendix II

### List of Treasury Inspector General for Tax Administration and Government Accountability Office Reports Reviewed

No.	Report Number	Audit Report Title	Report Issuance Date
1	GAO-21-162	*Financial Audit: IRS's FY 2020 and FY 2019 Financial Statements	November 10, 2020
2	2021-20-003	Security Controls Over Electronic Crimes Labs Need Improvement	December 21, 2020
3	2021-26-006	Systems Processing Economic Impact Payments Performed Well and the Get My Payment Application Security Vulnerabilities Are Being Remediated	December 28, 2020
4	2021-30-010	Fiscal Year 2021 Biannual Independent Assessment of Private Collection Agency Performance	December 28, 2020
5	2021-45-017	Additional Security Processes Are Needed to Prevent Unauthorized Release of Tax Information Through the Income Verification Express Service Program	February 16, 2021
6	2021-IE-R002	Interim Report: The IRS Leveraged Its Telework Program to Continue Operations During the COVID-19 Pandemic	March 23, 2021
7	GAO-21-401R	Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls	May 4, 2021
8	2021-25-032	Streamlined Critical Pay Authority for Information Technology Positions Is Being Successfully Implemented	May 27, 2021
9	2021-25-025	Taxpayer First Act: Data Security in the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center	May 28, 2021
10	2021-20-028	Opportunities Exist to Improve Hiring and Retaining Employees With Information Technology Expertise	June 2, 2021
11	2021-20-024	Improvements Are Needed to More ██████████ ██████████ the Virtual Host Infrastructure Platform	June 3, 2021
12	2021-20-046	Select Post-Award Financial Management and Documentation Controls for Information Technology Service Contracts Need Improvement	August 9, 2021
13	2021-20-056	Laptop and Desktop Sanitization Practices Need Improvement	September 20, 2021
14	2021-20-065	The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating As Intended, but Improvements Are Needed	September 27, 2021

**Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021**

No.	Report Number	Audit Report Title	Report Issuance Date
15	2021-20-066	The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement	September 27, 2021
16	2021-20-063	██████████ Platform Management Needs Improvement	September 28, 2021
17	2021-20-072	Fiscal Year 2021 IRS Federal Information Security Modernization Act Evaluation	September 28, 2021
18	2021-25-058	Efforts to Implement Taxpayer First Act Section 2101 Have Been Mostly Successful	September 29, 2021
19	2021-20-059	Enterprise Case Management Deployed Its Initial Release, but Process Improvements Are Needed for Future Releases	September 30, 2021
20	GAO-21-583	Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls	September 30, 2021

\* FY = Fiscal Year.

## Appendix III

Glossary of Terms

Term	Definition
Active Directory	A Microsoft Corporation software system for administering and securing computer networks. It manages the identities and relationships of computing resources that comprise a network. It also enables administrators to assign enterprise-wide policies, deploys programs to many computers, and applies critical updates to an entire organization simultaneously from a central, organized, accessible database. It simplifies system administration and provides methods to strengthen and consistently secure computer systems.
Adjudication	The formal processes of judgment or ruling that render a final decision.
Agent (in the context of information technology)	A software routine that waits in the background and performs an action when a specified event occurs. For example, an encryption agent would transform information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
Agile	Software development methodologies centered around the idea of iterative development, where requirements and solutions evolve through collaboration between self-organizing cross-functional teams.
Application Program Interface	A set of routines, protocols, and tools referred to as "building blocks" used in business application software development.
Artifact	The output of an activity performed in a process/procedure, which is created throughout the life cycle of a project.
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticator	The means used to confirm the identity of a user, processor, or device, <i>e.g.</i> , user password or token.
Authorization	Access privileges granted to a user, program, or process, or the act of granting those privileges.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Backlog	An ever-evolving list of items relating to needed product functionality or actions, <i>e.g.</i> , bug fix, prioritized by the Product Owner, that conveys to an agile team what functionality is desired to be implemented first.
Base Award	The original written contract prior to any amendments or modifications.

## Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021

Term	Definition
Baseline	A benchmark that includes project costs, schedule, and scope against which project performance is measured.
Blacklist	List of applications to which users should not have access.
Business Process	A set of structured activities or tasks that, once completed, will accomplish specific organization goals.
Business Process Heat Map	A tool designed to track and visualize the retirement status of systems, see the migration status of individual business processes, and facilitate decommissioning decision-making.
Business Unit	A title for major IRS organizations, such as the IRS Independent Office of Appeals, the Wage and Investment Division, the Office of Professional Responsibility, and the IT organization.
Call Site	Provides telephone assistance for individual and business taxpayers on tax-related issues.
Campus	The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.
Career Connector	The name of the Treasury-wide automated applicant management system. It posts electronic job lists and allows candidates to submit resumes via the Internet, <i>i.e.</i> , online.
Change Request	The method for requesting approval to change a baselined product or other controlled item.
Cipher	Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text, or in which units of plain text are rearranged, or both.
Cloud	The use of computing resources, <i>e.g.</i> , hardware and software, which are delivered as a service over a network (typically the Internet).
Cold Site	A datacenter space without any server-related equipment installed. It provides power, cooling, and/or office space when an event occurs causing significant outage to the main datacenter. It requires extensive support from engineering and information technology personnel to get all necessary servers and equipment migrated and functional.
Computer Investigative Specialist	Supports special agents in collecting and analyzing digital evidence to prosecute criminal cases.
Computer Security Incident Response Center	Part of the IRS IT organization's Cybersecurity function. Its mission is to ensure that the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify and eradicate cyberthreats or cyberattacks. One of its primary duties is to provide 24-hour monitoring and support for IRS operations seven days a week, 365 days a year.
Continuous Diagnostics and Mitigation	Provides tools, integration services, and dashboards to all participating agencies to improve their respective agency security postures to defend against cybersecurity threats and vulnerabilities.

## Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021

Term	Definition
Contracting Officer Representative	The principal program representative assigned to Government procurements. The primary role of the contracting officer representative is to provide technical direction, monitor contract performance, and maintain an arm's length relationship with the contractor ensuring that the Government pays only for the services, materials, and travel authorized and delivered under the contract.
Credential	An object or data structure that authoritatively binds an identity – via an identifier or identifiers and (optionally) additional attributes – to at least one authenticator possessed and controlled by a subscriber.
Credentialed Scan	A scan in which the scanning computer has an account on the computer being scanned that allows a scanner to perform a more thorough check for problems that cannot be seen from the network.
Criminal Investigation	An IRS business unit that serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law.
Cross-Site Scripting	A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client.
Customer Account Data Engine 2	Establishes a single database that houses all individual taxpayer accounts, including Individual Master File data, which provides IRS employees the ability to view updated account information online.
Dashboard	A user interface or web page that gives a current summary of key information, usually in graphic, easy-to-read form, relating to progress and performance.
Database	A computer system with a means of storing information in such a way that information can be retrieved.
Decommission	To remove something, <i>e.g.</i> , system, server, from service.
Decommissioning Cost Funding Model	A tool used to determine the ability of the ECM program to “self-fund” or offset the cost of retiring legacy case management systems by comparing operations and maintenance savings realized as a result of past legacy case management system retirements.
Defense Information Systems Agency	An agency that oversees the information technology/technological aspect of organizing, delivering, and managing defense-related information.
Delivery Partners	Organizations or individuals assigned responsibility and accountability for management of an enterprise process.
Domain Group	Used to help control access to shared resources and to delegate specific domain-wide roles.
E-Services	A suite of web-based tools that allows tax professionals and taxpayers to complete certain transactions online with the IRS. These services are available 24 hours a day, seven days a week, via the Internet.

## Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021

Term	Definition
[REDACTED]	[REDACTED]
Enterprise Computing Center	A data center that supports tax processing and information management through a data processing and telecommunications infrastructure.
Enterprise Life Cycle	A framework used by IRS information technology projects to ensure consistency and compliance with Government and industry best practices.
Enterprise Standards Profile	The authoritative repository for IRS-approved products and standards. It allows project owners and other stakeholders to select preapproved technology products and standards. Development teams should determine which standards and approved products apply to their areas of responsibility. Lists in the Enterprise Standards Profile include guidance for usage that should be reviewed for useful, relevant information.
Expedited Delivery Process	A new approach to accelerate process design, elaboration, and platform configuration for business processes that can deliver a prototype within 90 to 120 days.
Exploit	A general term for any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.
Federal Acquisition Regulation	The primary acquisition regulation for use by all Federal executive agencies in their acquisition of supplies and services with appropriated funds.
Federal Employee Viewpoint Survey	An Office of Personnel Management survey that measures employee perceptions of whether, and to what extent, conditions characterizing successful organizations are present in Federal agencies. Survey results provide valuable insight into the challenges organization leaders face in ensuring that the Federal Government has an effective civilian workforce and how well they are responding.
Federal Procurement Data System	Contains contracting data that provide the Federal Government with information to assess where its money is being spent.
Federal Supply Code	A code that corresponds to a material group code and provides a more detailed description of the expense for financial accounting purposes. It is also known as the product service code.
Federal Tax Information	Consists of Federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code and subject to the § 6103(p)(4) safeguarding requirements including IRS oversight.
Federation	A collection of realms (domains) that have established trust among themselves. The level of trust may vary, but typically includes authentication and may include authorization.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.

## Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021

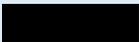
Term	Definition
Firmware Component	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Folders Management Module	A part of the Procurement for Public Sector application that stores contract file documents as the IRS's official system of record.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
High Value Asset	Refers to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical Federal operations or house unique collections of data (by size or content), making them of particular interest to criminal, politically motivated, or State-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the Government.
██████████	A ██████████ environment intended to meet strategic needs for partnership-driven, secure data analytics at scale. It creates an agile, efficient, and scalable platform for hosting projects, including the ISAC.
Homeland Security Presidential Directive-12 Credential	Directive which mandates a Federal standard to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Governmentwide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).
Host	Any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, servers, personal electronic devices, and multifunctional devices.
Hot Fix	A single, cumulative package, which includes one or more files, that is used to address a problem in a product.
Hot Site	Mirrors a datacenter infrastructure. The backup site is populated with servers, cooling, power, and office space, if applicable. The most important feature offered from a "hot" site is that the production environment(s) are running concurrently with the main datacenter. This syncing allows for minimal impact and downtime to business operations. In the event of a significant outage event to the main datacenter, the hot site can take the place of the impacted site immediately.
Human Capital Office	Provides strategies and tools for recruiting, hiring, developing, and retaining a highly skilled and high-performing workforce.

## Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021

Term	Definition
Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Participant Area	An area in the ISAC to access FTI and reports, <i>etc.</i> Access to this area requires the completion of annual ISAC security and rules of behavior training.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
Information Leakage	The intentional or unintentional release of information to an untrusted environment.
Information System Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency. The term information technology includes computers, ancillary equipment, software, firmware, services (including support services), and related resources.
Information Technology Organization	The IRS business unit responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.
Infrastructure	The hardware, software, and network resources and services required for the existence, operation, and management of an enterprise information technology environment. It allows an organization to deliver information technology solutions and services to its employees, partners, and customers.
Injection	An attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application.
Input Validation	The proper testing of any input supplied by a user or application to prevent improperly formed data from entering an information system.
Integrated Data Retrieval System	IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.
Integrated Financial System	Contains the IRS's core financial systems, including expenditure controls, accounts payable, accounts receivable, general ledger, and budget formulation. The system includes a managerial cost accounting capability that enables the IRS to make informed and timely performance-based business and budgetary decisions.
Integrated Master Schedule	Contains a high-level overview of project schedules along with additional program tasks, including high-level start/end dates, project/application milestones, cross-project dependencies, and program milestones.
Internal Revenue Manual	The IRS's primary source of instructions to its employees related to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.

Term	Definition
[REDACTED]	[REDACTED]
Kernel	Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept.
Key Management Solution	A solution used to manage encryption keys of various activities, including key generation, exchange, distribution, rotation, replacement, storage, access, backup, and destruction. Encryption cannot be deployed without an associated working key management solution, also referred to as a key management system.
Knowledge Incident/Problem Service Asset Management System	An application that maintains the complete IRS inventory of information technology and non-information technology assets, computer hardware, and software. It is also the reporting tool for problem management with all IRS-developed applications.
Landing Page	The section of a website accessed by clicking a hyperlink on another web page, typically the website's home page.
Legacy System	An information system that may be based on outdated technologies but is critical to day-to-day operations. In the context of computing, it refers to outdated computer systems, programming languages, or application software that are used instead of more modern alternatives.
Limited Area	An area in a building where access is limited to authorized personnel only. All who access a Limited Area must have a verified official business need to enter. Limited Area space can be identified by the Chief, Facilities Management and Security Services, Physical Security Section, based on critical assets.
[REDACTED]	[REDACTED]
Material Group Code	A code that describes the expense category of a contract for financial accounting purposes.
Mechanism	Logical assembly of components, elements, or parts, and the associated energy and information flows, that enable a machine, process, or system to achieve its intended result.
Middleware	A software that functions at an intermediate layer between applications and the operating system and database management system or between the client and server.
Milestone	A management decision point placed at a natural breakpoint in the life cycle, at the end of the phase, where management determines whether a project can proceed to the next phase.
Mission-Critical Skill	Competencies essential to the operation of an organization.
[REDACTED]	A private, independent, not-for-profit organization, chartered to work in the public's interest. [REDACTED] has set up the ISACs for the health industry (which, like the IRS, has laws requiring protection of sensitive data) and for the airline industry and has prior technological expertise in building ISACs.

## Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021

Term	Definition
Modification	Any formal change to the terms and conditions of a contract, delivery order, or task order, either within or outside the scope of the original agreement.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Online 5081	A web-based application that allows users to request access, modify existing accounts, reset passwords, and request deletion of accounts when access is no longer needed to specific systems. The application also allows the IRS to track user access history, generate reports, and document an audit trail of user actions.
Operating System	The software that serves as the user interface and communicates with computer hardware to allocate memory, process tasks, and access disks and peripherals.
Patch	Updates to an operating system, application, or other software issued specifically to correct particular problems with the software.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, and biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date of birth, place of birth, and mother's maiden name.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Platform	A computer or hardware device, an associated operating system, or a virtual environment on which software can be installed or run.
	
Portfolio	The combination of all information technology assets, resources, and investments owned or planned by an organization in order to achieve its strategic goals, objectives, and mission.
PowerShell™	A task-based, command-line shell and scripting language built on the .NET that helps system administrators and power users rapidly automate tasks that manage operating systems and processes.
Private Debt Collection Program	A program implemented by the IRS to use private collection agencies to collect taxes on cases involving inactive tax receivables.
Privileged	Accounts with set "access rights" for certain users on a given system. Sometimes referred to as system or network administrative accounts.

## Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021

Term	Definition
Processing Year	The calendar year in which the tax return or document is processed by the IRS.
Procurement for Public Sector Application	An application used by the IRS to request, fund, and award contracts; execute delivery orders; and verify receipt and acceptance of products and services as well as accrue procurement-related liabilities and process payments.
Production	The location where the real-time staging of programs that run an organization are executed; this includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
Program Increment	A length of time, usually eight to 12 weeks comprised of multiple iterations, during which incremental value of working, tested software and systems is delivered.
Public Key Infrastructure	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Release	A specific edition of software that is deployed into production.
Requirement	Describes a condition or capability to which a system must conform, either derived directly from user needs, or stated in a contract, standard, specification, or other formally imposed document. A desired feature, property, or behavior of a system.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of an information system. Incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
Risk-Based Decision	A decision made when meeting a requirement is technically or operationally not possible or is not cost-effective. It is required for any situation in which the system will be operating outside of IRS information technology security policy or NIST guidelines, whether related to a technical, operational, or management control.
Scaled Agile Framework	A framework for scaling agile development principles across an enterprise, which provides guidance for all the levels of the enterprise engaged in solution development, created and owned by Scaled Agile, Inc.
Section 508	A part of the Rehabilitation Act of 1973, requiring Federal agencies to make their electronic and information technology accessible to people with disabilities.
Sector	The smallest physical storage unit on a hard disk, which is 512 bytes in size.
[REDACTED]	[REDACTED]
Security Assertion Markup Language	An open standard that simplifies the login experience for users. It allows users to access multiple applications with one set of credentials, usually entered just once.

## Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021

Term	Definition
Security Assessment Report	Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.
Sensitive But Unclassified	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under the Privacy Act, <sup>1</sup> which could result from inadvertent or deliberate disclosure, alteration, or destruction.
Sequencing	A process of evaluating scalability, business affect, capabilities, and processes to determine the order for migrating systems.
Service Pack	A software program that corrects known bugs or problems or that adds new features. Typically released when the number of individual patches to the application becomes too large. It is easier to install than groups of patches.
Software Patch	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
[REDACTED]	[REDACTED]
Subscriber	A party who has received a credential or authenticator from a credential service provider. If the applicant is successfully proofed, the individual is then termed a subscriber of that credential service provider.
System	A set of interdependent components that perform a specific function and are operational. It may also include software, hardware, and processes.
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Tabletop Exercise	The incidence response tabletop exercise brings members of the incidence response team together to simulate their response to a security and privacy incident scenario(s). It is a cost-effective and efficient way to identify gaps, overlaps, and discrepancies in the incidence response handling capabilities.
Tax Processing Center	The arm of the IRS that processes paper-filed tax returns.
Tax Transcript	Provides financial tax account information, such as payments, penalty assessments, and adjustments made by the taxpayer or the IRS.
Tax Year	The 12-month period for which tax is calculated. For most individual taxpayers, the tax year is synonymous with the calendar year.
Tax-Exempt and Government Entities Division	The IRS established the business unit to improve its ability to meet the special needs of pension plans, exempt organizations, and government entities in complying with the tax laws.

<sup>1</sup> 5 U.S.C. § 552a.

**Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2021**

<b>Term</b>	<b>Definition</b>
Taxpayer Advocate Service	An independent organization within the IRS, led by the National Taxpayer Advocate.
[REDACTED]	[REDACTED]
Transcript Delivery System	Allows external third parties to view and obtain tax transcripts for both individuals and businesses.
[REDACTED]	[REDACTED]
Trojan Horse	A malicious program that pretends to be harmless in order to trick people into downloading it.
Unpaid Assessments	A database that consists of all tax modules that show a debit balance on the Individual Master File, Business Master File, and Automated Non-Master File.
Virtual Private Network	A secure way of connecting to a private local area network at a remote location, using the Internet or any unsecure public network to transport the network data packets privately, using encryption.
Virus	A piece of programming code usually disguised as something else that causes some unexpected and, for the victim, usually undesirable event and is often designed so it is automatically spread to other computers.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten the network's security.
Wage and Investment Division	The IRS business unit that serves taxpayers whose only income is derived from wages and investments.
Warm Site	A datacenter space having some pre-installed server hardware. The difference between a "hot" and a "warm" site is that the "hot" site provides a mirror of the production datacenter and its environment(s), while a "warm" site contains only servers ready for the installation of the production environment(s). A warm site makes sense for an aspect of the business which is not critical, but requires a level of redundancy.
Waterfall	Distinguished by development of a solution with frequent reviews and formal approvals required at multiple points in the life cycle prior to additional work being performed.
Worm	A type of malicious software program whose primary function is to infect other computers while remaining active on infected systems.

## Appendix IV

### Abbreviations

CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CIO	Chief Information Officer
CIS	Computer Investigative Specialist
COVID-19	Coronavirus Disease 2019
DARE	Data at Rest Encryption
ECM	Enterprise Case Management
EDR	Endpoint Detection and Response
FISMA	Federal Information Security Modernization Act of 2014
FTI	Federal Tax Information
GAO	Government Accountability Office
IRS	Internal Revenue Service
ISAC	Identity Theft Tax Refund Fraud Information Sharing and Analysis Center
IT	Information Technology
IVES	Income Verification Express Service
MSS	Memphis Sanitization Site
NIST	National Institute of Standards and Technology
██████████	██
TFA	Taxpayer First Act of 2019
TIGTA	Treasury Inspector General for Tax Administration
TTP	Trusted Third Party
UNS	User and Network Services



**To report fraud, waste, or abuse,  
call our toll-free hotline at:**

(800) 366-4484

**By Web:**

[www.treasury.gov/tigta/](http://www.treasury.gov/tigta/)

**Or Write:**

Treasury Inspector General for Tax Administration

P.O. Box 589

Ben Franklin Station

Washington, D.C. 20044-0589

Information you provide is confidential, and you may remain anonymous.