TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Mainframe Computing Environment Security Needs Improvement

September 28, 2020

Reference Number: 2020-20-045

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

HIGHLIGHTS: Mainframe Computing Environment Security Needs Improvement

Final Audit Report issued on September 28, 2020
Reference Number 2020-20-045

Why TIGTA Did This Audit

This audit was initiated to review the effectiveness and efficiency of the IRS's mainframe systems security and operations. The mainframe computers are part of the foundation of a complex environment of computer systems.

Impact on Taxpayers

In Fiscal Year 2019, the IRS processed more than 253 million tax returns and forms. It collected more than $3.5 trillion in Federal taxes paid by individuals and businesses, issuing more than $452 billion in refunds. To support these efforts, the IRS employs two mainframe platforms.

Maintaining the confidentiality, integrity, and availability of tax and financial data is vital to tax processing operations. Security weaknesses could have serious adverse effects on tax administration and the protection of taxpayer data.

What TIGTA Found

The IRS mainframe platform is not satisfying minimum mainframe security requirements in several key areas **********2**********. Access controls were working as intended. However, the IRS continues to use **********2********** ********2********** and does not use **********2********** to validate the security and integrity of the mainframe platform as agreed to in a prior audit report. The planned follow-on solution *********2******** *********2*******, originally scheduled to be delivered ******2******** *********2*******, now has an implementation date *********2*****. In addition, the IRS did not ********2********** ****2*** within the required 60-day time period, and *******2******** **********2********** **********2**********.

The IRS did not approve a risk-based decision for a deviation from an existing agency security policy that required the IRS to protect information systems from malicious code. In addition, inaccurate and incomplete information contained within **********2********** **********2********** hardware inventory records resulted in a total of 62 errors identified in the inventory data. Finally, the IRS failed to report 52 logical partitions to the Department of the Treasury's Cybersecurity Analysis and Reporting Dashboard.

What TIGTA Recommended

The Chief Information Officer should ensure that the *******2******* ********2******* follow-on solution is delivered without further delay, **********2********** **********2********** are timely remediated based on agency-defined timelines, a comprehensive and accurate inventory of the mainframe platform system components is maintained, personnel are properly trained on IRS procedures governing hardware asset management, a reconciliation procedure is established that includes communication between the affected functions that update and validate the inventory, a risk-based decision is developed and approved for one deviation from existing agency security policies, and the data collection matrix is updated to ensure that accurate information is reported to the Department of the Treasury.

The IRS agreed with all nine recommendations. The IRS plans to prioritize resources to ensure delivery of the **********2********** *****2***** follow-on solution, maintain comprehensive and accurate inventories, train personnel to comply with policies governing hardware asset management, submit a risk-based decision for the deviation from policy, and ensure that accurate information is reported to the Department of the Treasury. The IRS stated that it timely remediated **********2********** **********2*********.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 28, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Mainframe Computing Environment Security Needs Improvement (Audit # 202020001)

This report presents the results of our review to evaluate the effectiveness and efficiency of the Internal Revenue Service's (IRS) mainframe systems security and operations. This review is part of our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenge of *Security Over Taxpayer Data and Protection of IRS Resources*.

Management's complete response to the draft report is included as Appendix III.

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

Table of Contents

Background ..... Page 1

Results of Review ..... Page 2

The International Business Machines Mainframe Platform Is Not Satisfying Minimum Security Requirements in Several Key Areas ..... Page 2

Recommendation 1: ..... Page 6

Recommendations 2 through 4: ..... Page 7

Mainframe Hardware Asset Inventories Were Inaccurate and Incomplete ..... Page 7

Recommendations 5 through 7: ..... Page 10

Two Security Policies Were Not Met ..... Page 11

Recommendation 8: ..... Page 13

The Department of the Treasury Cybersecurity Analysis and Reporting Dashboard Report Was Inaccurate and Incomplete ..... Page 13

Recommendation 9: ..... Page 14

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 15

Appendix II – Outcome Measures ..... Page 17

Appendix III – Management's Response to the Draft Report ..... Page 18

Appendix IV – Glossary of Terms ..... Page 23

Appendix V – Abbreviations ..... Page 26

Background

In Fiscal Year 2019, the Internal Revenue Service (IRS) processed more than 253 million tax returns and forms. It collected more than $3.5 trillion in Federal taxes paid by individuals and businesses, issuing more than $452 billion in refunds. To support these efforts, the IRS employs two mainframe platforms. One platform employs the International Business Machines® (IBM) mainframe systems infrastructure, which includes mainframe computers operating with either the **********2**********
**********2**********.[1] The other platform is comprised of Unisys mainframe systems.[2] The mainframe computers are part of the foundation of a complex environment of computer systems and are under the responsibility of the Information Technology organization's Enterprise Operations function. The mainframe computing environment provides access control functionality to maintain the confidentiality, integrity, and availability of tax and financial data that are integral to support tax processing operations. In addition, the Cybersecurity function's Security Operations Branch performs reviews, analyzes, and reports compliance and security issues affecting the mainframe systems.

**********2**********,[3] **********2**********
**********2**********
**********2**********
**********2**********.[4] *****2**********
**********2**********
**********2**********.

**********2**********
**********2**********

*********2********	*********2********
****2***	****2***
****2***	****2***
****2***	****2***
****2***	****2***

**********2**********
**********2**********.

[1] See Appendix IV for a glossary of terms.

[2] We did not include the Unisys mainframe platform in the scope of this audit.

[3] **********2**********
**********2**********.

[4] National Institute of Standards and Technology, Federal Information Processing Standard 199, *Federal Information Processing Standards Publication, Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

Results of Review

The International Business Machines Mainframe Platform Is Not Satisfying Minimum Security Requirements in Several Key Areas

Security controls provide a range of safeguards and countermeasures for organizations and information systems to protect information during processing, while in storage, and during transmission. The National Institute of Standards and Technology[5] provides security controls that are designed to facilitate compliance with applicable Federal laws, Executive orders, directives, policies, regulations, standards, and guidance. Compliance with the National Institute of Standards and Technology guidance necessitates organizations to execute due diligence with regard to information security and risk management. Information security due diligence includes using all appropriate information as part of an organization-wide risk management program to effectively use the tailoring guidance and inherent flexibility in the National Institute of Standards and Technology publications so that the selected security controls documented in organizational security plans meet the mission and business requirements of organizations. In addition, the IRS has adopted as policy the more technically explicit controls in the Defense Information Systems Agency's (DISA) Security Technical Implementation Guide (STIG). Finally, the Internal Revenue Manual (IRM)[6] provides mainframe guidance to:

- Protect the critical infrastructure and assets of the IRS.
- Prevent unauthorized access to IRS assets.
- Enable IRS information technology computing environments that meet agency security control requirements and support the business needs of the organization.

We found that the IBM mainframe platform did not satisfy the minimum mainframe security requirements in several key areas **********2**********, but access controls were working as intended. Security weaknesses could have serious adverse effects on tax administration and the protection of taxpayer data.

**********2**********

**********2**********
**********2**********
**********2**********:

- **********2**********.
- **********2**********
  **********2**********.
- **********2**********
  **********2**********.

[5] National Institute of Standards and Technology, Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4 (Apr. 2013).
[6] IRM 10.8.32, *Information Technology Security – IBM Mainframe System Security Requirements* (July 2018).

**********2**********
**********2**********.

**********2**********

****2*** ****2*** ****2*** ****2***	****2*** ****2*** ****2*** ****2*** ****2***	****2*** ****2*** ****2*** ****2***	****2*** ****2*** ****2*** ****2***	****2*** ****2*** ****2*** ****2***
****2***	**2**	**2**	**2**	**2**
****2***	**2**	**2**	**2**	**2**
**** 2***	**2**	**2**	**2**	**2**

**********2**********
*********2**********.

**********2**********

**********2**********
**********2**********
**********2**********
**********2**********.

**********2**********
**********2**********.[7] **********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********.

[7] **********2**********
**********2**********.

******************2*****************

****2***	****2***	****2*** ****2***
**********2********* **********2*********	**********2*********	**********2*********
***2**	***2** ***2** [8] ***2**	***2** ***2** ***2**

***2**.

2
2
2
2
2
2
2
2
2
2
********************2*****************.

2
2
2
2
2
2
2
2
*********2*******.

2
2
2
2
2
2
2
2
2
2
2
2
2

8 ***2***
*********2*******.

**********2**********
**********2**********
******2****.
**********2**********
**********2**********
**********2**********.

**********2**********

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
*******2*****.
**********2**********
**********2**********
confidentiality, integrity, and availability of the system.

**********2**********

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
*****************2***************.
**********2**********
**********2**********
**********2**********
***********2********.
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********.

Access controls are working as intended

We reviewed the privileged and service account access controls over the IBM mainframe platform and determined all related agency security policies are effectively implemented and working as intended. We reviewed the following with no discrepancies noted:

- Privileged and service account access was properly authorized.
- Inactive privileged and service accounts were properly removed.
- Expiration dates in the Online 5081 system used to revoke system access to contractors was based on the contract completion date (end of base contract plus exercised options).

The IRM states that the Online 5081 system shall be used to register all users for access to any IRS information technology resource for which they require access. In addition, the IRS shall implement and maintain periodic follow-up reviews and corrective action procedures to ensure timely adjustment of access privileges.

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********.

Our review of the Online 5081 account access authorizations for this audit revealed that all system administrator and service accounts had the required approvals, to include associated documentation, to access the IBM mainframe platform environment. We also reviewed the Online 5081 Manager Guide[9] and found that the updated guidance includes a field to ensure that expiration dates for non-IRS employees (*e.g.*, contractors) are used in the Online 5081 system.

By providing adequate administrative oversight of system access controls, the IRS protects the security posture of the mainframe platform and helps prevent unauthorized system access.

The Chief Information Officer should:

Recommendation 1: Prioritize resources to ensure that the **********2********** follow-on solution is delivered without further delay in order to maintain the confidentiality, integrity, and availability of data and information processed by the IBM mainframe platform.

Management's Response: The IRS agreed with this recommendation. The IRS will prioritize resources to ensure that the **********2********** follow-on solution for

[9] IRS, *Online 5081 Manager Guide* (Apr. 2019).

**********2********** is delivered without further delay in order to maintain the confidentiality, integrity, and availability of data and information processed by the IBM mainframe platform. In addition, the IRS will maintain the *********2********* **********2**********.

Recommendation 2: Ensure that the Security Regulatory Compliance Operations Team uses the **********2********** *********2********* during its review of the security and integrity of the IBM mainframe platform *********2********** until the follow-on solution is fully operational.

Management's Response: The IRS agreed with this recommendation. The Cybersecurity function will implement the use of the **********2********** **********2********** to review the security and integrity of the IBM mainframe platform *********2********* until the delivery of alternate solutions and capabilities are available. The delivery of alternative solutions and capabilities is contingent on budgetary constraints.

Recommendation 3: Ensure that the *********2********** are timely remediated based on agency-defined timelines to protect the confidentiality, integrity, and availability of the information system.

Management's Response: The IRS agreed with this recommendation. The Cybersecurity function has ensured that the **********2**********, which related to the **********2**********, were timely remediated based on agency-defined timelines to protect the confidentiality, integrity, and availability of the information system.

Recommendation 4: Ensure that the required **********2********** **********2**********, are completed by **********2********** rather than using the System Security Plan to validate the security and integrity of **********2********** ******2******.

Management's Response: The IRS agreed with this recommendation. The Cybersecurity function will ensure that **********2********** **********2**********, which are conducted **********2**********, are completed by **********2**********.

Mainframe Hardware Asset Inventories Were Inaccurate and Incomplete

The User and Network Services function is responsible for managing the IRS's information technology hardware assets. Although the User and Network Services function is the business process owner of the hardware asset inventory data, the Information Technology organization is responsible for verifying and certifying the inventory accuracy of the hardware assets under its respective control. Asset owners, stakeholders, and personnel responsible for hardware play a critical role in ensuring the accuracy of the hardware asset inventory.

Within the User and Network Services function, the Service Asset and Configuration Management's Hardware Asset Management office is responsible for providing enterprise-wide

oversight, coordination, and guidance on hardware asset management. The IRS uses the **********2********** [10] to track its hardware asset inventory.

Hardware asset inventories

We evaluated the hardware asset inventory specific to the IBM mainframe platform. The inventory system relies heavily on manual data entry and currently does not sufficiently leverage available automated tools to assist in maintaining an up-to-date, complete, and accurate inventory. We determined that the November 2019 and January 2020 inventory reports were both inaccurate and incomplete and did not contain the level of granularity required for timely and up-to-date tracking and reporting. However, throughout the course of the audit, the Enterprise Operations function's **2** Support Branch and the User and Network Services function's Hardware Asset Management office completed multiple updates to the IBM mainframe platform inventory. As a result, the March 2020 inventory was accurate and current.

In the November 2019 and January 2020 inventory reports, we found 62 policy exceptions **********2********** **********2**********. Some specific examples of inaccurate and incomplete reporting include:

- The November 2019 inventory report listed eight assets as *In Use;* however, we found that the eight assets should have been listed as *Retired*.
- The January 2020 inventory report documented **********2********** **********2**********; however, we found that ******2**** are located at the **********2**********.
- During a site visit to the **********2**********, we identified *******2****** **********2********** that were not included on either the November 2019 or the January 2020 inventory reports. Further analysis determined that the **********2********** were incorrectly assigned to the Enterprise Network function.

**********2**********

2	***2*** ***2***	***2***	***2*** ***2***	***2*** ***2***	***2*** ***2***	***2***
******2******	**2**	**2**	**2**	**2**	**2**	**2**
******2******	**2**	**2**	**2**	**2**	**2**	**2**
******2******	**2**	**2**	**2**	**2**	**2**	**2**
Total ******2****	**Total **2**	**Total **2**	**Total **2**	**Total **2**	**Total **2**	**Total **2**

*********2********** **********2**********.

The IRM[11] requires system owners to develop and document an inventory of information system components that is accurate, includes all components within the authorization boundary of the

[10] **********2********** is a component of the Knowledge, Incident/Problem Service Asset Management system, **********2**********.
[11] IRM 10.8.1, *Information Technology Security – Policy and Guidance* (May 2019).

information system, captures both hardware and software, and contains the level of granularity deemed necessary for tracking and reporting. In addition, the Hardware Asset User Guide[12] states that key fields must be both complete and accurate and that asset record updates be submitted within 10 business days of the completed action.

The *2* Support Branch has primary responsibility for the day-to-day IBM mainframe inventory management, to include creating new asset records and submitting updates for existing assets. The **2** Support Branch officials stated that they were unaware of any policies or procedures related to required timelines for the submission of inventory-related information. The Enterprise Operations function's Authorizing Official Management Branch uploads a version of the IBM mainframe inventory into the Treasury Federal Information Security Modernization Act of 2014 (FISMA)[13] Inventory Management System. We compared the inventory information uploaded into the Treasury FISMA Inventory Management System with the information contained in the **********2********** inventory, **********2********** ********2********, and found 16 discrepancies between the two inventories. In addition, there is no communication or reconciliation mechanism between the **2** Support Branch and the Authorizing Official Management Branch regarding the IBM mainframe inventory.

Lastly, the User and Network Services function's Hardware Asset Management group stated that an ongoing project that began in November 2019, called the Information Technology Asset Management initiative, will automate the population of the key inventory-related fields. These actions will significantly aid in the proper classification of information technology assets. Specifically, the Information Technology Asset Management initiative, once implemented, will:

- Automate hardware asset inventory (*i.e.*, barcode scanning).
- Integrate Radio Frequency Identifiers scanning to enable real-time posting and tracking of computer room asset inventory.
- Leverage **********2********** automation capabilities to improve currency and accuracy of General Support System data attributes.

Equipment refresh

The **********2********** **********2********** **********2********** **********2**********. Following several weeks of installation, configuration, and equipment swap-out, the **********2********** were placed into the production environment between August 3 and October 6, 2019.

We reviewed the November 2019 IBM mainframe platform inventory and identified the following discrepancies:

- The **********2********** already operating in the production environment were not listed in the inventory.
- Of the **********2********** that were documented, **********2********** **********2********** were listed as *In Use,* but they should have been listed as

[12] IRS, *Asset Management – User and Network Services Hardware User Guide,* Version 1.0 (Nov. 2017).
[13] Pub. L. No. 113-283, 128 Stat. 3703. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

In Stock. **********2********** were listed as *In Stock,* but no updates were submitted to indicate that they needed to be *Retired*.

The initial asset records for the **********2********** computers were created on October 24, 2019, 107 calendar days following receipt of the equipment. The Asset Management – UNS Hardware User Guide states that initial asset records must be submitted to be updated within 10 workdays of receipt of the equipment to notify the Hardware Asset Management office that the equipment has been received.

The **2** Support Branch officials stated that, despite being responsible for the day-to-day management of the IBM mainframe platform inventory, they never received any formal training on IRS policies, procedures, forms, or operating tools relating to hardware asset management. As a result, they were unaware of the requirement to submit tickets to create asset records within 10 days of receipt of the equipment. Throughout the course of the audit, the **2** Support Branch worked closely with the User and Network Services function's Hardware Asset Management office to correct all of the discrepancies we identified. As a result, the March 2020 inventory report provided an accurate and up-to-date list of **********2********** associated with the IBM platform.

Without accurate inventories of the IBM mainframe platform, the IRS cannot ensure that it is properly monitoring and maintaining mainframe computer components in a secure manner.

The Chief Information Officer should:

Recommendation 5: Ensure that a comprehensive and accurate inventory of the IBM mainframe platform system components is maintained that includes the level of detail necessary for tracking and reporting.

Management's Response: The IRS agreed with this recommendation. The Enterprise Operations function will ensure that a comprehensive and accurate inventory of the IBM mainframe platform system components is maintained, which will include the level of detail necessary for tracking and reporting.

Recommendation 6: Ensure that personnel are properly trained to understand and comply with IRS policies and procedures governing hardware asset management.

Management's Response: The IRS agreed with this recommendation. The Enterprise Operations function will ensure that personnel are properly trained to understand and comply with IRS policies and procedures governing hardware asset management.

Recommendation 7: Establish a reconciliation procedure that includes communication between the affected functions that update and validate the IBM mainframe platform hardware asset inventory.

Management's Response: The IRS agreed with this recommendation. The Enterprise Operations function will establish internal written reconciliation procedures with appropriate functions responsible for the update and validation of the IBM mainframe platform hardware asset inventory and ensure that these procedures are disseminated to all key personnel.

Two Security Policies Were Not Met

We evaluated whether the IBM mainframe platform has implemented adequate tools and processes to detect and remediate software vulnerabilities and ensure protection from malicious code. To minimize the exposure of these vulnerabilities, organizations implement vulnerability management practices designed to proactively mitigate or prevent the exploitation of system vulnerabilities. This process involves the identification, classification, remediation, and mitigation of various vulnerabilities within a system.

Vulnerability scanning and remediation

We determined that the IRS implemented the necessary tools and processes to detect and remediate software vulnerabilities on its IBM mainframe platform. The IRM requires system owners to deploy vulnerability scanning tools that scan, at least monthly, for software flaws and improper configurations and measure vulnerability impacts. The IRM also requires that legitimate vulnerabilities be remediated in accordance with agency approved response times based on the severity level of the vulnerability. Vulnerabilities are prioritized by Common Vulnerability Scoring System scores provided by the scanning tools. Figure 5 shows vulnerability severity risk-level score ranges and their associated remediation timeframes.

Figure 5: Common Vulnerability Scoring System Ranges by Severity Risk Level and Remediation Timeframes

Score Range	Vulnerability Severity Risk Level	Remediation Timeframe
0.0	None	None
0.1–3.9	Low	180 Days
4.0–6.9	Medium	120 Days
7.0–8.9	High	High-Value Assets = 60 Days All Other Systems = 90 Days
9.0–10.0	Critical	30 Days

Source: IRM 10.8.1.

In addition, the IRM states that all information systems with an overall Medium or High Federal Information Processing Standard risk rating are to implement privileged access authorization to all information system components for selected vulnerability scanning activities to facilitate more thorough scanning.[14] Scans that use these privileged access authorizations are called credentialed or authenticated scans. Examples of significant advantages to vulnerability scanning while authenticated to the host are:

- Credentialed scans reveal much more information about what is running on the hosts that leads to testing for more vulnerabilities.
- Credentialed scans are more accurate with a lower rate of false positives.

[14] **********2**********2**********.

We requested credentialed vulnerability reports for the IBM mainframe platform. The IRS provided uncredentialed vulnerability scan reports for August 2019, September 2019, November 2019, and December 2019. Based on our evaluation of the uncredentialed reports, we determined the following:

- 4,146 unique vulnerabilities, to include: 46 critical vulnerabilities, 134 high vulnerabilities, 66 medium vulnerabilities, and 3,900 low vulnerabilities.
- 33 of the 46 critical vulnerabilities have exceeded the IRS policy of 30 days for remediation.
- 10 of the 134 high vulnerabilities have exceeded the IRS policy of 60 days for remediation.

**********2**********. Officials from both the Cybersecurity and Enterprise Operations functions provided evidence demonstrating that these findings were false positives. In addition, the Cybersecurity function's Enterprise Vulnerability Scanning office is working with the vendor to develop a fix that will prevent the false positive from reappearing in future vulnerability scans.

The 10 high vulnerability findings resulted from **********2********** **********2**********. These vulnerabilities are also presenting operational challenges throughout the IRS enterprise, affecting a total of **********2********** **********2**********. As a result, an enterprise-wide Plan of Action and Milestones was created to track both findings across all operating systems and is still in process.

On December 13, 2019, the Enterprise Technical Assessment office stated that it could not perform **********2**********. We met with employees from the vulnerability scanning vendor, who confirmed that performing *********2********** ******2***** is not possible primarily due to a lack of known vulnerabilities to develop adequate tests and Common Vulnerability Scoring System scores.

Existing IRM procedures require that, if a security control or requirement cannot be met, then a risk-based decision is needed for the deviation from the existing policy. When asked if a risk-based decision existed for this issue, the Enterprise Vulnerability Scanning office stated that there was no risk-based decision related to the **********2**********. Following our discussion, the Cybersecurity organization initiated management action by developing the risk-based decision, which was approved on May 6, 2020.

Malicious code protections

In addition to vulnerability scanning and remediation, the IRS is required to protect information systems from malicious code. Malicious code protection mechanisms shall be updated whenever new releases are available in accordance with IRS configuration management policy and procedures and shall be configured to perform weekly scans. According to IBM subject matter experts, however, the IRS IBM mainframe platform does not implement malicious code mechanisms due to a lack of known viruses that would allow for virus definition development. Officials from the Cybersecurity and Enterprise Operations functions stated that there was no requirement for a risk-based decision regarding this deviation from policy because another internal security policy included an exception stating that, if the mainframe has no function or capability for providing malicious code scanning or protection, this requirement is not applicable. However, during a follow-on conversation, a management official from the

Cybersecurity function's Architecture and Implementation Division agreed to update a previously approved 2015 risk-based decision related to this finding and route for approval.

According to IRS policy, organizations should thoroughly document a security weakness, the risks arising from the weakness, all mitigations which were considered, the cost of mitigations, and their technical feasibility in order for the Authorizing Official to make informed risk-based decisions.[15] The National Institute of Standards and Technology[16] states that leaders must recognize that explicit, well-informed, risk-based decisions are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure. The National Institute of Standards and Technology also states that effectively managing information security risk for an organization requires, in part, ongoing recognition and understanding by senior leaders and executives of the information security risks to organizational operations and assets arising from the operation and use of information systems. By not adhering to the risk-based decision process, critical infrastructure and information technology assets may not be properly protected from external attacks or potential insider threats. Without explicit, well-informed, risk-based decisions, the IRS risks leadership being uninformed of security risks posed by these information systems.

Recommendation 8: The Chief Information Officer should develop and approve a risk-based decision for deviating from IRM 10.8.32, which requires mainframe computers to automatically update malicious code protection mechanisms, and configure these mechanisms to perform weekly scans of the information system.

Management's Response: The IRS agreed with this recommendation. The Enterprise Operations function will work with Cybersecurity Architecture & Implementation Architect and Engineering Advisory Security Policy in submitting a risk-based decision with the Authorizing Official.

The Department of the Treasury Cybersecurity Analysis and Reporting Dashboard Report Was Inaccurate and Incomplete

The Cybersecurity function's Office of Strategy and Business Analytics is responsible for all facets of the monthly Department of the Treasury Cybersecurity Analysis and Reporting Dashboard (CARD) submission. This includes requesting and consolidating data inputs from key stakeholders and subject matter experts, reviewing inputs for possible errors and anomalies, and submitting the final report to the Department of the Treasury. **********2**********
**********2**********.[17]
**********2**********
**********2**********. As a result, 52 logical partitions were unreported.

[15] IRS, *Risk Acceptance and Risk-Based Decision Standard Operating Procedures,* Version 7.0 (Apr. 2020).
[16] National Institute of Standards and Technology, Special Publication 800-39, *Managing Information Security Risk* (Mar. 2011).
[17] To satisfy this reporting requirement, the IRS reports the total number of logical partitions operating within the mainframe systems.

**********2**********
**********2**********:

- **********2**********
  **********2**********
  **********2**********
  **********2**********.
- **********2**********
  *********2**********.

The FISMA directs Federal agencies to report annually to the Office of Management and Budget Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and on compliance with the FISMA. In addition to the annual FISMA reporting requirements, the Office of Management and Budget also directs Federal agencies to report monthly on key information security metrics. To support the IRS's monthly data collection process, the Cybersecurity function's Office of Strategy and Business Analytics uses a Data Collection Matrix to identify subject matter experts, points of contact, and data sources for each of the CARD's different reporting areas. However, no subject matter experts or data sources were listed for the mainframe portion of the Data Collection Matrix.

We found that multiple groups within the Enterprise Operations function are indirectly involved in the monthly data collection process; however, no specific group has been assigned the responsibility of ensuring accurate logical partition data collection and reporting to support the CARD report. Although the Enterprise Operations function's Authorizing Official Management Branch's mission statement clearly indicates that it provides direct support for General Support System accreditation, including inventory, status, and metric reporting, Enterprise Operations function officials emphasized that they were not involved with the CARD reporting process.

**********2**********
**********2**********
******2*****. Without accurate logical partition reporting, senior IRS leadership and executive and external stakeholders will not have accurate information for decisionmaking.

Recommendation 9: The Chief Information Officer should ensure that the CARD Data Collection Matrix is updated with procedures to include validated subject matter experts, data sources, and all reportable mainframe logical partitions connected to unclassified networks to ensure that accurate information is reported to the Department of the Treasury.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity function, with support from the Enterprise Operations function's subject matter experts, will ensure that the CARD Data Collection Matrix is updated with procedures to include validated subject matter experts, data sources, and all reportable mainframe logical partitions connected to unclassified networks to ensure that accurate information is reported to the Department of the Treasury.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the effectiveness and efficiency of the IRS's mainframe systems security and operations. To accomplish our objective, we:

- Determined whether **********2********** met minimum baseline security controls established by the National Institute of Standards and Technology and the IRM by reviewing security configuration setting reports, Online 5081 access authorizations, and the updated Online 5081 Manager Guide.
- Determined the completeness and accuracy of the **********2********** hardware asset inventory by reviewing relevant National Institute of Standards and Technology guidance, IRS policies, and multiple **********2********** *****2**** inventory reports.
- Determined whether proper controls were in place to discover and remediate security vulnerabilities on the **********2********** based on security controls established by the National Institute of Standards and Technology and the IRM. We reviewed multiple security vulnerability reports and interviewed vendors to determine system capabilities and limitations.
- Determined the completeness and accuracy of the reported total number of mainframe logical partitions on the monthly Treasury CARD report by reviewing monthly Treasury CARD reports, **********2********** summary reports, and monthly FISMA metric reports.

Performance of This Review

This review was performed during the period October 2019 through June 2020 at the **2** **********2**********. We worked closely with the Information Technology organization's Cybersecurity, Enterprise Operations, and User and Network Services functions. We conducted this performance audit 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 Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jena Whitley, Director; Jason McKnight, Audit Manager; Naomi Koehler, Lead Auditor; Mike Curtis, Senior Auditor; and Johnathan D. Elder, Information Technology Specialist, Applied Research and Technology.

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. We determined that the

following internal controls were relevant to our audit objective: National Institute of Standards and Technology requirements for the administration of mainframe computer security and IRM policies related to mainframe security administration and inventory procedures. Through interviews with IRS employees and analysis of relevant documentation provided by the IRS, we were able to determine whether the mainframe platform was administered effectively in order to maintain the confidentiality, integrity, and availability of tax and financial data that are integral to supporting tax processing operations. We obtained data from IRS systems to evaluate IBM mainframe platform access controls, to include user accounts, service accounts, and privileged accounts. We also examined inventory reports developed from the ******2***** **********2********** and the Department of the Treasury CARD reports.

Appendix II

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Reliability of Information – Actual; ***2*** mainframe computers were not accurately listed on the November 2019 **********2********** inventory report (see Recommendation 5).

Methodology Used to Measure the Reported Benefit:

We reviewed **********2**********. We also performed site visits **********2********** **********2**********, to verify the location, barcode, and serial number of all IBM Mainframe Platform assets. Our analysis determined that the November 2019 **********2********** **********2********** inventory report did not accurately list *******2******* mainframe computers.

Type and Value of Outcome Measure:

- Reliability of Information – Actual; 52 logical partitions connected to unclassified networks were not accurately listed on the February 2020 Department of the Treasury CARD report (see Recommendation 9).

Methodology Used to Measure the Reported Benefit:

We reviewed the IRS's submission for the February 2020 CARD monthly report. Our analysis determined that the February 2020 CARD report included **********2********** ******2*****. We determined that the IRS should have reported that ********2********** ******2********* were connected to its unclassified networks. This resulted in 52 ********2******* ******2***** unreported logical partitions.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

August 14, 2020

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger Nancy A. Sieger Digitally signed by Nancy A. Sieger Date: 2020.08.14 17:00:30 -04'00'
Acting, Chief Information Officer

SUBJECT: Response to Draft Audit Report – Mainframe Computing Environment Security Needs Improvement

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. We appreciate your acknowledgment of the Internal Revenue Service's (IRS) success in Mainframe Computing Environment Security, and that you acknowledge that our access controls are working as intended, as they continue to provide functionality to maintain the confidentiality, integrity, and availability of tax and financial data that are integral to support tax processing operations. We appreciate your recommendations on how to improve the security posture.

We concur with the recommended measurable benefits on tax administration, as noted in the July 15th memo and the draft report. In response to your recommendations, we have attached our corrective action plan. We are committed to implementing the corrective actions.

The IRS values the continued support and assistance provided by your office. Should you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Darrin Brown, Director, Enterprise Server Division, at (202) 384-8570.

Attachment

Attachment

Draft Audit Report – Mainframe Computing Environment Security Needs Improvement (Audit # 202020001)

RECOMMENDATION 1: Prioritize resources to ensure that the **********2********** *******2****** follow-on solution is delivered without further delay in order to maintain the confidentiality, integrity, and availability of data and information processed by the IBM mainframe platform.

CORRECTIVE ACTION 1: The Internal Revenue Service (IRS) agrees with this recommendation. The IRS will prioritize resources to ensure that the *******2********** *****2**** follow-on solutions **********2********** is delivered without further delay in order to maintain the confidentiality, integrity, and availability of data and information processed by the IBM mainframe platform. In addition, the IRS will maintain the**********2**********.

IMPLEMENTATION DATE: July 15, 2021

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 2: Ensure that the Security Regulatory Compliance Operations Team uses the **********2********** **********2********** during its review of the security and integrity of the IBM mainframe platform **********2********** until the follow-on solution is fully operational.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. Cybersecurity will implement the use of the **********2********** **********2********** to review the security and integrity of the IBM mainframe platform **********2********** until the delivery of alternate solutions and capabilities are available. The delivery of alternative solutions and capabilities is contingent on budgetary constraints.

IMPLEMENTATION DATE: November 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 3: Ensure that the **********2********** are timely remediated based on agency-defined timelines to protect the confidentiality, integrity, and availability of the information system.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. Cybersecurity has ensured that the **********2**********, which related to the **********2********** were timely remediated based on agency-defined timelines to protect the confidentiality, integrity, and availability of the information system.

Attachment

Draft Audit Report – Mainframe Computing Environment Security Needs Improvement (Audit # 202020001)

IMPLEMENTATION DATE: November 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 4: Ensure that the required **********2********** ********** **********2********** **********2********, are completed by **********2********** **********2********, rather than using the System Security Plan to validate the security and integrity of **********2**********.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. Cybersecurity will ensure **********2**********, which are conducted **********2**********, are completed **********2********** **********2**********.

IMPLEMENTATION DATE: November 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 5: Ensure that a comprehensive and accurate inventory of the IBM mainframe platform system components is maintained that includes the level of detail necessary for tracking and reporting.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. Enterprise Operations will ensure that a comprehensive and accurate inventory of the IBM mainframe platform system components is maintained, which will include the level of detail necessary for tracking and reporting.

IMPLEMENTATION DATE: September 15, 2020

OUTCOME MEASURE: Concur

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Operations

RECOMMENDATION 6: Ensure that personnel are properly trained to understand and comply with IRS policies and procedures governing hardware asset management.

CORRECTIVE ACTION 6: The IRS agrees with this recommendation. Enterprise Operations will ensure that personnel are properly trained to understand and comply with IRS policies and procedures governing hardware asset management.

IMPLEMENTATION DATE: December 15, 2020

Attachment

Draft Audit Report – Mainframe Computing Environment Security Needs Improvement (Audit # 202020001)
RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Operations

RECOMMENDATION 7: Establish a reconciliation procedure that includes communication between the affected functions that update and validate the IBM mainframe platform hardware asset inventory.

CORRECTIVE ACTION 7: The IRS agrees with this recommendation. Enterprise Operations will establish internal written reconciliation procedures with appropriate functions responsible for the update and validation of the IBM mainframe platform hardware asset inventory and ensure these procedures are disseminated to all key personnel.

IMPLEMENTATION DATE: September 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Operations

RECOMMENDATION 8: The Chief Information Officer should develop and approve a risk-based decision for deviating from IRM 10.8.32, which requires mainframe computers to automatically update malicious code protection mechanisms and configure these mechanisms to perform weekly scans of the information system.

CORRECTIVE ACTION 8: The IRS agrees with this recommendation. Enterprise Operations will work with Cybersecurity Architecture & Implementation Architect and Engineering Advisory Security Policy in submitting risk-based decision with the Authorizing Official (AO).

IMPLEMENTATION DATE: November 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Operations

RECOMMENDATION 9: The Chief Information Officer should ensure that the CARD Data Collection Matrix is updated with procedures to include validated subject matter experts, data sources, and all reportable mainframe logical partitions connected to unclassified networks to ensure that accurate information is reported to the Department of the Treasury.

CORRECTIVE ACTION 9: The IRS agrees with this recommendation. Cybersecurity, with support from Enterprise Operation's subject matter experts (SMEs), will ensure that the CARD Data Collection Matrix is updated with procedures to include validated SMEs, data sources, and all reportable mainframe logical partitions connected to unclassified networks to ensure that accurate information is reported to the Department of the Treasury.

Attachment

Draft Audit Report – Mainframe Computing Environment Security Needs Improvement
(Audit # 202020001)

IMPLEMENTATION DATE: November 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

OUTCOME MEASURE: Concur

Appendix IV

Glossary of Terms

Term	Definition
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems to which the information system is connected.
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.
Common Vulnerability Scoring System	An open framework for communicating the characteristics and severity of software vulnerabilities.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture or functionality of the information system.
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.
False Positive	An alert that incorrectly indicates that a vulnerability is present.
Federal Information Processing Standards Publication 199	Defines three levels of potential impact (low, moderate, or high) on organizations or individuals should there be a breach of security (*i.e.*, a loss of confidentiality, integrity, or availability). The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Federal Information Security Modernization Act of 2014	Amendment to The Federal Information Security Management Act of 2002 that allows for further reform to Federal information security, signed 12 years after the passing of the original law. This bill amends Chapter 35 of Title 44 of the United States Code (Pub. L. No. 113-283). The original statute requires agencies to assess risks to information systems and provide information security protections commensurate with the risks, integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget.
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.
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, personal electronic devices, thin clients, and multifunctional devices.

Logical Partition	Segments a high-capacity hardware configuration into multiple independent operating units. Each configuration is a distinct operating environment and may be grouped together, but the configurations need to be reviewed individually because they are often configured differently.
Mainframe	A powerful, multiuser computer capable of supporting simultaneously many hundreds of thousands of users.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
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.
Platform	A computer or hardware device, associated operating system, or a virtual environment on which software can be installed or run.
Privileged Accounts	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts.
Production Environment	The location where the real-time staging of programs that run an organization are executed, including the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
Protocols	A set of rules and formats, semantic and syntactic, permitting information systems to exchange information.
Radio Frequency Identifier	A technology that uses electromagnetic fields to automatically identify and track items.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Service Accounts	Represents a process or a set of processes to manage authentication service operations with the operating system or network resources.
Simple Mail Transfer Protocols	The primary protocol used to transfer electronic mail messages on the Internet.
Vulnerability	Weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.
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.

*********2******** *********2********	**********2********** **********2********** ******2*****.
*********2******** *********2******** *********2********	**********2********** **********2********** ******2**********.
*********2******** *********2********	**********2********** **********2**********.

Appendix V

Abbreviations

CARD	Cybersecurity Analysis Reporting Dashboard
DISA	Defense Information Systems Agency
ECC	Enterprise Computing Center
FISMA	Federal Information Security Modernization Act of 2014
IBM	International Business Machines
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
STIG	Security Technical Implementation Guide
2	**********2**********
2	**********2**********
2	**********2**********