

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Mainframe Platform Configuration Compliance Controls Need Improvement

September 30, 2022

Report Number: 2022-20-050

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 | www.treasury.gov/tigta

HIGHLIGHTS: Mainframe Platform Configuration Compliance Controls Need Improvement

Final Audit Report issued on September 30, 2022

Report Number: 2022-20-050

Why TIGTA Did This Audit

The IRS relies extensively on two mainframe platforms to support its financial and mission-related operations. This audit was initiated to determine the effectiveness of configuration management controls for the IRS mainframe platforms.

Impact on Tax Administration

In Fiscal Year 2021, the IRS processed more than 261 million tax returns and forms. It collected more than \$4.1 trillion in gross taxes and issued more than \$1.1 trillion in tax refunds (including \$586 billion in economic impact payments and advance child tax credits).

Security vulnerabilities within the mainframe platform can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing, all of which compromise the integrity, confidentiality, and availability of the platform and taxpayer data.

What TIGTA Found

The IRS mainframe platforms are not satisfying minimum security requirements in several key areas, including logical partition configuration compliance controls, vulnerability remediation, [REDACTED], and vulnerability age tracking. However, the mainframe change management process was mostly effective.

In February 2022, only [REDACTED]

[REDACTED] for at least the past five calendar years. Furthermore, the weighted configuration scores did not include the results of the completed [REDACTED]

The IRS did not approve a risk-based decision for a deviation from an existing agency security policy that requires systems and applications to be [REDACTED].

The configuration compliance issue age is not tracked by the mainframe vulnerability assessment tools. In addition, the IRS is [REDACTED] mainframe platform by using criteria that are no longer supported by the issuing authority.

Finally, the IRS could not provide documentation of executive approval for two emergency change requests that were implemented between February and March 2022.

What TIGTA Recommended

TIGTA made 10 recommendations to the Chief Information Officer. They include ensuring that the weighted configuration compliance scores include the results of the completed [REDACTED]; all required [REDACTED] are completed and validated; the checklist adjudication process for logical partitions is formalized; agency procedures are updated to include checklist adjudication requirements for mainframe platforms; data elements are added to the mainframe vulnerability reporting tool; phasing out use of the unsupported and outdated platform is considered; and emergency change requests are approved and documented adequately.

The IRS agreed with nine recommendations but disagreed with one. The IRS plans to base the configuration compliance score [REDACTED]; ensure monitoring of all production logical partitions; formalize the checklist adjudication process for logical partitions; and update checklist adjudication procedures to include mainframe platforms.

The IRS disagreed with the recommendation to consider phasing out its use of an unsupported and outdated platform. The IRS stated that it plans to continue exploring feasible solutions for modernizing critical business systems that run on this platform.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 30, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Mainframe Platform Configuration Compliance
Controls Need Improvement (Audit #202220021)

This report presents the results of our review to determine the effectiveness of configuration management controls for the Internal Revenue Service (IRS) mainframe platforms. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of 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

<u>Background</u>	Page 1
<u>Results of Review</u>	Page 2
<u>Mainframe Platforms Are Not Satisfying Minimum Security Requirements in Several Key Areas</u>	Page 2
<u>Recommendations 1 and 2:</u>	Page 7
<u>Recommendation 3:</u>	Page 8
<u>Recommendation 4:</u>	Page 10
<u>Recommendation 5:</u>	Page 11
<u>Recommendations 6 and 7:</u>	Page 12
<u>Configuration Vulnerability Age Is Not Tracked</u>	Page 12
<u>Recommendation 8:</u>	Page 12
<u>Configuration Compliance Criteria Being Used Are No Longer Supported</u>	Page 13
<u>Recommendation 9:</u>	Page 13
<u>The Mainframe Change Management Process Was Mostly Effective</u>	Page 13
<u>Recommendation 10:</u>	Page 16
Appendices	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 17
<u>Appendix II – Outcome Measures</u>	Page 19
<u>Appendix III – Management’s Response to the Draft Report</u>	Page 21
<u>Appendix IV – Glossary of Terms</u>	Page 27
<u>Appendix V – Abbreviations</u>	Page.30

Background

The mission of the Internal Revenue Service (IRS) is to provide America's taxpayers top quality service by helping them understand and meet their tax responsibilities and enforce the law with integrity and fairness to all. In Fiscal Year 2021, the IRS processed more than 261 million tax returns and forms.¹ It collected more than \$4.1 trillion in gross taxes and issued more than \$1.1 trillion in tax refunds (including \$586 billion in economic impact payments and advance child tax credits). To support these efforts, the IRS relies extensively on two mainframe platforms to support its financial and mission-related operations. The two mainframe platforms provide functionality to maintain the confidentiality, integrity, and availability of tax and financial data that are integral to support tax processing operations. As such, the IRS must ensure that its mainframe platforms are effectively secured to protect sensitive financial and taxpayer data and are operating as intended.

One platform employs the [REDACTED] mainframe infrastructure, which includes mainframe computers operating with either [REDACTED]. The [REDACTED] mainframes provide primary support for application programs and databases, including the Information Returns Master File, the Individual Master File, and the Automated Collection System, among others. The other platform employs the [REDACTED] mainframe infrastructure, which includes mainframe computers operating with the [REDACTED]. The [REDACTED] platform supports major tax applications, which include the Electronic Filing System and the Integrated Data Retrieval System.

The mainframe platforms are under the responsibility of the Information Technology organization's Enterprise Operations (EOps) function. In addition, the Cybersecurity function's Security Operations Branch performs reviews, analyzes, and reports compliance and security issues affecting the mainframe systems.

The [REDACTED] mainframe platform is comprised of eight mainframes; [REDACTED]. The [REDACTED] platform is comprised of four mainframes, with [REDACTED]. The mainframes are subdivided into logical partitions that support the production² and the development and testing environments. Figure 1 provides the active production logical partition distribution among the operating systems.

¹ See Appendix IV for a glossary of terms.

² During this review, we only evaluated logical partitions operating in the production environment.

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



Source: Treasury Inspector General for Tax Administration's (TIGTA) analysis of evidence provided by the IRS and through discussions with IRS management.

Results of Review

Mainframe Platforms Are 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 (NIST)³ provides security controls that are designed to facilitate compliance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Compliance with the NIST 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 organizationwide risk management program to effectively use the tailoring guidance and inherent flexibility in the NIST publications so that the selected security controls documented in organizational security plans meet the mission and business requirements of organizations. Finally, the Internal Revenue Manual (IRM)⁴ lays the foundation

³ NIST, Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5 (Sept. 2020).

⁴ IRM 10.8.33, *Information Technology Security, Mainframe System Security Policy* (Feb. 24, 2022).

to implement and manage minimum security controls and guidance for the use of mainframe systems for the purpose of protecting the agency against potential threats and vulnerabilities and ensures compliance with Federal mandates and legislation.

We found that both the [REDACTED] and the [REDACTED] mainframe platforms did not satisfy the minimum mainframe security requirements in several key areas, including logical partition configuration compliance controls, vulnerability remediation, [REDACTED], and vulnerability age tracking. Security weaknesses can have serious adverse effects on tax administration and the protection of taxpayer data.

Production logical partitions are not in compliance with configuration requirements

The IRM⁵ requires that vulnerability monitoring tools and techniques be used that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for enumerating platforms, software flaws, and improper configurations. In addition, the Department of Homeland Security states that each vulnerability found on a network should be given a numeric score, meant to represent the risk of not mitigating that vulnerability.⁶ Lastly, per the IRS user guide,⁷ hosts are considered compliant if their weighted compliance score is 90 percent or higher with no high-severity ratings.



In February 2022, the IRS's reported average weighted configuration compliance score for all [REDACTED] mainframe platform production logical partitions was [REDACTED] with configuration requirements. Figure 2 summarizes the [REDACTED] mainframe platform active production logical partition configuration compliance status by specific operating system.

⁵ IRM 10.8.1, *Information Technology Security, Policy and Guidance* (Sept. 28, 2021).

⁶ Department of Homeland Security, *Continuous Diagnostics and Mitigation, Agency-Wide Adaptive Risk Enumeration Technical Design Document* (Nov. 1, 2017).

⁷ IRS, *Hindustan Computer Limited BigFix Configuration Settings Management Dashboard User Guide, Ver. 1.0* (Nov. 19, 2020).

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



Source: TIGTA's analysis of IRS Mainframe Compliance Dashboard Reporting and evidence provided by the IRS.

In April 2022, the IRS also reported that both [redacted] production logical partitions were compliant with average weighted configuration compliance scores of [redacted]. [redacted] Figure 3 summarizes the [redacted] mainframe platform active production logical partition configuration compliance status for the [redacted] operating system.

Figure 3: April 2022 IRS Reported Average Weighted Configuration Compliance Scores and Compliant Active Production Logical Partitions for [redacted] Mainframes



Source: TIGTA's analysis of IRS Mainframe Compliance Dashboard Reporting and evidence provided by the IRS.

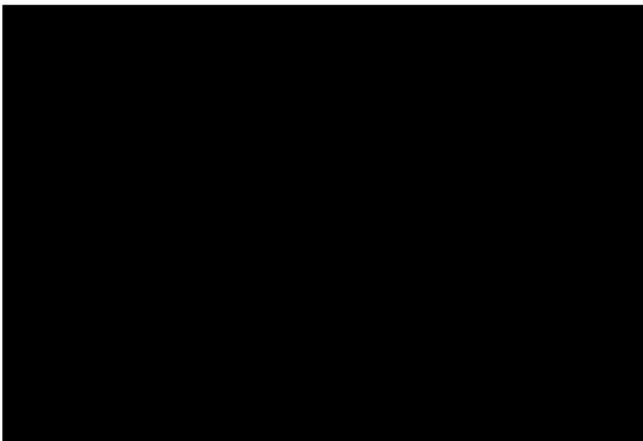
⁸ [redacted]

⁹ Our determination was based on both [redacted] logical partitions [redacted]

****2* production logical partitions**

We reviewed the February 2022 configuration compliance reporting dashboard results for the [redacted] active production [redacted] logical partitions and found that [redacted]

[redacted] check or having a weighted compliance score of less than [redacted]. More specifically, we found that [redacted]



The IRM states that legitimate vulnerabilities shall be remediated in accordance with agency-approved response times based on the severity level of the vulnerability. Vulnerabilities with the highest risk shall be prioritized and remediated first. High-risk vulnerabilities, if exploited, could result in elevated privileges and lead to significant data loss or system downtime. Similarly, medium-risk vulnerabilities, if exploited, could result in the loss of sensitive system information.

In September 2020,¹⁰ we reported that the follow-on solution to replace the current [redacted] tool had been delayed due to resource constraints and competing priorities. The IRS's initial implementation date of November 15, 2018, for the follow-on solution, [redacted], had been extended to July 15, 2021. The IRS agreed with our recommendation to prioritize resources to ensure that the [redacted] follow-on solution is delivered without further delay in order to maintain the confidentiality, integrity, and availability of data and information processed by the [redacted] mainframe platform. On June 29, 2021, the IRS began using [redacted] to validate the configuration compliance settings for the [redacted] mainframe [redacted] logical partitions.

We reviewed [redacted] configuration setting scan reports from October 2021 through March 2022 and determined there were a total of [redacted]

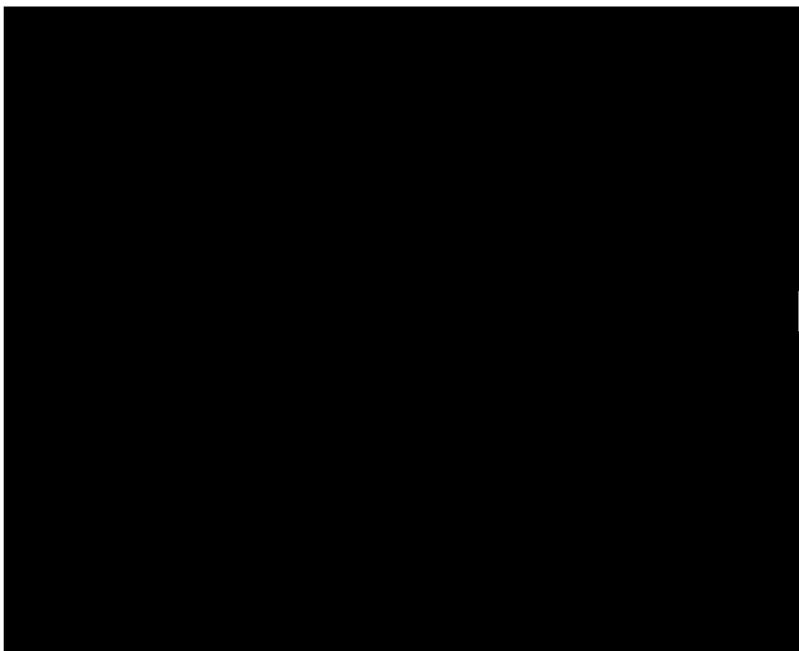
- [redacted]¹¹
- [redacted]

The following findings exceeded the IRS remediation response times:

- [redacted]
- [redacted]

¹⁰ TIGTA, Report No. 2020-20-045, *Mainframe Computing Environment Security Needs Improvement* (Sept. 2020).

¹¹ Several scanned mainframe logical partitions can have the same unique finding, *i.e.*, vulnerability. Therefore, one unique finding can occur multiple times across the mainframe platform.



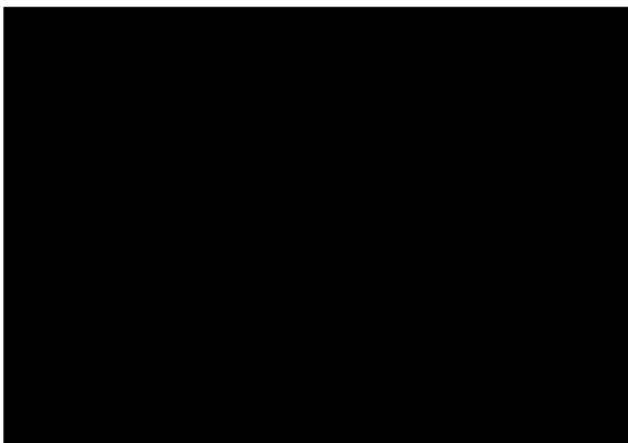
The IRM states that a Plan of Action and Milestones (POA&M) must be developed to document the planned remediation actions to correct system weaknesses or deficiencies. Further, the IRM states that both scan results and automated testing results can be added to a POA&M as multiple line items. On June 15, 2022, a management official from the EOps function's Authorizing Official Management Branch informed us that two POA&Ms were created to address the findings identified by the [REDACTED] and also to group together the medium- and high-risk findings. In addition, the POA&Ms will be used to capture findings identified in both new and future scans. Each finding within the associated POA&M has a unique identified milestone date that is used to track the mitigation of the finding. Lastly, the POA&M due date is the date the POA&M will be closed and no longer accept any new medium- or high-risk findings.

We confirmed that there are two active POA&Ms addressing the medium- and high-risk findings noted above, with planned completion dates of [REDACTED] [REDACTED].¹² We found that the IRS is making progress mitigating the individual findings within each of these POA&Ms while prioritizing the remediation efforts based on the vulnerability risk severity level. Failing to timely remediate medium- and high-risk [REDACTED] security vulnerabilities could compromise the security posture of the mainframe platform and could lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing, all of which compromise the integrity, confidentiality, and availability of the platform.

¹² POA&M 45117, which addresses the high-risk findings, has a planned completion date of [REDACTED]. POA&M 45125, which addresses the medium-risk findings, has a planned completion date [REDACTED].

****2** production logical partitions**

We reviewed the February 2022 configuration compliance reporting dashboard results for the [redacted] production [redacted] logical partitions and found that both were [redacted].



The Cybersecurity function's Counter Insider Threat Office stated that its office has been unable to validate the configuration setting compliance of the [redacted] logical partitions since December 2021 due to the EOps function not submitting evidence to support that the security controls are in place and working as intended. According to documentation we reviewed, the reason this evidence was not submitted is because the EOps function had not identified which organization is responsible for specific controls. In April 2022, during the course of our review, the EOps function stated that it will meet internally to identify the specific organization responsible for the implementation of the controls for the [redacted] logical partitions. Without completing the required monitoring of all production logical partitions, the IRS cannot adequately define its current security posture because [redacted].

The Chief Information Officer should:

Recommendation 1: Ensure that the IRS prioritizes establishing which organization is responsible for the implementation and management of specific configuration setting controls.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will identify the organization responsible for the implementation and management of specific configuration setting controls.

Recommendation 2: Ensure that the IRS performs required monitoring of all production logical partitions.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will develop a process ensuring monitoring of all production logical partitions.

****2*** production logical partitions**



[redacted] ¹³ On July 8, 2021, the IRS reported that this planned corrective action had been fully implemented and closed the

¹³ TIGTA, Report No. 2016-20-050, [redacted] (July 2016).

recommendation.¹⁴ However, when asked to provide evidence of completed [REDACTED] [REDACTED] has not been used for at least the past five calendar years.¹⁵ The management official further stated that not using the required [REDACTED] was an administrative oversight. On February 28, 2022, following our inquiry, the Counter Insider Threat Office began using the required [REDACTED] to validate the configuration compliance for the [REDACTED] mainframe logical partitions.

We reviewed the results of the [REDACTED] completed on March 31, 2022, for both [REDACTED] logical partitions and found that [REDACTED] logical partitions [REDACTED]. As a result, we determined that [REDACTED] logical partitions [REDACTED].

In April 2022, the IRS reported¹⁶ that the [REDACTED] logical partitions were satisfying agency configuration compliance requirements with an average weighted score [REDACTED]. However, we determined that this reporting only included assessment results from the [REDACTED]. As a result, the IRS inaccurately reported the configuration compliance status for the [REDACTED] logical partitions.

On March 24, 2022, a management official from the Cybersecurity function's Architecture and Implementation group stated that, because the reporting requirements for the [REDACTED] [REDACTED] as part of the [REDACTED] overall weighted compliance score. However, once this functionality has been added, the results of the [REDACTED] would be included in the overall weighted compliance score. Without accurate logical partition configuration compliance reporting, senior IRS leadership and executive stakeholders will not have accurate information for decision making.

Recommendation 3: The Chief Information Officer should ensure that the weighted configuration compliance scores include the results of completed [REDACTED].

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will base the configuration compliance score on all checks required [REDACTED].

¹⁴ The original due date for this planned corrective action was November 15, 2017.

¹⁵ The IRS was unable to provide an exact time period but confirmed that it has not used the required [REDACTED] since at least July 2016. In February 2022, the IRS began using the [REDACTED].

¹⁶ This reporting reflected configuration compliance assessments completed in March 2022.

Configuration compliance validation

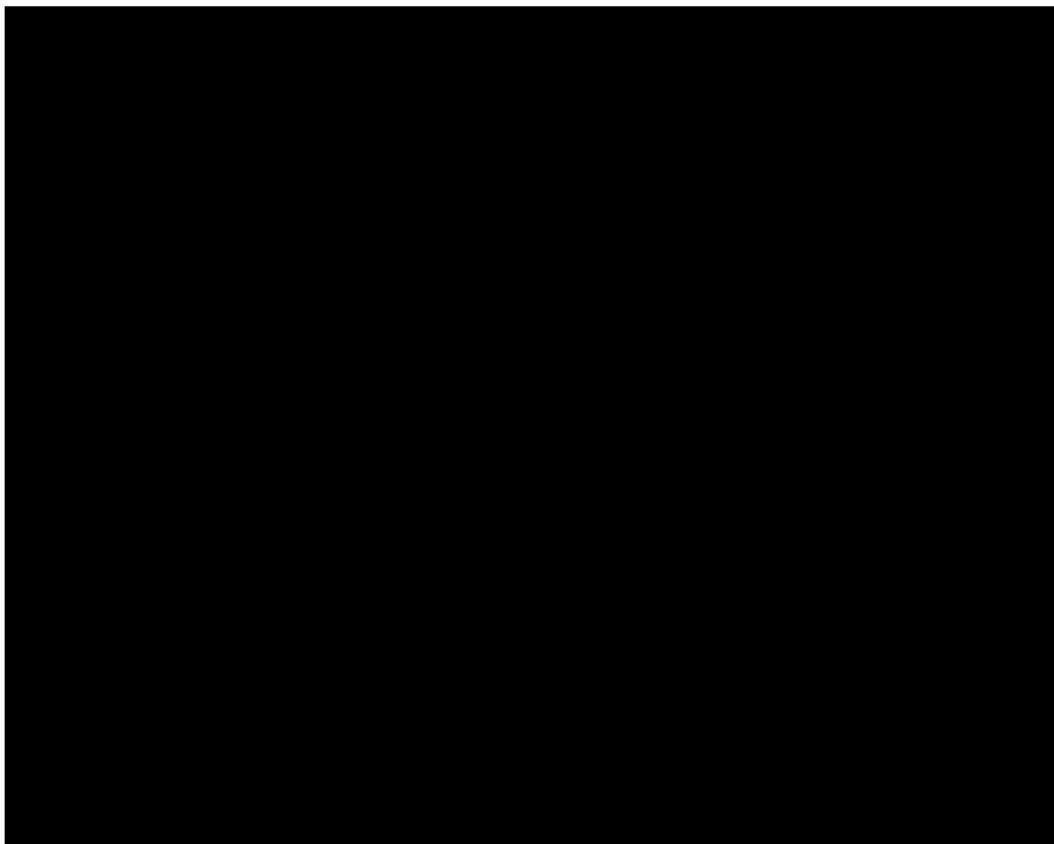
Per the IRM, all systems and applications are required to be [REDACTED]. Furthermore, automated mechanisms shall be used to manage, apply, and verify configuration settings for all systems components for which the IRS has defined configuration baselines. Because no automated scanning tool is available, the IRS uses a Defense Information Systems Agency (DISA)-published [REDACTED]¹⁷ for the [REDACTED] to validate the configuration compliance settings. In addition, the IRS uses a similar DISA-published [REDACTED]¹⁸ [REDACTED]. Lastly, agency security policies also require an actual examination of the [REDACTED].

On August 31, 2020, the Cybersecurity function's Counter Insider Threat Office implemented a new procedure for the [REDACTED] logical partitions that [REDACTED].

Agency security policies state 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 why the decision was made to not [REDACTED] per agency security requirements, a management official from the Cybersecurity function's Counter Insider Threat Office stated that they do not have the ability to satisfy the [REDACTED] requirement due to a lack of automation and resources. When asked if a risk-based decision for this deviation from an existing security requirement was approved, the Director, Cybersecurity Operations, stated that there was no risk-based decision for this issue because the agency believes it is meeting the intent of the security requirement. He further stated that, [REDACTED].

17 [REDACTED]

18 [REDACTED]



In September 2020,¹⁹ the IRS agreed with our recommendation to ensure that the required [redacted] for the [redacted]

[redacted] On November 10, 2020, the IRS reported that a planned corrective action had been implemented to [redacted] and closed the recommendation. We determined that using static documentation does not meet the intent of the security requirement for [redacted]. By failing to properly verify and [redacted] the security posture and the availability of the system could be compromised. In addition, 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.

The Chief Information Officer should:

Recommendation 4: Develop and approve a risk-based decision for deviating from the IRM, which requires all systems and applications to be [redacted]

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will develop and document a risk-based decision regarding the [redacted]

¹⁹ TIGTA, Report No. 2020-20-045, *Mainframe Computing Environment Security Needs Improvement* (Sept. 2020).

Recommendation 5: Ensure that all required [REDACTED] are completed by [REDACTED] including an actual examination of the logical partition systems.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will implement a process ensuring that actual examination of [REDACTED] on [REDACTED] logical partitions.

Mainframe configuration settings checklist adjudication process

According to the NIST,²⁰ common secure configurations, including configuration checklists, provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products. The NIST²¹ further states that organizations should review, customize, and test checklists to ensure that they comply with local rules, regulations, and mandates. In addition, the IRM states that the IRS should identify, document, and approve any deviations from established configuration settings for individual components with IRS systems based on explicit operational requirements.

Configuration settings checklist adjudication is a complex process involving numerous activities to successfully scope, review, approve, and implement approved [REDACTED]. The IRS stated that the checklist used to scan for configuration compliance for the [REDACTED] logical partitions is provided as part of a vendor installation package from the scanning tool vendor. When asked if there was a checklist adjudication process for the vendor-provided [REDACTED] checklist, the IRS stated that, while a review process for the [REDACTED] logical partitions does exist, it is less formal than what has been recently developed for Tier II devices as part of the Continuous Diagnostics and Mitigation program. The IRS added that the Continuous Diagnostics and Mitigation program plans to formalize the adjudication process for the [REDACTED] logical partitions checklists during Fiscal Year 2022.

Lastly, the IRS has published guidance related to checklist adjudication,²² which provides procedures for developing compliance adjudication packages for review and approval. However, we determined that this guidance does not include any information related to checklist adjudication for the mainframe platforms. A management official from the Cybersecurity function's Architecture and Implementation group stated that this occurred because the original guidance for the Continuous Diagnostics and Mitigation program that was developed by the Department of Homeland Security was limited to Tier II devices and did not extend to mainframe platforms. Without ensuring that this process occurs, critical and unique security requirements may not be applied to IRS mainframe systems.

²⁰ NIST, Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020).

²¹ NIST, Special Publication 800-70, Rev. 4, *National Checklist Program for IT Products-Guidelines for Checklist Users and Developers* (Feb. 2018). IT = Information Technology.

²² IRS, *Configuration Settings Management, Checklist Adjudication Standard Operating Procedures, Ver. 0.43* (Aug. 30, 2021).

The Chief Information Officer should:

Recommendation 6: Ensure that the checklist adjudication process for the [REDACTED] logical partitions is formalized to align with the current process for Tier II devices.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will formalize the checklist adjudication process for [REDACTED] logical partitions to align with the current process for Tier II devices.

Recommendation 7: Ensure that agency procedures are updated to include checklist adjudication requirements for the mainframe platforms.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will ensure that checklist adjudication procedures are updated to include all mainframe platforms.

Configuration Vulnerability Age Is Not Tracked

Vulnerability management is the process of identifying, categorizing, prioritizing, and resolving vulnerabilities in operating systems and enterprise applications. It is an ongoing process which seeks to identify vulnerabilities that can be remediated through patching and configuration of security settings. The IRM requires that vulnerabilities be remediated in accordance with agency-approved response times based on the severity level of the vulnerability.

We reviewed the February 2022 configuration vulnerability assessments and found that none of the mainframe vulnerability assessment tools²³ report the date first seen or date remediated for discovered configuration compliance issues. In response, management officials from the Cybersecurity function's Architecture and Implementation group stated that these data elements are not available for reporting on mainframe platforms. In addition, they stated that, when the configuration settings management capability for the mainframe platform is matured, this capability will be added during a future sprint as a Continuous Diagnostics and Mitigation requirement. However, this functionality is still in the assessment and planning phase, and there is no current timeline for this requirement to be added. Without age tracking capabilities for configuration compliance issues, remediation and prioritization will be inaccurate and inefficient, and mainframes will remain at risk.

Recommendation 8: The Chief Information Officer should prioritize adding the date first seen and date remediated data elements capability to the mainframe vulnerability reporting tool.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will add functionality to track aging of configuration vulnerabilities for mainframes.

²³ These tools include the [REDACTED]

Configuration Compliance Criteria Being Used Are No Longer Supported

The IRS has adopted as policy the more technically explicit controls in the DISA Security Technical Implementation Guides (STIG). In addition, the NIST requires Federal agencies to use appropriate security configuration checklists from the National Checklist Program when available.

[REDACTED]

24

[REDACTED]

Recommendation 9: The Chief Information Officer should consider phasing out the use of the unsupported and outdated [REDACTED] platform.

Management's Response: The IRS disagreed with this recommendation. The IRS will continue to explore feasible solutions for modernizing critical business systems that run on the [REDACTED] mainframes. The IRS goal is to establish a holistic mainframe migration process that improves performance while minimizing risk.

Office of Audit Comment: The IRS agrees that it is using [REDACTED] to evaluate [REDACTED] mainframe configuration compliance. However, we believe the continued use of the [REDACTED] could result in critical vulnerabilities not being timely detected and remediated, placing this platform at a higher risk. In addition, there is [REDACTED]

The Mainframe Change Management Process Was Mostly Effective

Changes such as upgrades to platforms are often needed to meet new business requirements and evolving demands. Changes to production environments or applications can introduce new or increase existing security vulnerabilities that heighten risk to the overall information

²⁴ DISA was unable to provide an exact time period, but it confirmed that the [REDACTED]

technology infrastructure. The process of tracking and monitoring changes to the IRS infrastructure is critical to effectively managing the individual information system and its supporting infrastructure as well as the information resources that support the daily activities of IRS employees.²⁵

We reviewed the process flow and associated roles and responsibilities for managing and documenting change requests (emergency, standard, normal, and Tier I code promotion) approved for implementation and subsequent scheduling of the deployment. We found that change management controls for standard, normal, and Tier I code promotion change requests were working as intended. However, we determined that change management controls for emergency change requests need improvement.

Code promotion change requests

The Production Environment Control Process is a year-round, automated process for approving changes to the various information technology environments. Any update that changes the information technology configuration baseline is required to be approved by the appropriate authority based on an assessment of the risk and the resulting approval level.

From October 1, 2021, through March 14, 2022, there were 69 moderate- to high-risk-level code promotion changes implemented on the production mainframe platforms. We judgmentally sampled²⁶ nine of the 69 code promotion changes and evaluated whether they met minimum agency requirements related to change management policies and procedures. We determined that all nine of the code promotion changes satisfied minimum agency change management requirements. Figure 4 summarizes the mainframe code promotion changes and required approval levels.

Figure 4: Summary of Mainframe Code Promotion Changes Implemented From October 2021 Through March 2022

Code Promotion Change Ticket Number	Approval Time Period	Required Approval Level	Met Agency Requirements
C00093513	Non-Filing Season	Section Chief	Yes
C00094704			
C00098303			
C00109647			
C00102260			
C00104137			
C00106717	Elevated	Associate Chief Information Officer Approval Group	Yes
C00115426			
C00115543			

Source: TIGTA’s analysis of evidence provided by the IRS and through discussions with IRS management.

²⁵ IRS, *IT Cybersecurity Security Change Management Standard Operating Procedures, Ver. 8* (Nov. 24, 2020).

²⁶ A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Agency requirements state that code promotion change requests can be approved at the Section Chief level during a non-filing season period.²⁷ In addition, during the high-risk and elevated approval periods, approval from an authorized executive is required. Of the nine change requests evaluated, two change requests were within the elevated approval period time frame.

- For the two code promotion change requests implemented during the elevated approval period, approval was granted by an authorized approver within the Associate Chief Information Officer Approval Group.
- For the seven code promotion change requests implemented during the non-elevated and non-high-risk period, approval was granted by a Section Chief.

Emergency change requests

Per the IRS's Change Management procedures,²⁸ emergency change requests bypass the Knowledge Incident/Problem Service and Asset Management approval process. Therefore, any required approvals should be documented either through the Incident Management process, such as during a Service Restoration Team call, or via other means outside of Knowledge Incident/Problem Service and Asset Management. In addition, the Information Technology Operations Command Center procedures²⁹ state that the Management Service Restoration Team meeting is where approval for an emergency change request is granted. Lastly, according to the Production Environment Control Process,³⁰ in order to resolve a Priority One or Priority Two incident ticket, a change must be approved by an authorized executive or a delegated proxy approver.

As part of our review, we evaluated three moderate-risk emergency change requests that were implemented between January 2022 and March 2022. We determined that two (67 percent) of the three emergency change requests did not satisfy minimum agency requirements.

We reviewed two Priority Two incident tickets that were created in Knowledge Incident/Problem Service and Asset Management on February 24, 2022, and March 3, 2022, respectively, relating to work stoppages on an application supported by the [REDACTED] mainframe platform. Once the root cause and solution were identified, emergency change requests were created for both incidents to track and monitor the implementation of the solutions. Because these tickets were created during the 2022 Filing Season, approval is required by an executive or a delegated proxy approver.

For the incident ticket from February 24, 2022, while the incident details log does indicate that the emergency change request was approved, there is no record of the authorized executive who performed this action. Despite providing numerous responses, the IRS was unable to provide sufficient evidence documenting which executive approved this change request.

²⁷ [REDACTED] are designated [REDACTED]. In addition, [REDACTED] is designated as an elevated approval period.

²⁸ IRS, *IT Change Management Procedure Transmittal* (May 18, 2017).

²⁹ IRS, *IT Operations Command Center Incident and Problem Management Branch Incident Management Section Standard Operating Procedures* (Apr. 2022).

³⁰ IRS, *Reference Guide for the Production Environment Control Process for 2022, Ver. 1.3* (Apr. 2022).

For the incident ticket from March 3, 2022, there is also no record of approval by an authorized executive. An official from the Applications Development function's Delivery Management Redesign Branch stated that, since the Incident Manager of Record had already approved the change, the Filing Season team did not submit the change request for executive-level approval. However, the Incident Manager of Record is a Section Chief and is not authorized to approve emergency change requests. For both incidents, the IRS failed to properly document the required executive-level approval due to the urgency of implementing the required code fixes. Without following the Change Management procedures, there is an increased risk that changes could expose taxpayer data to unauthorized access or unauthorized data sharing.

Recommendation 10: The Chief Information Officer should ensure that emergency change requests are approved and documented based on agency-defined policies and procedures.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that emergency change requests are approved and documented based on agency-defined policies and procedures.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine the effectiveness of configuration management controls for the IRS mainframe platforms. To accomplish our objective, we:

- Determined whether medium- and high-risk configuration vulnerabilities were timely remediated within agency security policies by reviewing mainframe configuration scan reports. We also reviewed relevant IRMs and interviewed IRS personnel to determine the tools and technologies used for mainframe configuration scans.
- Evaluated the checklist adjudication process in place for mainframes by reviewing the IRS Standard Operating Procedure for checklist adjudication and relevant IRMs and NIST publications for checklist requirements. We also interviewed IRS personnel to determine the sources of checklists used in mainframe configuration scans.
- Determined the appropriate process flow for each change request based on their change category and evaluated whether the changes were implemented by authorized personnel by obtaining and reviewing reports of changes to the mainframes. We also reviewed the policies and procedures for managing and documenting change requests approved for implementation and interviewed IRS personnel.

Performance of This Review

This review was performed during the period October 2021 through July 2022. Due to the ongoing Coronavirus Disease 2019 pandemic, we conducted all audit work virtually. We held meetings and interviews via teleconference. We worked closely with the Information Technology organization's Cybersecurity and EOps 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, Director; Mike Curtis, Acting Audit Manager; Daniel Preko, Lead Auditor; Paula Benjamin-Grant, Auditor; and Julia Woods, Information Technology Specialist (Data Analytics).

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 reviewed IRM policies related to the logical control of information technology, Standard Operating Procedures for checklist adjudication, baseline system configurations, and configuration scanning of production systems. We evaluated controls by interviewing personnel in the Cybersecurity, and EOps

Mainframe Platform Configuration Compliance Controls Need Improvement

functions and by reviewing documentation including policies and procedures related to configuration scanning, change management, and scanning reports.

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: Potential; [REDACTED] logical partitions with inaccurately reported configuration compliance statuses (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

We reviewed the results of [REDACTED] completed on March 31, 2022, for [REDACTED] logical partitions and found that both logical partitions [REDACTED]. As a result, per agency requirements, we determined that [REDACTED] logical partitions were [REDACTED].

In April 2022, the IRS reported that [REDACTED] logical partitions were satisfying agency configuration compliance requirements, with an average weighted score of [REDACTED]. However, we determined that this reporting only included assessments results from the [REDACTED] tool and did not include the results of [REDACTED].

Type and Value of Outcome Measure:

- Reliability of Information: Potential; one planned corrective action inaccurately reported as implemented for a recommendation related to the required [REDACTED] security configuration compliance checks for the [REDACTED] logical partitions (see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

On August 31, 2020, the Cybersecurity function's Counter Insider Threat Office implemented a new procedure for the [REDACTED] logical partitions that [REDACTED].

When asked if a risk-based decision for this deviation from an existing security requirement was approved, the Director, Cybersecurity Operations, stated that there was no risk-based decision for this issue because the agency believes it is meeting the intent of the security requirement. He further stated that, [REDACTED] the IRS includes the relevant operational and managerial controls in its review of the [REDACTED] logical partitions as these controls are in the form of static

documentation. We determined that using static documentation does not meet the intent of the security requirement for validating the [REDACTED]

In September 2020,¹ the IRS agreed with our previous recommendation to ensure that the required [REDACTED]

[REDACTED] On November 10, 2020, the IRS reported that the planned corrective action related to the above recommendation had been implemented and closed the recommendation. We determined that the recommendation was inaccurately closed because the IRS continues to not perform an actual examination of the [REDACTED]

¹ TIGTA, Report No. 2020-20-045, *Mainframe Computing Environment Security Needs Improvement* (Sept. 2020).

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CHIEF INFORMATION OFFICER

August 30, 2022

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger /s/ Nancy A. Sieger
Chief Information Officer

SUBJECT: Draft Audit Report – Mainframe Platform Configuration
Compliance Controls Need Improvement (Audit # 202220021)

Thank you for the opportunity to review and comment on the draft audit report. Configuration management controls are important to ensuring the effectiveness of tax processing operations, and the IRS is committed to increasing the overall effectiveness of our information technology infrastructure. The IRS' mainframe platforms are effective, with multi-layered security in place to ensure the integrity of our operating systems.

We have taken several steps to address the process improvements identified in the draft audit report. As noted by the audit team, we are mitigating risks to mainframes while prioritizing remediation efforts based on the vulnerability risk severity level. With one exception, we agree with the audit team's recommendations and have provided a detailed corrective action plan. We do not agree that the TIGTA recommendation to move away from [REDACTED] mainframe systems is within scope of this audit. The [REDACTED] mainframe systems in use at the IRS are highly effective and secure and we do not have plans to phase out use of [REDACTED] in the near-term. We continue to explore feasible solutions for modernizing critical business systems as part of the larger effort to continuously modernize in a secure operating environment without any major disruptions to the tax system. We will continue to focus on security and improving performance while minimizing risk.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Frank Henderson, Director, Security Operations and Standards, at (681) 260-3680.

Attachment

Mainframe Platform Configuration Compliance Controls Need Improvement

Attachment

Draft Audit Report – Mainframe Platform Configuration Compliance Controls Need Improvement (Audit # 202220021)

RECOMMENDATION 1

The Chief Information Officer should ensure that the IRS prioritizes establishing which organization is responsible for the implementation and management of specific configuration setting controls.

CORRECTIVE ACTION

The IRS agrees with this recommendation. The IRS will identify the organization responsible for the implementation and management of specific configuration setting controls and identify the responsible organization.

IMPLEMENTATION DATE

November 15, 2022

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Enterprise Operations

RECOMMENDATION 2

The Chief Information Officer should ensure the IRS performs required monitoring of all production logical partitions.

CORRECTIVE ACTION

The IRS agrees with this recommendation. The IRS will develop a process ensuring monitoring of all production logical partitions.

IMPLEMENTATION DATE

November 15, 2022

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Cybersecurity

Attachment

Draft Audit Report – Mainframe Platform Configuration Compliance Controls Need Improvement (Audit # 202220021)

RECOMMENDATION 3

The Chief Information Officer should ensure that the weighted configuration compliance scores include the results of completed [REDACTED]

CORRECTIVE ACTION

The IRS agrees with this recommendation. The IRS will base the configuration compliance score on all checks required [REDACTED]

IMPLEMENTATION DATE

April 15, 2023

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 4

The Chief Information Officer should develop and approve a risk-based decision for deviating from the IRM, which requires all systems and applications to be [REDACTED]

CORRECTIVE ACTION

The IRS agrees with this recommendation. The IRS will develop and document a risk-based decision [REDACTED]

IMPLEMENTATION DATE

November 15, 2022

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Cybersecurity

Attachment

Draft Audit Report – Mainframe Platform Configuration Compliance Controls Need Improvement (Audit # 202220021)

RECOMMENDATION 5

The Chief Information Officer should ensure that all required [REDACTED] are completed by [REDACTED], including an actual examination of the logical partition systems.

CORRECTIVE ACTION

The IRS agrees with this recommendation. The IRS will implement a process ensuring actual examination of configuration compliance checks are completed monthly on all logical partitions.

IMPLEMENTATION DATE

November 15, 2022

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 6

The Chief Information Officer should ensure the checklist adjudication process for [REDACTED] logical partitions is formalized to align with the current process for Tier II devices.

CORRECTIVE ACTION

The IRS agrees with this recommendation. The IRS will formalize the checklist adjudication process for [REDACTED] to align with the current process for Tier II devices.

IMPLEMENTATION DATE

April 15, 2023

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Cybersecurity

Mainframe Platform Configuration Compliance Controls Need Improvement

Attachment

Draft Audit Report – Mainframe Platform Configuration Compliance Controls Need Improvement (Audit # 202220021)

RECOMMENDATION 7

The Chief Information Officer should ensure that agency procedures are updated to include checklist adjudication requirements for the mainframe platforms.

CORRECTIVE ACTION

The IRS agrees with this recommendation. The IRS will ensure checklist adjudication procedures are updated to include all mainframe platforms.

IMPLEMENTATION DATE

July 15, 2023

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 8

The Chief Information Officer should prioritize adding the date first seen and date remediated data elements capability to the mainframe vulnerability reporting tool.

CORRECTIVE ACTION

The IRS agrees with this recommendation. The IRS will add functionality to track aging of configuration vulnerabilities for mainframes.

IMPLEMENTATION DATE

December 15, 2022

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Cybersecurity

Attachment

Draft Audit Report – Mainframe Platform Configuration Compliance Controls Need Improvement (Audit # 202220021)

RECOMMENDATION 9

The Chief Information Officer should consider phasing out its use of the unsupported and outdated [REDACTED] platform.

CORRECTIVE ACTION

The IRS disagrees with the recommendation to consider phasing out its use of the [REDACTED] platform in the near-term. The IRS will continue to explore feasible solutions for modernizing critical business systems that run on the [REDACTED] mainframes. Our goal is to establish a holistic mainframe migration process that improves performance while minimizing risk.

IMPLEMENTATION DATE

N/A

RESPONSIBLE OFFICIAL(S)

N/A

RECOMMENDATION 10

The Chief Information Officer should ensure that the emergency change requests are approved and documented based on agency-defined policies and procedures.

CORRECTIVE ACTION

The IRS agrees with this recommendation. The IRS will ensure that emergency change requests are approved and documented based on agency-defined policies and procedures.

IMPLEMENTATION DATE

October 15, 2022

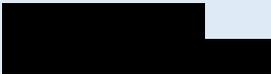
RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Enterprise Operations

Glossary of Terms

Term	Definition
Application	A software program hosted by an information system.
Approval	The activity required to deploy a change.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affects the security posture or functionality of the information system.
Continuous Diagnostics and Mitigation	A program providing cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security posture.
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.
Elevated Privilege	Any user right assignment that is above the baseline.
Emergency Change	A change whose trigger is an interruption of service requiring expedited or immediate action.
Enterprise Computing Center	Supports tax processing and information management through a data processing and telecommunications infrastructure.
Filing Season	The period from January 1 through mid-April when most individual income tax returns are filed.
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.
Incident	An unplanned interruption to an information technology service or reduction in the quality of an information technology service.
Incident Management	The process responsible for managing the life cycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized.
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.
Internal Revenue Manual	Primary source of instructions to employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Knowledge Incident/Problem Service and Asset Management	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.

Mainframe Platform Configuration Compliance Controls Need Improvement

Term	Definition
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.
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.
Plan of Action and Milestones	A corrective action plan to identify and document the resolution of information security weaknesses and periodically report to the Office of Management and Budget, the Department of the Treasury, and Congress.
Platform	A computer or hardware device, an associated operating system, or a virtual environment on which software can be installed or run.
Priority One	Priority is based on impact and urgency and is used to identify required times for actions to be taken. Priority One incidents are defined as: 1) a severe business disruption, 2) a critical user or group is unable to operate, or 3) a critical system component failed or is severely impaired. The target resolution time is four hours.
Priority Two	Priority is based on impact and urgency and is used to identify required times for actions to be taken. Priority Two incidents are defined as: 1) a major business disruption, 2) a critical user or group is unable to operate, or 3) a business unit is experiencing a significant reduction in system performance. The target resolution time is eight hours.
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.
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. The Authorizing Official approves the decision.
	
Sprint	A process that develops a piece of functionality of the system with repeated cycles of requirements discovery, planning, design, development, and testing. The goal of each sprint is to get a subset of the project's functionality to a production-ready state.
Tailoring	Modification of a standard approach to customize it for a specific situation.
Tier I	Supercomputers and mainframe hardware and software, including peripheral subsystems used in a mainframe system environment.

Mainframe Platform Configuration Compliance Controls Need Improvement

Term	Definition
Tier II	Minicomputers, <i>i.e.</i> , computers usually containing multiple microprocessors, capable of executing multiple processes simultaneously. They may serve multiple users by way of a communications network, including hardware, software, and peripheral subsystems used in that environment.
Vulnerability	Weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Abbreviations

DISA	Defense Information Systems Agency
EOps	Enterprise Operations
█	██
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
STIG	Security Technical Implementation Guide
TIGTA	Treasury Inspector General for Tax Administration
█	*****2*****
█	██
█	██
█	██



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

(800) 366-4484

By Web:

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.