

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Security Weaknesses Are Not Timely Resolved and Effectively Managed

August 9, 2023

Report Number: 2023-20-042

HIGHLIGHTS: Security Weaknesses Are Not Timely Resolved and Effectively Managed

Final Audit Report issued on August 9, 2023

Report Number 2023-20-042

Why TIGTA Did This Audit

The timely identification and resolution of information security weaknesses are the primary cornerstones of a sound information security program. All Federal agencies are required to develop and implement a corrective action plan, known as a Plan of Action and Milestones (POA&M), to identify and document the resolution of information technology security weaknesses.

This audit was initiated to review the effectiveness of the IRS information technology POA&M process and determine if it complies with required Federal and agency security policies.

Impact on Tax Administration

The IRS is required to report identified information security weaknesses and document remediation. Failure to timely review, track, and close POA&Ms to resolve information security weaknesses puts the IRS at risk for exploitation by threat actors. In addition, tracking associated resources required to resolve POA&Ms facilitates informed decision-making.

What TIGTA Found

Between January 1, 2005, and August 26, 2022, the IRS created 12,089 POA&Ms. Of these 12,089 POA&Ms, remediation efforts for 9,534 have been finalized while 2,555 are open with efforts still ongoing. TIGTA selected a judgmental sample of 401 POA&Ms for analysis.

The IRS did not timely review 291 (73 percent) of 401 POA&Ms TIGTA analyzed based on agency security policies nor did it perform the required closure reviews within the 60-day time period for 138 (49 percent) of 282 POA&Ms marked as either Accepted, Completed, or Validated.

Due to staffing shortfalls, IRS employees are not facilitating the timely resolution of information security weaknesses. Agency-wide, there are more than 500 POA&Ms categorized as Late, including 23 with risk severity ratings of either critical or high. Of those 23, there are four POA&Ms where the security weakness was first identified in 2017.

In addition, business units are not timely creating POA&Ms or consistently entering required POA&M information. For example, 1,381 (32 percent) of 4,370 POA&Ms created on or after January 1, 2018, through August 26, 2022, were not created within agency permitted timelines, and 295 (74 percent) of 401 POA&Ms TIGTA analyzed lacked either the required status updates, required due date comments, or had insufficient documentation to justify a modified POA&M due date. Further, there were 304 instances where POA&Ms were missing required data elements.

Finally, the IRS is not accurately identifying and tracking resources required to resolve information security weaknesses. For the 12,089 POA&Ms, there was a total estimated cost of \$2.6 billion to resolve the information security weaknesses. From January 1, 2018, through August 26, 2022, the IRS finalized remediation efforts for 3,139 POA&Ms with total estimated costs of \$134.5 million to resolve the information security weaknesses. However, during the closure process, the IRS did not reevaluate the estimated budget and update it with actual costs at closure, as required.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer: 1) consolidate the best business unit POA&M remediation practices and implement a consistent process agency-wide to manage security risk remediation; 2) prioritize staffing and other resource allocations to address security weaknesses; 3) consider POA&M estimated costs in budget formulation; and 4) collaborate with business unit representatives to ensure POA&M costs are updated at closure.

The IRS agreed with all four recommendations. The Chief Information Officer plans to implement a consistent process; prioritize staffing and other resource allocations; and ensure that POA&M estimated costs are accurately updated at closure.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

August 9, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Security Weaknesses Are Not Timely Resolved and Effectively Managed (Audit # 202220017)

This report presents the results of our review of the effectiveness of the information technology plan of action and milestones process. This audit is included in our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS [Internal Revenue Service] Resources*.

Management's complete response to the draft report is included as Appendix IV. 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>The Plan of Action and Milestones Process Is Not Facilitating the Timely Resolution of Information Security Weaknesses</u>	Page 2
<u>Recommendations 1 and 2:</u>	Page 6
<u>Resources Needed to Resolve Information Security Weaknesses Are Not Tracked or Updated</u>	Page 6
<u>Recommendations 3 and 4:</u>	Page 7
Appendices	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 9
<u>Appendix II – Outcome Measure</u>	Page 11
<u>Appendix III – Plan of Action and Milestones Status Definitions</u>	Page 12
<u>Appendix IV – Management’s Response to the Draft Report</u>	Page 13
<u>Appendix V – Glossary of Terms</u>	Page 16
<u>Appendix VI – Abbreviations</u>	Page 18

Background

According to the Internal Revenue Service (IRS), the timely identification and resolution of information security weaknesses are the primary cornerstones of a sound information security program.¹ The Federal Information Security Modernization Act of 2014 (FISMA)² mandates that all Federal agencies develop and implement a corrective action plan, known as a Plan of Action and Milestones (POA&M), to identify and document the resolution of information technology security weaknesses.³

Further, the National Institute of Standards and Technology (NIST) provides guidance related to developing and updating a POA&M to document the planned remediation actions to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system.⁴ Compliance with the NIST guidance necessitates organizations to execute due diligence with regard to information security and risk management. Lastly, the Internal Revenue Manual requires IRS system owners to provide updates to POA&Ms at least quarterly.⁵

The Federal Information Security Modernization Act of 2014 (FISMA) mandates all Federal agencies develop and implement a corrective plan of action, known as a Plan of Action & Milestones (POA&M).



POA&Ms are used to identify and document resolution of information technology security weaknesses.

The IRS uses the Treasury FISMA Inventory Management System (TFIMS) tool to manage the collection and reporting of information associated with the FISMA. System owners are required to report identified weaknesses for FISMA classified systems in the TFIMS tool to identify, track, and manage information technology weaknesses along with documenting remediation efforts.

In an effort to comply with the NIST and Internal Revenue Manual guidance, the Enterprise FISMA POA&M Standard Operating Procedures provide system owners with the necessary guidance and procedures for developing, maintaining, and reporting POA&Ms. In addition, the Standard Operating Procedures state that the purpose of the POA&M process is to assist executive and senior leadership in identifying, assessing, prioritizing, and monitoring the

¹ IRS, *Enterprise FISMA POA&M Standard Operating Procedures*, Ver. 10.1 (June 19, 2020).

² 44 U.S.C. § 3551, et seq. (2018).

³ See Appendix V for a glossary of terms.

⁴ NIST, Special Publication 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020).

⁵ Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance* (Dec. 13, 2022).

progress of corrective actions for security weaknesses found in programs and information systems.



The Cybersecurity function’s Enterprise FISMA Services (EFS) organization is responsible for the oversight and maintenance of the POA&M and risk-based decision processes. These processes are worked by EFS employee teams. Within IRS business units, the overall responsibility for managing POA&Ms rests with the authorizing official of each system. While much of the focus of security at the system level involves information security personnel, collaboration must occur with senior leadership to ensure weakness mitigation plans, funding, and allocation of other needed resources are in alignment with the business unit mission.

Results of Review

The Plan of Action and Milestones Process Is Not Facilitating the Timely Resolution of Information Security Weaknesses

Between January 1, 2005, and August 26, 2022, the IRS created 12,089 POA&Ms with total estimated costs of \$2.6 billion to resolve the information security weaknesses. Of these 12,089 POA&Ms, remediation efforts for 9,534 have been finalized while 2,555 are open with efforts still ongoing. The IRS classifies POA&Ms into eight status categories: Accepted, Cancelled, Completed, Draft, Duplicate, In-Progress, Late, and Validated.⁶ From the 12,089 POA&Ms, 4,370 were created on or after January 1, 2018, and reflect a current status of one of the following: Accepted, Completed, In Progress, Late, or Validated.⁷ In consultation with our agency’s statistician, we selected a judgmental sample of 401 POA&Ms from the five status codes for analysis.⁸ Figure 1 summarizes the number of POA&Ms selected for analysis.

Figure 1: Total Number of POA&Ms Reviewed and Selected Sample Sizes

	Accepted POA&Ms	Completed POA&Ms	In-Progress POA&Ms	Late POA&Ms	Validated POA&Ms	Totals
 Created on or after January 1, 2018	166	208	778	453	2,765	4,370
 Selected Judgmental Sample Size	12	17	78	41	253	401

Source: Treasury Inspector General for Tax Administration’s analysis of IRS POA&Ms obtained via the TFIMS tool on August 26, 2022.

⁶ See Appendix III for the definitions of the POA&M status categories.

⁷ The remaining four POA&M status categories were not chosen for review because they are not in an active status and do not require further analysis.

⁸ A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Management oversight of the POA&M process is lacking

We determined that 291 (73 percent) of the 401 POA&Ms selected for analysis were not timely reviewed based on agency security policies. Per agency security policies, newly created POA&Ms are required to be reviewed within 45 days of creation, Late POA&Ms are required to be reviewed within 45 days of it entering Late status, and closure reviews are required to be conducted within 60 days of POA&M closure. We found that the required closure reviews were not performed within the required 60-day time period for 138 (49 percent) of 282 POA&Ms marked as either Accepted, Completed, or Validated. While the required reviews were ultimately completed, the continued extensions of remediation timelines may lengthen the period of exposure of critical tax systems to known information security vulnerabilities which may provide expanded opportunities for threat actors to access and exploit data.

As of November 2022, the IRS had approximately 1,800 active POA&Ms and a staff of eight employees who are responsible for managing roughly 225 POA&Ms each.⁹ POA&M team members stated that due to the large work volume (including management of the agency's risk-based decision process) and the current staff size, they are able to perform only basic level POA&M program oversight.

In 2016, the POA&M team had 16 full-time employees. However, due to natural attrition and reorganizations, including moving some EFS programs to another team, the staff was reduced to 12 full-time employees in 2020. Since then, the staff has been further reduced to the current number of eight full-time employees. EFS management officials stated they are seeking to use funding from the Inflation Reduction Act of 2022 to request additional full-time employees to address the increased workload.¹⁰

Due to a lack of management oversight and operational staffing shortfalls, the POA&M process does not support timely resolution of information security weaknesses. Agency-wide, there are more than 500 Late POA&Ms, including 23 with risk severity ratings of either critical or high. Of those 23, there are four POA&Ms related to configuration management, access control, and audit and accountability where the security weakness was first identified in 2017. Failure to timely review, track, and close POA&Ms to resolve the information security weaknesses puts the IRS at risk for exploitation by threat actors.

Business units are not timely creating POA&Ms or consistently entering required data elements

Agency security policies require that POA&Ms be entered into the TFIMS tool within 60 days of the initial identification of the information security weakness. Once a POA&M is entered into the TFIMS tool, the POA&M team is required to provide an initial review within 45 days to determine if the POA&M is compliant with minimum agency requirements. For noncompliant POA&Ms, the POA&M team provides guidance for corrective action and a due date for resubmission. For the 4,370 POA&Ms created on or after January 1, 2018, through August 26, 2022.

- 2,989 (68 percent) of the 4,370 POA&Ms were created within agency permitted timelines.

⁹ Active POA&Ms are those with a status of either In Progress, Late, or Completed.

¹⁰ Public Law No. 117-169, 136 Stat. 1818.

Security Weaknesses Are Not Timely Resolved and Effectively Managed

- 1,381 (32 percent) of the 4,370 POA&Ms were not created within agency permitted timelines.
 - 90 (7 percent) of the 1,381 POA&Ms are categorized as critical and high severity information security weaknesses that impact 35 of 142 IRS systems.
 - 1,291 (93 percent) of the 1,381 POA&Ms are categorized as low and moderate severity information security weaknesses that impact 139 of 142 IRS systems.



In addition, 295 (74 percent) of the 401 POA&Ms we analyzed lacked either the required status updates, required due date comments, or had insufficient documentation to justify a modified POA&M due date. Lastly, we identified 304 instances where POA&Ms were missing required data elements.

Subsequently, we interviewed eight business unit representatives to discuss their internal POA&M processes, to include the management, oversight, and prioritization of existing POA&Ms, process for developing new POA&Ms, and staffing and resource challenges.



From these interviews, we determined that the following root causes were key contributors to the business units not timely creating POA&Ms and not consistently entering the required POA&M information:


- Staffing and funding resource constraints.
- Lack of an internal POA&M management process.
- Lack of a formalized escalation process for noncompliant POA&Ms.


For example, multiple business units' management expressed their inability to hire the technical personnel required to resolve information security weaknesses. In September 2020, the Chief Information Officer issued a memorandum stating that all work related to the determination of information technology solutions and investments, cybersecurity (protection of IRS systems), and technology products used in the Information Technology organization is inherently information technology and should not be staffed from within business units outside of the Information Technology organization. Business units' management also stated that a lack of Operations and Maintenance funding is a significant impairment to their ability to timely remediate information security weaknesses. The following tables summarize some highlights from our interviews with specific business units' and General Support System-34 management:

	Research, Applied Analytics, and Statistics	
140 (88 percent) of 160 active POA&Ms classified as Late.		
No business unit specific POA&M remediation procedures.		
Only 1.5 employees assigned to solving technical issues related to POA&Ms.		
Funding challenges have delayed the hiring of additional technical employees.		
Subsequent to our initial interview, they submitted evidence to close 25 POA&Ms.		

Security Weaknesses Are Not Timely Resolved and Effectively Managed

 <u>Taxpayer Advocate Service</u> 
Six (60%) of 10 active POA&Ms were classified as Late.
No business unit specific POA&M remediation procedures.
One full-time employee supporting FISMA-related activities (started in August 2022).
Lack of POA&M progress due largely to systems designated by the Applications Development function as either Break-Fix only or Keeping Lights On. ¹¹

 <u>Criminal Investigation</u>
73 (57 percent) of 128 active POA&Ms were classified as Late.
A new internal POA&M process was implemented in 2022 to help address aging and past due POA&Ms.
Two full-time employees supporting POA&M activities.
Challenges hiring and retaining technical personnel.

 <u>General Support System-34</u>
40 (30 percent) of 135 active POA&Ms were classified as Late.
Within the past 18 months, two full-time employees were hired along with adding two contractors who dedicate part time to POA&M activities.
Implemented new internal POA&M Standard Operating Procedures in February 2022.
Prioritized hiring employees with compliance and risk management experience.

Business units with the highest percentage of Late and noncompliant POA&Ms did not have internal POA&M management processes. In addition, the POA&M team lacked a formalized escalation process for noncompliant POA&Ms. Due to not having these processes in place, responsible individuals within each business unit lacked the required guidance and oversight needed to ensure that POA&Ms were created timely and to correct noncompliant POA&Ms.

Management Action: In March 2023, the POA&M team updated the IRS Enterprise FISMA POA&M Standard Operating Procedures to include an escalation process for noncompliant POA&Ms. The new escalation process outlines the various stakeholders and management officials included in each of the three escalation levels. In addition, this new process was communicated via e-mail to all agency POA&M stakeholders.

¹¹ In May 2020, the Associate Chief Information Officer, Applications Development, implemented a new policy for designating production support categories for 395 tax systems and applications.

Security Weaknesses Are Not Timely Resolved and Effectively Managed

The Chief Information Officer should:

Recommendation 1: Consolidate the best business unit POA&M remediation practices and implement a consistent process agency-wide to adequately manage security risk remediation in accordance with Federal guidelines.

Management’s Response: The IRS agreed with this recommendation. The Chief Information Officer will work collaboratively with business units to identify best practices and consolidate into an agency-wide process to assist with adequately managing security risk remediation.

Recommendation 2: Prioritize staffing and other resource allocations to address both management and remediation of POA&Ms agency-wide and review progress on an ongoing basis.

Management’s Response: The IRS agreed with this recommendation. The Chief Information Officer will prioritize staffing and other resource allocations to address both management and remediation of POA&Ms agency-wide and review progress on an ongoing basis.

Resources Needed to Resolve Information Security Weaknesses Are Not Tracked or Updated

Per the agency POA&M Standard Operating Procedures, business units are required to identify the resources needed and the source of the funding to resolve the information security weakness. From January 1, 2018, through August 26, 2022, the IRS associated \$905 million in estimated costs to resolve information security weaknesses via the POA&M process. Figure 2 summarizes the estimated costs for POA&Ms created during Calendar Years 2018 through 2022.

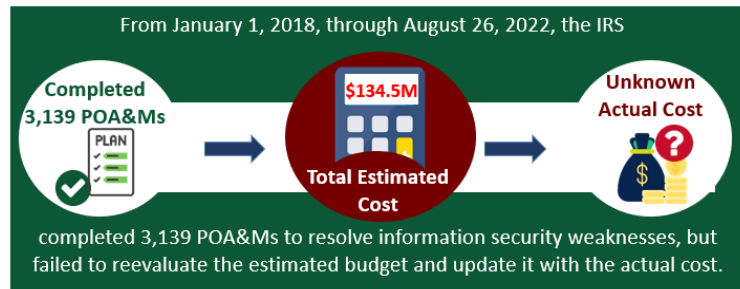
**Figure 2: Estimated Costs for POA&Ms Created Calendar Years 2018 – 2022
(in millions)**

	CY 2018	CY 2019	CY 2020	CY 2021	CY 2022	Totals
Accepted	\$8.5	\$0.36	\$0.15	\$0.11	\$0.02	\$9.3
Completed	\$0.24	\$0.48	\$0.26	\$0.58	\$0.53	\$2.1
In Progress	\$0.54	\$82.1	\$87.5	\$50	\$382	\$602
Late	\$38.5	\$22.7	\$2.4	\$5	\$0.49	\$69.1
Validated	\$44.5	\$17.5	\$48.7	\$12	\$0.44	\$123.1
Other	\$3.1	\$13.8	\$0.83	\$3.6	\$78	\$99.3
Totals	\$95.4	\$137	\$139.8	\$71.3	\$461.5	\$904.9

Source: Treasury Inspector General for Tax Administration’s calculations of IRS POA&M estimated costs obtained via the TFIMS tool on August 26, 2022. CY = Calendar Year. The totals may not calculate due to rounding.

Security Weaknesses Are Not Timely Resolved and Effectively Managed

From January 1, 2018, through August 26, 2022, the IRS finalized remediation efforts for 3,139 POA&Ms with total estimated costs of \$134.5 million to resolve the information security weaknesses. However, during the closure process, the IRS did not reevaluate the estimated budget and update it with actual costs at closure, as required. Agency POA&M procedures state that every weakness identified in a POA&M must include an estimated budget, which will identify the



resources required and the source of funding to resolve it. In addition, business units must reevaluate the estimated budget and update it with the actual cost when closing a POA&M. We found that the IRS did not update the budget at POA&M closure to reflect the actual cost for any of the 3,139 completed POA&Ms. Tracking associated resources required to resolve POA&Ms facilitates informed decision making.

During discussions with the POA&M team, management officials stated that due to staffing and resource constraints, they are unable to enforce the requirement for business units to reevaluate and update the POA&M estimated budget at time of closure. We also conducted interviews with eight business units, and none were aware of the requirement to update the estimated budget at closing. One business unit initiated action during our audit work and obtained permission to leverage the agency's financial system to implement the use of Single Entry Time Reporting codes to track associated POA&M costs and resources.

Lastly, the Office of Management and Budget requires that POA&Ms be tied to the agency's budget submission through the unique project identifier of a system.¹² During discussions with the Strategy and Planning function's Financial Management Services organization, management officials stated that while individual POA&Ms were not considered as inputs into the budget formulation process, the need to address existing POA&Ms (as an aggregate) are considered as part of the agency's Operations and Maintenance funding request.

The Chief Information Officer should:

Recommendation 3: Specifically consider POA&M estimated costs in budget formulation.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will partner with the business units to establish a process ensuring that POA&M estimated costs are considered in budget formulation.

Recommendation 4: Collaborate with business unit representatives to ensure POA&M costs are updated at closure.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will ensure estimated POA&M costs are accurately updated at

¹² Office of Management and Budget, OMB M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly Information Technology Security Reporting* (Aug. 2003).

Security Weaknesses Are Not Timely Resolved and Effectively Managed

closure in accordance with the IRS Enterprise FISMA POA&M Standard Operating Procedures.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to review the effectiveness of the information technology POA&M process and to determine if it complies with required Federal and agency security policies. To accomplish our objective, we:

- Determined the effectiveness of management and oversight of the POA&M process over the tracking and remediation of information security weaknesses by reviewing relevant NIST guidance and the Internal Revenue Manual, interviewing members of the POA&M team, and evaluating whether the POA&M management team is providing the required level of oversight of the POA&M process based on their current duties and staffing size.
- Determined whether the POA&M process facilitates the timely resolution of information security weaknesses by evaluating whether POA&Ms are being created and entered into the TFIMS tool in a timely manner based on agency policies and are being timely resolved based on the assigned due date.
- Selected the POA&Ms that were created on or after January 1, 2018, and reflect a current status of one of the following: Accepted, Completed, In Progress, Late, or Validated, which resulted in a population size of 4,370 POA&Ms. Subsequently, we consulted with our agency's statistician and selected a judgmental sample size of 401 POA&Ms for analysis.¹ We selected a judgmental sample because we did not plan to project to the population.
- Determined whether the required ongoing updates and completion of POA&M elements related to the resolution of information security weaknesses are performed per agency requirements by reviewing status comments and due date comments for our selected sample to determine if resolutions are documented and updated as required.
- Determined whether the IRS accurately identifies and tracks the resources required (funding, staffing, equipment, training, *etc.*) to resolve information security weaknesses by reviewing POA&Ms to determine whether an estimated budget was completed at creation, re-evaluated, and updated at closure with the total amount required to resolve the weakness. We also interviewed key stakeholders and reviewed relevant criteria to evaluate the process used by the business units to track the costs of POA&Ms.

Performance of This Review

This review was performed remotely with information obtained from the Information Technology; Criminal Investigation; IRS Independent Office of Appeals; National Taxpayer Advocate; and the Research, Applied Analytics, and Statistics organizations during October 2022 through April 2023. 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

¹ A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

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; Kenneth Bensman, Acting Audit Manager; Myron Gulley, Audit Manager; Paula Benjamin-Grant, Lead Auditor; Mike Curtis, Senior Auditor; Joseph Dryden, Student Intern; Laura Christoffersen Information Technology Specialist (Data Analytics); and Kevin Nielsen, Information Technology Specialist (Data Analytics).

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of the POA&M data obtained from the TFIMS website. We evaluated the data by 1) ensuring that the information was legible and contained alphanumeric characters; 2) reviewing required data elements; and 3) reviewing the data to detect obvious errors, duplicate values, and missing data. We determined that the data were sufficiently reliable to support our conclusions, findings, and recommendations.

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: the Office of Management and Budget, NIST, and IRS policies related to the POA&M process. We evaluated these controls by interviewing personnel on the POA&M team and agency POA&M stakeholders; reviewing documentation including policies and procedures related to entering, closing, reviewing and tracking POA&Ms; and reviewing the associated resources needed to resolve information security weaknesses. We analyzed POA&Ms tracked in the TFIMS tool to assess both the timeliness and the adequacy of information provided in the required POA&M data elements.

Appendix II

Outcome Measure

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; 3,139 POA&Ms with estimated costs totaling \$134.5 million that were not updated at POA&M closing to reflect the actual cost (see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

From January 1, 2018, through August 26, 2022, the IRS finalized remediation efforts for 3,139 POA&Ms with total estimated costs of \$134.5 million to resolve information security weaknesses. Business units must reevaluate and update the estimated cost with the actual cost when closing a POA&M. We found that the IRS did not update the estimated cost for any (0 percent) of the 3,139 closed POA&Ms.

Appendix III

Plan of Action and Milestones Status Definitions

Term	Definition
Accepted	Used to document the authorizing official's decision to accept the risk via a signed Risk-Based Decision for a weakness documented in the POA&M.
Cancelled	Used when the identified weakness/condition still exists and is no longer an unacceptable risk. This should rarely happen.
Completed	Used for a fully resolved weakness with the corrective action tested and approved.
Draft	Used for initially created POA&Ms. This status provides time to gather necessary data/dates to establish a well-defined plan to mitigate the weakness/finding.
Duplicate	Used when a POA&M is created, and it is determined that another identical POA&M already existed. The IRS considers a duplicate POA&M closed.
In-progress	Used when POA&M weakness remediation is in progress. It indicates that activities needed to resolve weaknesses are in progress.
Late	POA&M is past its original due date and remains open.
Validated	Restricted for use by the POA&M team during review of completed POA&Ms. Used when POA&M actions are reviewed and validated as a good closure.

Source: IRS, Enterprise FISMA POA&M Standard Operating Procedures, Ver. 10.1 (June 19, 2020).

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

July 18, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya, Acting Chief Information Officer
Kaschit D. Pandya

Digitally signed by Kaschit D. Pandya
Date: 2023.07.19
13:33:01 -04'00'

SUBJECT: Draft Audit Report – Security Weaknesses Are Not Timely Resolved and Effectively Managed (Audit #202220017)

Thank you for the opportunity to review and comment on the subject draft audit report. The IRS is committed to fully and effectively addressing information technology security weaknesses. We concur with the recommendations and outcome measure in the draft report. We plan to complete implementation of all corrective actions by May 15, 2024, and have included a corrective action plan.

The agency's Plan of Action and Milestones (POA&Ms) management process is used to assist Information Systems Owners in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for information technology security weaknesses. Throughout the IRS, staffing levels associated with this management process have not kept pace with increasing workloads. We are taking a series of steps that include, but are not limited to, prioritizing staffing and other resource allocations associated with this process and enhancing communications with all agency POA&M stakeholders to clarify expectations and best practices in remediation. We expect these efforts will help to reduce risk, ensure system integrity, and maximize system availability for taxpayers. Your review of the agency's policies, procedures and recommendations for improvement will help us strengthen our program.

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 Cara Garr, Director of Security Risk Management, at (801) 620-4140.

Attachment

Security Weaknesses Are Not Timely Resolved and Effectively Managed

Attachment

TIGTA Audit 2022220017 – Security Weaknesses Are Not Timely Resolved and Effectively Managed

Recommendations

RECOMMENDATION 1: The Chief Information Officer should consolidate the best business unit POA&M remediation practices and implement a consistent process agency-wide to adequately manage security risk remediation in accordance with Federal guidelines.

CORRECTIVE ACTION 1: The IRS agrees with the recommendation. The Chief Information Officer will work collaboratively with business units to identify best practices and consolidate into an agency-wide process to assist with adequately managing security risk remediation.

IMPLEMENTATION DATE: May 15, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 2: The Chief Information Officer should prioritize staffing and other resource allocations to address both management and remediation of POA&Ms agency-wide and review progress on an ongoing basis.

CORRECTIVE ACTION 2: The IRS agrees with the recommendation. The Chief Information Officer will prioritize staffing and other resource allocations to address both management and remediation of POA&Ms agency-wide and review progress on an ongoing basis.

IMPLEMENTATION DATE: March 15, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 3: The Chief Information Officer should specifically consider POA&M estimated costs in budget formulation

CORRECTIVE ACTION 3: The IRS agrees with the recommendation. The Chief Information Officer will partner with the business units to establish a process ensuring that POA&M estimated costs are considered in budget formulation.

IMPLEMENTATION DATE: March 15, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

Security Weaknesses Are Not Timely Resolved and Effectively Managed

Attachment

TIGTA Audit 2022220017 – Security Weaknesses Are Not Timely Resolved and Effectively Managed

RECOMMENDATION 4: The Chief Information Officer should collaborate with business unit representatives to ensure POA&M costs are updated at closure.

CORRECTIVE ACTION 4: The IRS agrees with the recommendation. The Chief Information Officer will ensure estimated POA&M costs are accurately updated at closure in accordance with the IRS Enterprise FISMA Plan of Action and Milestones (POA&M) Standard Operating Procedure (SOP).

IMPLEMENTATION DATE: March 15, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

Glossary of Terms

Term	Definition
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Break-Fix	When system changes are limited to those required to “fix” the system/application to keep it operational and secure. No active development or discretionary work is performed without director-level approval.
Closure Review	Completed by the POA&M team to ensure that the finding and recommendation is correct and complete. In addition, it verifies that the POA&M is in the correct status and the necessary artifacts are loaded, accessible, and justify and support closure of the POA&M.
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. The original statute (Federal Information Security Management Act of 2002) 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.
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.
Keeping Lights On	Break-Fix plus the minimum development required to make changes approved by the director to keep the system operational, such as approved required regular, yearly, or legislative changes or filing season updates.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
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.
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.

Security Weaknesses Are Not Timely Resolved and Effectively Managed

Term	Definition
Severity Rating	One of five levels on a ratings scale to describe the risk associated with a vulnerability. The complete scale from lowest risk to highest risk is: Informational, Low, Medium, High, and Critical.
Single Entry Time Reporting	An online payroll system in the Totally Automated Personnel System that enables the input of Time and Attendance data to the National Finance Center.
Threat Actors	The instigators of risks with the capability to do harm.
Treasury FISMA Inventory Management System	The official FISMA data repository for all Department of the Treasury bureaus. The data maintained in this repository are used as part of the Treasury Department's efforts to comply with the E-Government Act of 2002 ¹ as well as NIST and Office of Management and Budget regulations and guidance.

¹Pub. L. 107-347, 116 Stat. 2899.

Abbreviations

EFS	Enterprise FISMA Services
FISMA	Federal Information Security Modernization Act of 2014
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
TFIMS	Treasury FISMA Inventory Management System



**To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at
oi.govreports@tigta.treas.gov.**

**To make suggestions to improve IRS policies, processes, or systems
affecting taxpayers, contact us at www.tigta.gov/form/suggestions.**

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