TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Actions Are Needed to Improve the Zero Trust Architecture Implementation

July 10, 2023

Report Number: 2023-20-039

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: Actions Are Needed to Improve the Zero Trust Architecture Implementation

Final Audit Report issued on July 10, 2023 **Report Number 2023-20-039**

Why TIGTA Did This Audit

The Zero Trust Architecture (ZTA) is an end-to-end approach to enterprise resource and data security that encompasses identity, credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure and is based on the premise that trust is never granted implicitly but must be continually evaluated.

Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), requires Federal agencies to advance a zero trust security model. In addition, the Office of Management and Budget Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022), established the milestones and criteria that agencies should follow to implement a ZTA.

This audit was initiated to determine the effectiveness of the IRS's enterprise strategy and implementation of ZTA technical solutions which restrict network accesses to trusted users, assets, and resources.

Impact on Tax Administration

The implementation of ZTA will help prevent unauthorized access across the enterprise. Without a well-developed ZTA, unauthorized access could result in substantial harm to systems and a loss of public confidence in the IRS.

What TIGTA Found

As of March 2023, the IRS developed a ZTA plan, reference architecture document, roadmap, and pilot program. However, the ZTA plan does not explicitly define the roles and responsibilities for implementing the plan. In addition, the plan was not created within the timeframe established in the Executive Order. The IRS also does not have a budget estimate for the Fiscal Year 2024 ZTA initiatives.

The Office of Management and Budget memorandum described strategic goals that align with five pillars (Identity, Devices, Networks, Applications and Workloads, and Data) of the draft Zero Trust Maturity Model developed by the Cybersecurity and Infrastructure Security Agency. The IRS performed an assessment of its zero trust maturity and hired an independent contractor to conduct an assessment of its maturity against the five pillars. The IRS assessed 10 (53 percent) of the 19 total controls differently from the contractor. The contractor assessed the IRS controls at a lower maturity level for eight of the 10 controls in which they disagreed. However, the IRS stated that it is maintaining its current levels of maturity and will perform an updated assessment in the future. TIGTA determined that the IRS did not accurately assess its zero trust maturity.

Finally, the IRS prioritized three of the five required pillars as part of their phased approach to performing ZTA maturity assessments. For example, the IRS implemented fully the federated identity services with the Department of the Treasury to address the Identity pillar. To address the Devices pillar, the IRS deployed endpoint detection and response tools to servers. For the Applications and Workloads pillar, the IRS developed a vulnerability disclosure platform standard operating procedure and created a web collection tool on the IRS.gov website. IRS management stated they received an external assessment of the Data and Networks pillars in March 2023.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer should: 1) identify a budget estimate of ZTA from the managed projects; 2) ensure the ZTA plan is revised to include defined roles and responsibilities; 3) enhance the ZTA roadmap to include a schedule for the five ZTA pillars; and 4) reassess the ZTA implementation progress to ensure management has accurate and complete information to inform planning and the budget process.

The IRS agreed with all four recommendations. The Chief Information Officer plans to obtain a budget estimate identified by the managed projects and initiatives that support ZTA; update the ZTA plan to include roles and responsibilities for programs, projects, and initiatives identified; enhance the ZTA roadmap to include specific activities based on the ZTA five pillars for the enterprise; and reassess the ZTA implementation progress and advise management for informational and budget planning purposes.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

July 10, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Actions Are Needed to Improve the Zero Trust Architecture Implementation (Audit # 202220004)

This report presents the results of our review to determine the effectiveness of the Internal Revenue Service's (IRS) enterprise strategy and implementation of zero trust architecture technical solutions which restrict network accesses to trusted users, assets, and resources. Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), requires agencies to move towards a zero trust architecture. 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 Resources.*

Management's complete response to the draft report is included as Appendix II. If you have any questions, please contact me or Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background

In August 2020, the National Institute of Standards and Technology issued zero trust architecture (ZTA) guidance that provided direction for Federal agencies to migrate and deploy ZTA security concepts to an enterprise environment.[1] The guidance states that ZTA is an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure and is focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.[2] The initial focus of ZTA should be on restricting resources to those with a need to access and grant only the minimum privileges, *e.g.*, read, write, delete, that are needed to perform the mission. According to the National Institute of Standards and Technology, Federal agencies have traditionally focused on perimeter defense and authenticated subjects are given authorized access to a broad collection of resources once on the internal network. As a result, unauthorized access within the environment has been one of the biggest challenges for Federal agencies.

Executive Order 14028 states that the Federal Government must adopt security best practices and advance toward ZTA.[3] Within 60 days of issuance, the head of each agency should have developed a plan to implement ZTA, including a plan for the adoption and use of cloud technology. The Executive Order also states that ZTA allows users full access but only to the bare minimum they need to perform their jobs. It also allows the concept of least-privileged access to be applied for every access decision, in which the answers to the questions of who, what, when, where, and how are critical for allowing or denying access to resources appropriately. If an enterprise is compromised, ZTA can ensure that the damage is contained. Per the Executive Order, once fully deployed, ZTA embeds comprehensive security monitoring, granular risk-based access controls, and system security automation in a coordinated manner throughout all aspects of the infrastructure to focus on protecting data in real-time within a dynamic threat environment.

On January 26, 2022, the Office of Management and Budget (OMB) issued a memorandum that described strategic goals that align with five pillars (Identity, Devices, Networks, Applications and Workloads, and Data) of the draft Zero Trust Maturity Model that was developed by the Cybersecurity and Infrastructure Security Agency (CISA). The maturity of each pillar is described in three stages (Traditional, Advanced, and Optimal). The CISA drafted the Zero Trust Maturity Model to assist agencies in complying with the Executive Order and released it for public comment from September 7, 2021, to October 1, 2021. The CISA issued an updated version of the guidance in April 2023 which introduced Initial as a fourth maturity stage.

The OMB memorandum requires agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year 2024.[4] The OMB memorandum also states that within

[1] National Institute of Standards and Technology, Special Publication 800-207, *Zero Trust Architecture* (Aug. 2020).

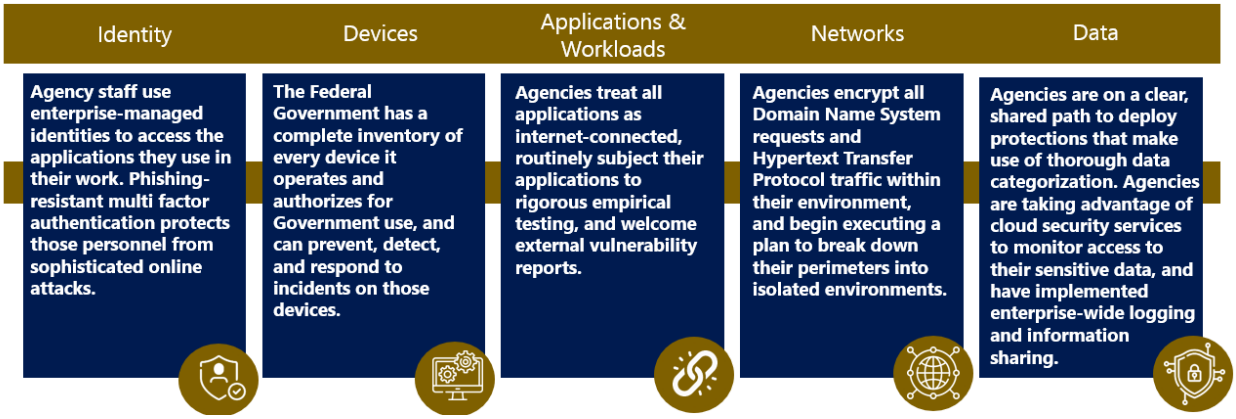
[2] See Appendix III for a glossary of terms.

[3] Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).

[4] OMB, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).

60 days from January 26, 2022, agencies must submit to the OMB and CISA an implementation plan for Fiscal Years 2022 through 2024 for OMB concurrence. In addition, agencies must submit a ZTA budget estimate for Fiscal Year 2024 to the OMB. Figure 1 describes the five ZTA pillars: Identity, Devices, Applications and Workloads, Networks, and Data.

Figure 1: Zero Trust Architecture Pillars



Source: OMB M-22-09 (January 26, 2022).

Results of Review

Zero Trust Architecture Efforts Are Underway, but Improvements and a Budget Estimate Are Needed

While the ZTA implementation is not required fully until the end of Fiscal Year 2024, the IRS performed the following actions.

- Completed a maturity model assessment of all five ZTA pillars in July 2021. The IRS used the draft maturity model to conduct the assessment.
- Prepared a ZTA plan. The IRS developed a ZTA plan dated March 11, 2022, and met the OMB required deadline. However, the plan was not prepared within 60 days, *i.e.*, by July 12, 2021, per the Executive Order guidance.
- Hired an independent contractor to complete a detailed maturity model assessment of three of five pillars of the IRS ZTA. The contractor report was based on the draft maturity model and completed in June 2022.
- Established a ZTA pilot in July 2022. The Enterprise Data Platform is serving as the model application to validate the IRS's design and implementation of a ZTA.
- Drafted an initial ZTA reference architecture document in September 2022. The IRS developed this document to provide an initial zero trust reference architecture for the cloud inclusive of design patterns and processes, to scale for future zero trust applications as the IRS moves towards conducting targeted pilots.

- Developed a ZTA overview and roadmap in October 2022. The roadmap depicts the IRS's high-level approach to an in-depth analysis of the initial maturity self-assessment and conducting detailed assessments and a gap analysis which will result in the design of an updated zero trust reference architecture.

However, the IRS did not have a Fiscal Year 2024 budget estimate for the ZTA initiatives as required by the OMB. According to the IRS ZTA Plan, a budget did not exist because the IRS needed to fully understand the remaining scope to complete each task before preparing a budget estimate.

The Cybersecurity function developed the plan to meet Executive Order requirements but the roles and responsibilities for implementing the plan have not been established fully. Cybersecurity officials stated the lead of ZTA should be within their organization.

Further, IRS management stated that they prioritized efforts on three (Identity, Devices, and Applications and Workloads) of the five ZTA pillars because those three pillars would help satisfy the remaining two pillars. However, the efforts completed on the three pillars did not identify any initiatives that would dually satisfy the remaining two pillars (Networks and Data). For example,

- Identity pillar - The IRS implemented the federated identity services fully with the Department of the Treasury.
- Devices pillar - The IRS deployed the endpoint detection and response tools to servers.
- Applications and Workloads pillar - The IRS developed a vulnerability disclosure platform standard operating procedure and created a web collection tool on the IRS.gov website.

For the remaining two pillars, IRS management stated that maturity in the Data pillar is tied to data classification, which is an effort that already exists and is underway within the IRS. In addition, due to the physical nature of the Networks pillar initiatives, these efforts provide comparatively limited protection to the overall ZTA.

According to IRS guidance, the IRS ZTA roadmap should cover the aspects necessary to evolve and sustain ZTA.[5] The roadmap should be an integrated program plan that identifies which teams are working on which ZTA projects and initiatives, and the key dependencies among these projects. The roadmap should be used to track the activities of the different teams that contribute to the ZTA build-out. The roadmap should:

- Articulate the capabilities of the IRS ZTA initiatives for all five pillars, expressed as a capability maturity.
- Identify a specific approach to reach the next level of maturity for each initiative.
- Provide a conceptual project plan to be used as a basis for developing a detailed project plan.
- Allocate responsibility to accomplish each of the activities.

[5] IRS, *Service-Oriented Architecture Roadmap, Version 2.1* (Apr. 11, 2007).

Without a budget estimate for implementing ZTA, clearly defined roles and responsibilities, and focusing on all five pillars, the IRS runs the risk of not implementing all ZTA controls and leaving the enterprise vulnerable to unauthorized access.

The Chief Information Officer should:

Recommendation 1: Identify a ZTA budget estimate from the managed projects and initiatives.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will obtain a budget estimate identified by the managed projects and initiatives that support ZTA.

Recommendation 2: Ensure the ZTA plan is revised to include defined roles and responsibilities.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will update the ZTA plan to include roles and responsibilities for programs, projects, and initiatives identified.

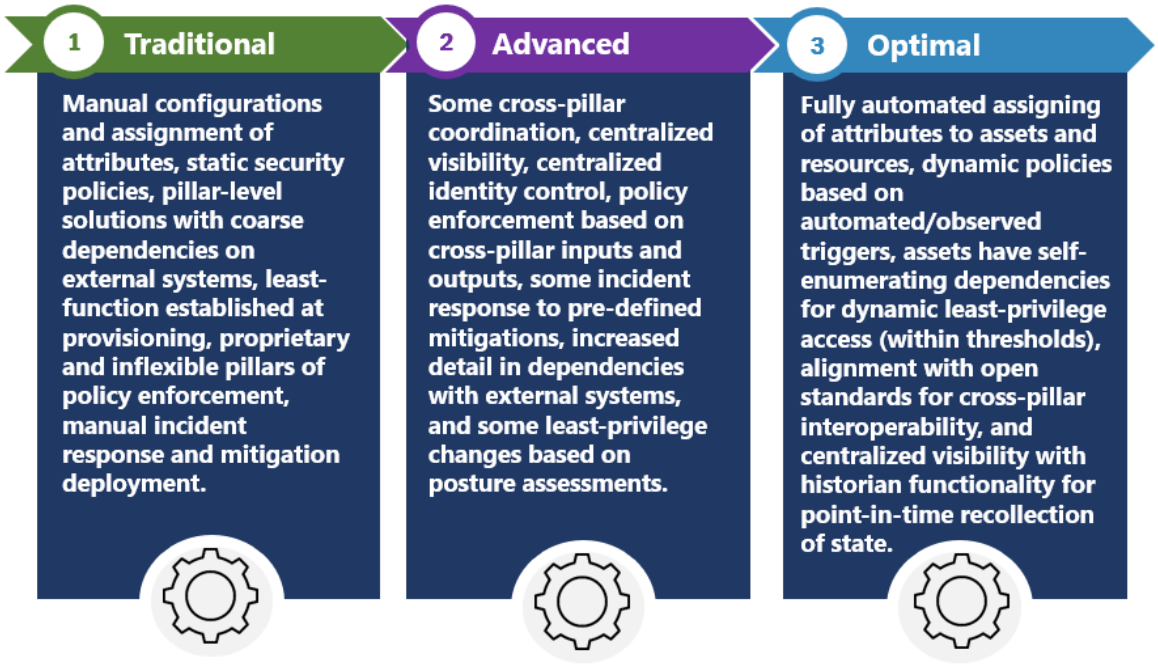
Recommendation 3: Enhance the ZTA roadmap to include a schedule for completion, address the gap analysis, and prioritize specific activities within each of the five ZTA pillars to ensure full implementation across the enterprise.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will enhance the ZTA roadmap to include specific activities based on the ZTA five pillars for the enterprise.

Maturity Level Assessments Varied Greatly Between an IRS Assessment and an Independent Contractor Assessment

In addition to the five ZTA pillars, the draft maturity model provides three stages (Traditional, Advanced, and Optimal) of maturity to help agencies identify their maturity level for each pillar. Figure 2 describes the three stages of ZTA pillar maturity.

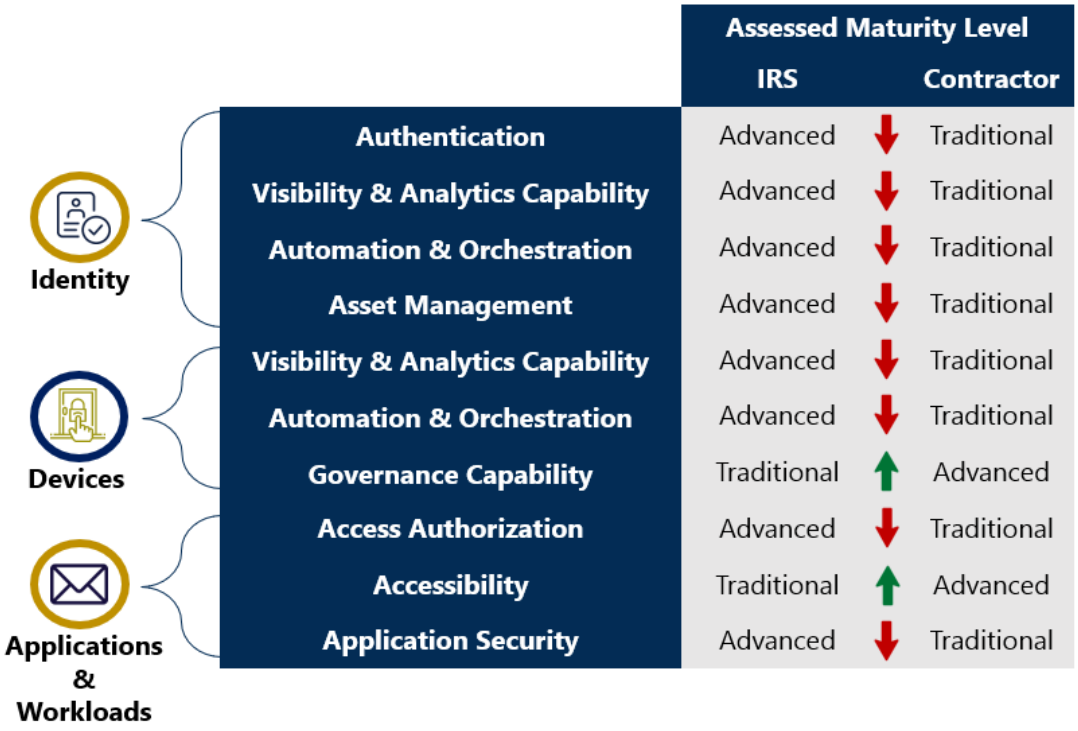
Figure 2: Zero Trust Stages of Maturity



Source: CISA Cybersecurity Division Draft Zero Trust Maturity Model, June 2021.

In July 2021, one month after the draft Federal guidance was released, the IRS conducted an internal assessment of its ZTA maturity. The IRS also contracted for an independent maturity assessment of its ZTA efforts that was completed in June 2022. We reviewed the contractor's assessment and compared it to the IRS's assessment of its ZTA implementation and found discrepancies. We determined that the IRS did not accurately assess its zero trust maturity. Specifically, 10 (53 percent) of the 19 ZTA controls that were assessed had a maturity level rating that differed from the IRS's internal maturity assessment. Figure 3 summarizes the 10 ZTA items which the contractor and the IRS assessed different maturity ratings.

Figure 3: Zero Trust Maturity Model Assessment Levels by Source



Source: IRS Cybersecurity function and contractor assessments.

According to the IRS, the ZTA maturity assessments varied due to the point in time in which they were completed. After the IRS received the contractor's assessment results, the IRS stated that it is maintaining its current levels of maturity and will perform an updated assessment in the future. On March 8, 2023, the contractor completed an assessment of the final two pillars (Networks and Data); however, the audit team did not complete a comparison with the IRS's results due to the timeframe of receiving the documentation. Without an accurate assessment of its ZTA maturity, the IRS may not be able to determine whether its enterprise is protected by appropriate ZTA controls.

Recommendation 4: The Chief Information Officer should reassess the ZTA implementation progress to ensure management has accurate and complete information to inform planning and the budget process.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will reassess the ZTA implementation progress and advise management for informational and budget planning purposes.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine the effectiveness of the IRS's enterprise strategy and implementation of ZTA technical solutions which restrict network accesses to trusted users, assets, and resources. To accomplish our objective, we:

- Determined whether the IRS will meet Federal requirements by interviewing IRS Cybersecurity function personnel, reviewing industry and Federal Government guidance and best practices, and assessing ZTA controls in place based on relevant documentation.
- Determined whether the IRS has developed an adequate budget for the implementation of ZTA by interviewing IRS Cybersecurity function personnel and by reviewing the ZTA budget request.
- Determined the IRS's ZTA implementation progress by evaluating the implementation metrics, interviewing IRS Cybersecurity function personnel to discuss the maturity stage for each of the five ZTA pillars, and evaluating the completeness of ZTA project items implemented in support of the five pillars by obtaining and reviewing the IRS's maturity model documentation.

Performance of This Review

This review was performed with information obtained from the Cybersecurity function responsible for ZTA located in the New Carrollton Federal Building in Lanham, Maryland, during the period May 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 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; Myron Gulley, Audit Manager; Kenneth Bensman, Acting Audit Manager; Charlene Elliston, Lead Auditor; and Laura Christoffersen, Data Analyst, Applied Research and Technology Division.

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 CISA draft Zero Trust Maturity Model guidance, IRS and independent contractor maturity model assessments, and Federal guidance from the Department of Homeland Security, the National Institute of

Standards and Technology, and the OMB. We evaluated these controls by interviewing IRS employees, analyzing relevant ZTA planning documentation, and reviewing the IRS and independent contractor assessments of the ZTA maturity.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

June 6, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Jeffrey W. King, Acting Chief Information Officer
Jeffrey King ffrkb cn=ffrkb, email=Jeffrey.W.King@irs.gov 2023.06.06 15:14:50 -04'00'

SUBJECT: Draft Audit Report – Actions Are Needed to Improve the Zero Trust Architecture Implementation (Audit #202220004)

Thank you for the opportunity to review and comment on the subject draft audit report. The IRS strives to continually evolve and sustain the robust and multi-layered cybersecurity program currently protecting taxpayer data and IRS resources. We intend to implement all the necessary controls under the Zero Trust Architecture (ZTA) framework to ensure the enterprise remains resilient against any unauthorized access.

Based on an independent assessment of the agency's ZTA maturity levels conducted just one month after draft Federal guidance was released in 2021, enterprise assets are protected at appropriate levels. Since that initial independent assessment was conducted, we have taken a series of additional steps, including implementing cost-effective solutions that meet or exceed federal cybersecurity standards.

The IRS previously submitted technical comments addressing several accuracies, contextual and other issues under a separate cover, and we appreciate your team making the necessary corrections. We concur with the four recommendations in this draft report and plan to complete implementation of all corrective actions by September 15, 2023.

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 Richard Therrien, Director of Cybersecurity Operations, at (240) 613-5262.

Attachment

Attachment

TIGTA Audit 202220004 – Actions Are Needed to Improve the Zero Trust Architecture Implementation

Recommendations

RECOMMENDATION 1: The Chief Information Officer should identify a ZTA budget estimate from the managed projects and initiatives.

CORRECTIVE ACTION: The IRS agrees with the recommendation. The Chief Information Officer will obtain a budget estimate identified by the managed projects and initiatives that support ZTA.

IMPLEMENTATION DATE: September 15, 2023

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

RECOMMENDATION 2: The Chief Information Officer should ensure the ZTA plan is revised to include defined roles and responsibilities.

CORRECTIVE ACTION: The IRS agrees with the recommendation. The Chief Information Officer will update the ZTA plan to include roles and responsibilities for programs, projects and initiatives identified.

IMPLEMENTATION DATE: September 15, 2023

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

RECOMMENDATION 3: The Chief Information Officer should enhance the ZTA roadmap to include a schedule for completion, address the gap analysis, and prioritize specific activities within each of the five ZTA pillars to ensure full implementation across the enterprise.

CORRECTIVE ACTION: The IRS agrees with the recommendation. The Chief Information Officer will enhance the ZTA roadmap to include specific activities based on the ZTA five pillars for the enterprise.

IMPLEMENTATION DATE: September 15, 2023

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

Attachment

TIGTA Audit 202220004 – Actions Are Needed to Improve the Zero Trust Architecture Implementation

RECOMMENDATION 4: The Chief Information Officer should reassess the ZTA implementation progress to ensure management has accurate and complete information to inform planning and the budget process.

CORRECTIVE ACTION: The IRS agrees with the recommendation. The Chief Information Officer will reassess the ZTA implementation progress and advise management for informational and budget planning purposes.

IMPLEMENTATION DATE: September 15, 2023

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

Appendix III

Glossary of Terms

Term	Definition
Cybersecurity	A function within the IRS Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Executive Order	A legally binding order given by the President, acting as the head of the Executive Branch, to Federal administrative agencies. Executive Orders are generally used to direct Federal agencies and officials in their execution of congressionally established laws or policies.
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.
Information Technology	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines for providing adequate information security for all Federal agency operations and assets.
Office of Management and Budget	The Federal agency that oversees the preparation and administration of the Federal budget and coordinates Federal procurement, financial management, information, and regulatory policies.
Pilot	A limited version (limited functionality or limited number of users) of a system being deployed to discover and resolve problems before full implementation.
Zero Trust Architecture	An end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure.

Appendix IV

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
IRS	Internal Revenue Service
OMB	Office of Management and Budget
ZTA	Zero Trust Architecture

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.