TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The IRS Implemented the Business Entitlement Access Request System; However, Improvements Are Needed

March 22, 2023

Report Number: 2023-20-013

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

HIGHLIGHTS: The IRS Implemented the Business Entitlement Access Request System; However, Improvements Are Needed

Final Audit Report issued on March 22, 2023 **Report Number 2023-20-013**

Why TIGTA Did This Audit

The IRS established a Continuous Diagnostics and Mitigation Program to be delivered in three phases. The second phase of the program supports the goal of managing "who is on the network" through identity and access management and privileged account management tools. This audit is focused on the second phase of the program.

The objectives of this audit were to evaluate the Continuous Diagnostics and Mitigation Program progress to date for deployment of the Business Entitlement Access Request System and the Privileged User Management Access System, and to determine if the Business Entitlement Access Request System access and security controls align with Federal guidance.

Impact on Tax Administration

Identity and access management is a fundamental and critical information technology capability ensuring that the right people have the right access to the right resources at the right time. If an unauthorized access occurs, it could result in substantial harm to systems and a loss of public confidence in the IRS.

What TIGTA Found

The IRS completed the first phase of the Continuous Diagnostics and Mitigation Program in April 2020 and implemented prior TIGTA recommendations. For the second phase, TIGTA determined that the Business Entitlement Access Request System is deployed and uses both on-premise servers and off-premise cloud-based servers. TIGTA reviewed configuration compliance reports for eight on-premise servers and found no failed risk issues. TIGTA also reviewed vulnerability scans for both on-premise and off-premise cloud-based servers and determined that the off-premise server vulnerability scans had limited risk severity and no historical aging information. The limited data showed open vulnerabilities that exceeded allowable remediation timeframes. In December 2022, TIGTA verified the cloud service provider upgraded its server vulnerability reporting to include aging and risk severity level information.

TIGTA also found that the remediation of on-premise server vulnerabilities is not consistently or accurately tracked with plans of action and milestones or risk-based decisions as required. The IRS created two plans of action and milestones eight and 21 months, respectively, after the vulnerabilities were identified, instead of within 60 days from identification, as required.

The Business Entitlement Access Request System is used to request, modify, and remove access for active users to systems; re-certify and validate user access; and remove access for separated and furloughed users and for user inactivity on the system. According to the IRS's Cybersecurity function, the Business Entitlement Access Request System's cloud-hosted solution resolved several outstanding security issues with the obsolete legacy system it replaced, such as multi-factor authentication and integration with the new Privileged User Management Access System.

TIGTA also determined that the deployment of the Privileged User Management Access System is complete and the system is operational. According to the IRS, the Privileged User Management Access System provides numerous security enhancements including advanced auditing of user activity, session recording, and multi-factor authentication.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that: 1) applicable monitoring is performed to provide adequate oversight of the off-premise servers; and 2) plans of action and milestones or risk-based decisions are timely documented, as required.

The IRS agreed with both recommendations. The IRS plans to monitor and provide adequate oversight of the off-premise servers and timely document plans of action and milestones or risk-based decisions, as required.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

March 22, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS Implemented the Business Entitlement Access Request System; However, Improvements Are Needed
(Audit # 202220019)

This report presents the results of our review to evaluate the Continuous Diagnostics and Mitigation Program progress to date for deployment of the Business Entitlement Access Request System and the Privileged User Management Access System, and to determine if Business Entitlement Access Request System access and security controls align with Federal guidance. This review is part of 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 III. 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

Appendices

Background

The Internal Revenue Service (IRS) developed a Continuous Diagnostics and Mitigation (CDM) Program Project Management Plan dated April 1, 2016, to align with the objectives of the Department of Homeland Security CDM Program that covers 15 continuous diagnostic capabilities to be delivered in three phases:

- Phase 1 – What is on the network (manage assets)?
- Phase 2 – Who is on the network (manage accounts for people/services)?
- Phase 3 – What is happening on the network (manage events)?

The CDM Program's Phase 2 supports business capabilities for identity and access management and privileged account management tools. The Business Entitlement Access Request System (BEARS) and the Privileged User Management Access System (PUMAS) together comprise CDM Phase 2. BEARS is designed to address identity and access management. The BEARS does not collect taxpayer information and replaced the obsolete Online 5081 system. In February 2021, the IRS began migrating applications and users over to the BEARS and completed migration in August 2022.

The BEARS system manages the identity access management at the IRS. The system is used to request, modify, and remove access for active users to IRS systems by managing the digital identity of individuals, roles, resources, and entitlements granted or removed.

The BEARS system uses a Commercial off the Shelf platform:

8 on-premise servers

9 off-premise cloud-based servers

The PUMAS manages privileged accounts and replaced the Total Privileged Access Management system.[1] In May 2021, the IRS began migrating privileged accounts and applications to the PUMAS and completed migration in December 2021.

Results of Review

Continuous Diagnostics and Mitigation Program Phase 1 Is Complete

IRS CDM Program Phase 1 entailed installing sensor tools to identify authorized hardware and software assets and ensure that they are properly configured with vulnerabilities mitigated. We determined that the IRS completed CDM Phase 1 in April 2020. We evaluated the CDM program's progress by reviewing documented accomplishments, milestones, lessons learned, and program status updates. For example, lessons learned included ensuring that contractors with development responsibilities are provided more timely security clearances and that more time and resources are allowed for transitioning applications using outdated technologies. The CDM Phase 1 program status updates included reports to governance boards and other stakeholders.

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

In addition, we followed up on three recommendations in a prior report on CDM Phase 1.[2]

- Recommendation 1: Implement performance metrics in order to enable management to better determine the program's status.

  The IRS consolidated standards, scope, and metrics and established step-by-step procedures in the new Data Quality and Consistency Monitoring Guide in August 2020. We reviewed the Data Quality and Consistency Monitoring Guide and determined that it sufficiently addressed our recommendation, if followed. We could not test these metrics because the CDM data feed from the IRS to the Department of the Treasury's (hereafter referred to as the Treasury Department) dashboard was shut down as directed by the Cybersecurity and Infrastructure Security Agency in January 2021. The IRS is currently working with the Treasury Department's designated contractor to set up the updated CDM data feed and dashboard. The IRS stated that the updated dashboard will likely be completed in the first quarter of Calendar Year 2023.

- Recommendation 2: Coordinate with segmented network administrators to obtain complete and accurate asset data.

  The IRS implemented the previous endpoint management sensor tool in all segmented networks. The IRS also implemented a new endpoint sensor tool that further improves on this data. We reviewed a November 2022 inventory report from the new sensor tool and determined that the IRS completed the work to implement asset discovery in all segmented networks. The report showed asset information per segmented network, such as the device counts, whether the devices were compliant, and the fail frequency of the devices.

- Recommendation 3: Complete the installation, configuration, and testing of sensor tools to ensure the accuracy of data transmitted to the Treasury Department's dashboard.

  In addition to working toward restoring the CDM data feed, the IRS also stated that the Treasury Department's contractor will perform data quality testing to ensure the integrity of the data sent to the dashboard. We reviewed the Data Quality Management Plan developed by the contractor and determined that the plan provides criteria, factors impacting data quality, and recommendations for improving data quality that, if implemented, should assist in the process of ensuring data integrity.

The IRS implemented corrective actions to address the prior recommendations; however, we could not test the effectiveness of the actions taken because the CDM data feed from the IRS to the Treasury Department's dashboard was shut down.

In October 2022, the Cybersecurity and Infrastructure Security Agency issued a binding operational directive that requires Federal agencies to complete the following actions:[3]

- By April 3, 2023:
  - Perform automated asset discovery every seven days.

[2] Treasury Inspector General for Tax Administration, Report No. 2020-20-013, *The Continuous Diagnostics and Mitigation Project Effectiveness Would Be Improved by Better Performance Metrics and Tools Data* (Mar. 2020).

[3] Cybersecurity and Infrastructure Security Agency, Binding Operational Directive 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks* (Oct. 3, 2022).

  - Initiate vulnerability enumeration across all discovered assets, including all discovered roaming devices (*e.g.*, laptops), every 14 days.
  - Deploy an updated CDM dashboard configuration that enables access to object-level vulnerability enumeration data.
- Within six months of the Cybersecurity and Infrastructure Security Agency publishing requirements for vulnerability enumeration performance data, all Federal agencies are required to initiate the collection and reporting of vulnerability enumeration performance data to the updated CDM dashboard.

The IRS CDM management team stated that the work to address this new directive is underway in another Cybersecurity function team. The new vulnerability enumeration performance data collected will be incorporated as necessary once the data feeds resume and the updated CDM dashboard is functional.

Management and Oversight of the Business Entitlement Access Request System Servers Needs Improvement

Configuration compliance of on-premise servers

Seventeen servers support the BEARS: nine off-premise cloud-based servers and eight on-premise servers. We reviewed multiple May 2022 configuration compliance reports for the eight BEARS on-premise servers and found that configuration management was compliant with no failed risk issues. According to the National Institute of Standards and Technology, the configuration of a system and its components has a direct impact on the security posture of the system.[4] The security-focused configuration management process is critical to maintaining a secure state under normal operations, contingency recovery operations, and reconstitution to normal operations. In addition, we requested but did not receive configuration compliance reports for the nine off-premise cloud-based servers. According to the BEARS System Security Plan, the IRS is not responsible for the configuration and maintenance of the nine off-premise cloud-based servers.

Security vulnerability remediation on off-premise servers

According to the BEARS project documentation[5] and the Federal Risk and Authorization Management Program documentation provided by the IRS, the Treasury Department is responsible for managing and remediating the vulnerabilities identified on the nine BEARS off-premise cloud-based servers. According to the BEARS System Security Plan, the IRS BEARS cloud-hosted solution leverages a cloud service managed by the Treasury Department. We reviewed vulnerability scan reports from November 2021 through March 2022 for the nine BEARS off-premise servers. However, those scans contained limited severity of risk data (*e.g.*, critical, high, medium, low) for the vulnerabilities identified and no historical aging information, such as first seen and last seen dates. This lack of information about the vulnerabilities hindered

[4] National Institute of Standards and Technology, Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (Aug. 2011).

[5] IRS, *Business Entitlement Access Request Cloud System Security Plan* (Jan. 26, 2021).

our ability to use the scans to conduct a thorough analysis. The IRS stated there were configuration issues with the cloud-based scan reporting tool during this time period.

During our review, the Treasury Department reconfigured its scan reporting tool to include the first seen and last seen dates of each vulnerability. The IRS provided new scans for the cloud-based servers dated September 16, 2022. We found in this off-premise server scan 743 (93 percent) of 796 vulnerabilities across eight of the nine cloud-based servers were identified as having a severity risk level of "None" and were listed merely for informational purposes. The remaining 53 vulnerabilities (7 percent) identified the first and last seen dates that potentially would allow us to determine whether remediation is occurring timely according to IRS policy. However, all 53 vulnerabilities were still unremediated and we could not determine how many would be remediated timely at some future date. Some vulnerabilities were open since July 2021 and are therefore already outside acceptable remediation timeframes.

According to the BEARS System Security Plan, the BEARS administrative team is supposed to review the off-premise vulnerability scans periodically to determine if new vulnerabilities exist, but the IRS could not provide evidence to demonstrate this process is occurring. If the off-premise server scans do not consistently provide complete vulnerability information, vulnerabilities that are not reviewed or timely remediated increase the potential risk of exploitation by external and internal threats.

Management Action: At the end of our audit, the IRS provided the December 2022 off-premise server scans and we verified that the scans now include aging and risk severity level information about vulnerabilities. This information will allow the IRS to determine the length of time such vulnerabilities have been unremediated and to better manage remediation priorities.

Recommendation 1: The Chief Information Officer should ensure that applicable monitoring is performed to provide adequate oversight of the Treasury-hosted BEARS servers.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will ensure that applicable monitoring is performed to provide adequate oversight of the Treasury-hosted BEARS servers.

Security vulnerability remediation on on-premise servers

The IRS manages and remediates vulnerabilities identified on the eight on-premise servers that support the BEARS. We reviewed the May 18, 2022, vulnerability scan report and determined:

There were 423 vulnerabilities:

- 348 (82 percent) critical (two unique) that were timely remediated.
- 31 (7 percent) medium and high vulnerabilities that were timely remediated.
- 44 (10 percent) medium and high vulnerabilities that were not timely remediated:
    - 5 high (one unique) vulnerabilities exceeded the IRS policy of 90 days for remediation.
    - 39 medium (six unique) vulnerabilities exceeded the IRS policy of 120 days for remediation.

The percentages do not add up to 100% due to rounding.

The Internal Revenue Manual states that vulnerabilities shall be prioritized for remediation based on risk severity (highest to lowest) using the Common Vulnerability Scoring System scores provided by the scanning tools.[6] Figure 1 shows the vulnerability severity risk level score ranges and their associated remediation timeframes.

Figure 1: Common Vulnerability Scoring System Ranges and the Associated Severity Risk Level and Remediation Timeframes

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

Source: Internal Revenue Manual 10.8.1.

Planned corrective actions

When a vulnerability cannot be remediated timely, the IRS Standard Operating Procedures requires system owners to develop a Plan of Action and Milestones (POA&M) for remediation or the authorizing officials must document the accepted risk to the network through a risk-based decision.[7]

We determined that 44 (10 percent) of the 423 vulnerabilities did require a POA&M or risk-based decision be created within 60 calendar days of the vulnerability identification according to Federal guidance for systems, like the BEARS, categorized as a moderate risk.[8] For the 44 unremediated vulnerabilities, we determined:

- The IRS properly tracked eight (18 percent) of the 44 vulnerabilities related to system upgrades with a documented POA&M.
    - POA&M 44611 covers five vulnerabilities (one unique) for which the POA&M was created within 60 calendar days of vulnerability identification.
    - POA&M 44412 covers three vulnerabilities (one unique) for which the POA&M was created within 60 calendar days of vulnerability identification.
- The IRS did not timely create POA&Ms for 36 (82 percent) of the 44 vulnerabilities.
    - POA&M 47230 covers seven vulnerabilities (one unique) for which the POA&M was not created within 60 calendar days of vulnerability identification. This POA&M was created over eight months after the vulnerability was first identified.

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

[7] IRS, *Enterprise Federal Information Security Modernization Act POA&M Standard Operating Procedures* (June 2020).

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

- POA&M 46773 covers 29 vulnerabilities (four unique) for which the POA&M was not created within 60 calendar days of vulnerability identification. This POA&M was created over 21 months after the vulnerabilities were first identified.

The IRS stated that the POA&Ms were delayed to allow additional time for resolution of issues involving a self-signed certificate, software upgrades, third-party migration efforts, and multiple project impacts across the infrastructure. In addition, the IRS stated these issues are enterprise-wide and are not specific to the BEARS. We concluded that the IRS is not ensuring that vulnerabilities exceeding remediation timeframes are consistently or accurately tracked as required via POA&Ms or risk-based decisions. Failure to resolve or track existing vulnerabilities compromises the security posture of the enterprise, potentially compromising taxpayer data and exposing information to unnecessary risk.

In addition, during our review of the BEARS POA&Ms, we identified two discrepancies between the date the vulnerability was first seen in the vulnerability scans and the date found in the Treasury Federal Information Security Management Act Inventory Management System where the IRS tracks POA&Ms. The IRS stated that a user error caused the creation of date discrepancies resulting in incorrect vulnerability age differences of over eight and 21 months, respectively. The IRS stated that every effort is made to align the date found to the actual scan finding. Errors in reporting and tracking vulnerability remediation may further expose systems and data by allowing internal and external actors more time to exploit known vulnerabilities.

Recommendation 2: The Chief Information Officer should ensure that POA&Ms or risk-based decisions are timely and accurately documented for vulnerabilities that exceed remediation timeframes for the BEARS servers.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will ensure that POA&Ms or risk-based decisions are timely and accurately documented for vulnerabilities that exceed remediation timeframes for the BEARS servers.

Identity and Access Management Is Accomplished Through the Business Entitlement Access Request System

We determined the IRS deployed the BEARS which provides identity and access management as part of its CDM Program's Phase 2. In order to confirm user identity and access management is managed through the BEARS, we asked the IRS to provide the population of user accounts with all fields of information associated with each of those accounts (*e.g.*, Name, User Status). The files requested and received were very large due to the number of IRS employees and systems, because each user entitlement is tracked separately for each system. The Cybersecurity function officials demonstrated what fields and information are tracked in the BEARS, and explained how each file addressed specific elements of our data request. Specifically, the IRS explained changes in the BEARS data between the June 2022 and November 2022 data extracts we reviewed. The June 2022 extract included 90,349 active users with a total of 990,215 system entitlements. The November 2022 extract included new entitlements for existing users, remaining migration efforts from the Online 5081 system that were completed in August 2022, and new user accounts for recently hired employees. The November 2022 extract shows the BEARS is tracking 116,542 active users with approximately 1.3 million system entitlements. The

IRS stated that the BEARS user information extract process will be improved to make user analysis more manageable.

National Institute of Standards and Technology guidelines classify identity and access management as a fundamental and critical information technology capability, and emphasize the importance of ensuring the right people have the right access to the right resources at the right time. The BEARS is used to request, modify, and remove access for active users to systems; re-certify and validate user access; and remove access for separated and furloughed users and for user inactivity on the system. In addition, Personally Identifiable Information, such as Employee Name, Standard Employee Identifier, Manager, and Office Number is also stored in the BEARS. According to Cybersecurity function officials, the BEARS cloud-hosted solution resolved several outstanding security issues with the obsolete legacy Online 5081 system it replaced. The BEARS security enhancements include: multi-factor authentication; elimination of custom legacy code that allows for efficient security updates and patches; direct connection with IRS systems to implement automated provisioning and deprovisioning of systems access based on user approval or revocation of BEARS entitlements; efficiencies in system account creation; and integration with the new PUMAS.

The Privileged User Management Access System Is Operational

The second part of the CDM Program Phase 2 included migrating user privileged account access controls from the Total Privileged Access Management system to the PUMAS. The Total Privileged Access Management system functioned as a server-based management tool for IRS users with approved privileged access; it was retired due to product end-of-life in December 2021. IRS officials stated that they began migrating privileged accounts and applications over to the PUMAS in May 2021 and completed this migration in December 2021. The PUMAS now manages administrative and service accounts on key infrastructure components such as Windows® and UNIX® servers, legacy computing platforms, and network devices.

We reviewed the PUMAS project documentation, such as migration schedules and system artifacts including the authority to operate and security plans and assessments, and determined that the migration to the PUMAS is complete and the system is operational. According to the IRS, the PUMAS provides numerous security enhancements including advanced auditing of user activity, session recording, and multi-factor authentication. We included an audit of PUMAS access controls management in our Fiscal Year 2023 Annual Audit Plan.

Appendix I

Detailed Objectives, Scope, and Methodology

The overall objectives of this audit were to evaluate the CDM Program progress to date for deployment of the BEARS and PUMAS, and to determine if BEARS access and security controls align with Federal guidance. To accomplish our objective, we:

- Determined whether CDM Phase 1 implementation was complete by interviewing CDM management for recent accomplishments, milestones, lessons learned, and program status; reviewing status reports to governance boards and other stakeholders; and assessing whether the IRS effectively implemented corrective actions for recommendations in our prior report.
- Determined whether configuration vulnerabilities were remediated within agency security policy for on-premise BEARS servers by analyzing server security configuration compliance reports.
- Determined the status of security controls in the BEARS and the system's alignment with Federal guidance by reviewing relevant criteria for systems development, deployment, and access and security controls; interviewing IRS officials and reviewing relevant project documentation to evaluate the status of the BEARS migration; and analyzing vulnerability scans of the on-premise servers and off-premise cloud-based servers. We also reviewed whether remediation occurred timely and whether accurate POA&Ms or risk-based decisions were created in lieu of timely remediation.
- Determined whether users are being managed by the BEARS by reviewing multiple data extracts spanning several months.
- Determined the current deployment status of the PUMAS by reviewing its System Security Plan, wave migration schedules, system records, and Authority to Operate, and by interviewing Cybersecurity function personnel about the status of the migration efforts.

Performance of This Review

This review was performed remotely with the CDM Program Office and the Cybersecurity function located in New Carrollton, Maryland, during the period March through December 2022. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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, Audit Manager; Mark Carder, Lead Auditor; Natalie Russell, Auditor; and Meera Dave, Information Technology Specialist (Data Extracts).

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 objectives: Internal Revenue Manual policies related to cloud computing security and information systems security requirements and National Institute of Standards and Technology requirements for controls that must be implemented within any system that processes, stores, or transmits information. We evaluated these controls by interviewing IRS employees, reviewing relevant CDM Program documentation, and analyzing configuration and security vulnerability scans of the BEARS.

Appendix II

Outcome Measure

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

Type and Value of Outcome Measure:

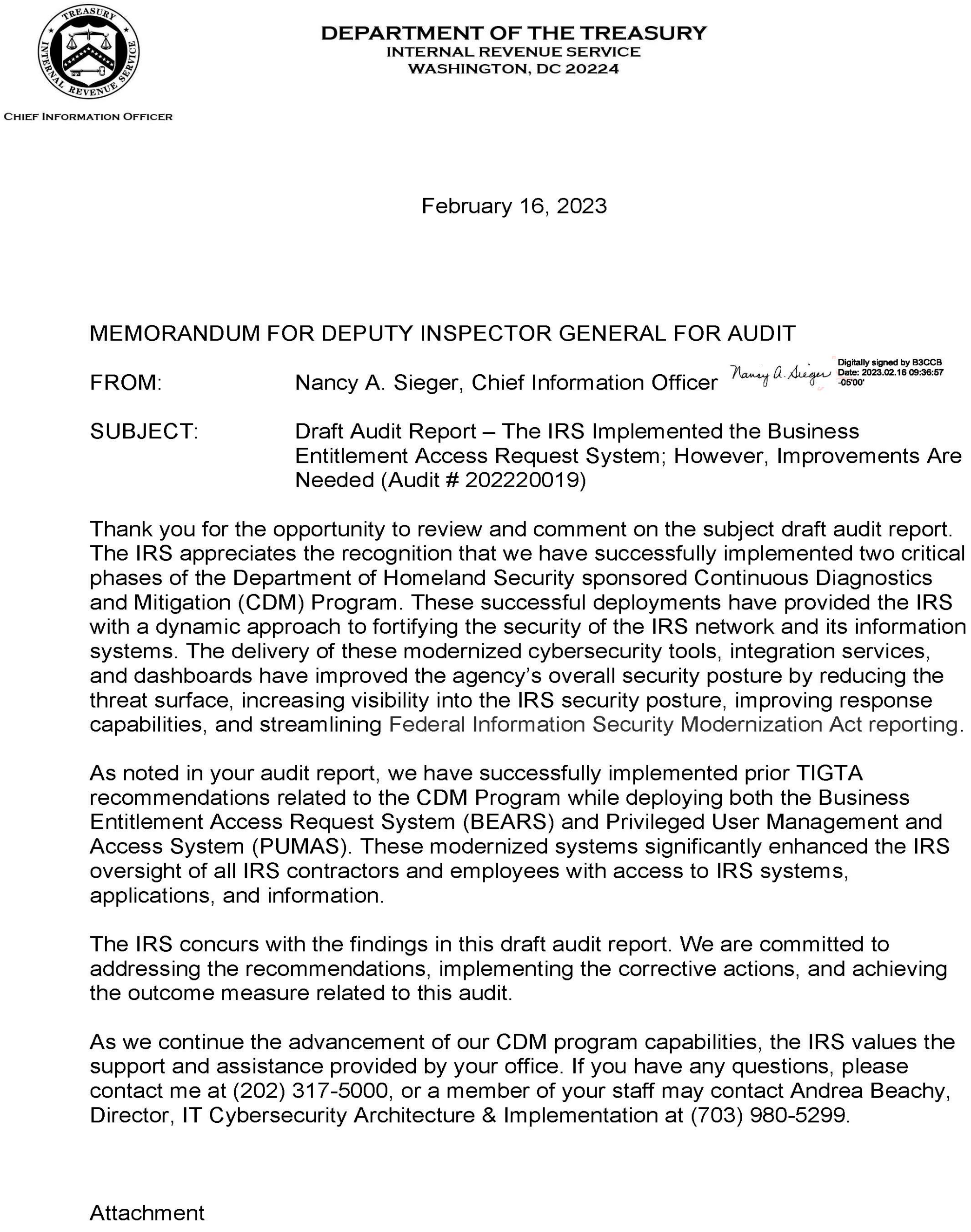
- Reliability of Information – Potential; 36 vulnerabilities (five unique) that exceeded the requirement for a POA&M to be created within 60 calendar days of vulnerability identification (see Recommendation 2).

Methodology Used to Measure the Reported Benefit

Our audit team analyzed the May 18, 2022, vulnerability scan report and found there were 44 vulnerabilities of which 36 vulnerabilities (five unique) across eight servers did not have timely POA&Ms. We also analyzed the first seen and last seen dates shown in the security vulnerability report to determine whether POA&Ms were timely created.

Appendix III

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

February 16, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger, Chief Information Officer Nancy A. Sieger Digitally signed by B3CCB Date: 2023.02.16 09:36:57 -05'00'

SUBJECT: Draft Audit Report – The IRS Implemented the Business Entitlement Access Request System; However, Improvements Are Needed (Audit # 202220019)

Thank you for the opportunity to review and comment on the subject draft audit report. The IRS appreciates the recognition that we have successfully implemented two critical phases of the Department of Homeland Security sponsored Continuous Diagnostics and Mitigation (CDM) Program. These successful deployments have provided the IRS with a dynamic approach to fortifying the security of the IRS network and its information systems. The delivery of these modernized cybersecurity tools, integration services, and dashboards have improved the agency's overall security posture by reducing the threat surface, increasing visibility into the IRS security posture, improving response capabilities, and streamlining Federal Information Security Modernization Act reporting.

As noted in your audit report, we have successfully implemented prior TIGTA recommendations related to the CDM Program while deploying both the Business Entitlement Access Request System (BEARS) and Privileged User Management and Access System (PUMAS). These modernized systems significantly enhanced the IRS oversight of all IRS contractors and employees with access to IRS systems, applications, and information.

The IRS concurs with the findings in this draft audit report. We are committed to addressing the recommendations, implementing the corrective actions, and achieving the outcome measure related to this audit.

As we continue the advancement of our CDM program capabilities, the IRS values the 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 Andrea Beachy, Director, IT Cybersecurity Architecture & Implementation at (703) 980-5299.

Attachment

Attachment

Recommendations

RECOMMENDATION 1: The Chief Information Officer should ensure that applicable monitoring is performed to provide adequate oversight of the Treasury-hosted BEARS servers.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will ensure that applicable monitoring is performed to provide adequate oversight of the Treasury-hosted BEARS servers.

IMPLEMENTATION DATE: July 15, 2023

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

RECOMMENDATION 2: The Chief Information Officer should ensure that POA&Ms or risk-based decisions are timely and accurately documented for vulnerabilities that exceed remediation timeframes for the BEARS servers.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will ensure that POA&Ms or risk-based decisions are timely and accurately documented for vulnerabilities that exceed remediation timeframes for the BEARS servers.

IMPLEMENTATION DATE: June 15, 2023

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

Appendix IV

Glossary of Terms

Term	Definition
Binding Operational Directive	A compulsory direction issued to Federal Executive Branch agencies for the purposes of safeguarding Federal information/information systems.
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.,* network, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Control	A process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. It comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. It also serves as the first line of defense in safeguarding assets.
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.
Cybersecurity and Infrastructure Security Agency	An agency that leads the national effort to understand, manage, and reduce risk to cyber and physical infrastructure and connects stakeholders in industry and Government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience.
Dashboard	Receives, aggregates, and displays information from Continuous Diagnostics and Mitigation project tools at the agency or Federal level.
Internal Revenue Manual	The primary, official source of IRS instructions to staff related to the organization, administration, and operation of the IRS.
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.
Off-Premise	A server hosted by a service provider. Providers are in charge of maintenance and administering the physical host or resources needed by an organization.
On-Premise	Servers hosted on a network or within a company infrastructure (*e.g.*, remote servers hosted in data centers) that are controlled, administered, and maintained by the organization.
Planned Corrective Action	The process of taking the appropriate steps to identify the root cause of a problem and implementing a solution that corrects the root cause as to prevent its recurrence.

Term	Definition
Privileged Access	Entry to an application or infrastructure that has its privileged accounts protected and that generally requires approval from either the requestor's manager, the application/infrastructure owner, or both.
Privileged Accounts	Accounts with set "access rights" for certain users on a given system. Sometimes referred to as system or network administrative accounts.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information services. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
Standard Employee Identifier	A five-digit code that identifies an IRS employee.
Unauthorized Access	The willful unauthorized access, attempted access, or inspection of taxpayer returns or return information.
User Activity Monitoring	The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information, *e.g.*, to detect insider threat.
User Status	The status of the employee as Active, Separated, or Inactive.
Vulnerability	Weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten network security.
Wave Migration	A summary/schedule of the accounts migrated from the Total Privileged Access Management system to the PUMAS and the estimated Go-Live date for each wave of accounts and the criteria attached to each wave.

Appendix V

Abbreviations

BEARS	Business Entitlement Access Request System
CDM	Continuous Diagnostics and Mitigation
IRS	Internal Revenue Service
POA&M	Plan of Action and Milestones
PUMAS	Privileged User Management Access System

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

(800) 366-4484

By Web:

www.tigta.gov

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 23291
Washington, D.C. 20026

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