TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Continuous Diagnostics and Mitigation Project Effectiveness Would Be Improved by Better Performance Metrics and Tools Data

March 18, 2020

Reference Number: 2020-20-013

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

THE CONTINUOUS DIAGNOSTICS AND MITIGATION PROJECT EFFECTIVENESS WOULD BE IMPROVED BY BETTER PERFORMANCE METRICS AND TOOLS DATA

Highlights

Final Report issued on March 18, 2020

Highlights of Reference Number: 2020-20-013 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

In Calendar Year 2013, the Department of Homeland Security established the Continuous Diagnostics and Mitigation Program as an implementation approach for continuously monitoring information systems. The Continuous Diagnostics and Mitigation Program is a multiyear program to automate security controls and deficiency management, and standardize risk reporting across Federal agencies. Incomplete data and insufficient data quality will result in IRS management using inaccurate information for decisionmaking concerning cybersecurity risks.

WHY TIGTA DID THE AUDIT

According to the Office of Management and Budget, the Continuous Diagnostics and Mitigation Program enhances the overall security posture of the Federal Government by providing agencies with capabilities to monitor vulnerabilities and threats to their networks in near real-time. This audit was initiated to determine the effectiveness and efficiency of the IRS's Continuous Diagnostics and Mitigation project implementation.

WHAT TIGTA FOUND

The IRS developed a schedule summary that provides the status of key milestones and completion dates for its Continuous Diagnostics and Mitigation project implementation. The IRS reported that it successfully completed key milestones for the first of two implementation waves. While data quality and the overall agency risk score have improved, the IRS did not fully develop and implement performance metrics to enable effective monitoring of the Continuous Diagnostics and Mitigation project deployment status and progress.

As part of the Continuous Diagnostics and Mitigation project, the IRS is installing sensor tools to identify authorized hardware and software assets and continuously ensure that they are properly configured with vulnerabilities mitigated. Data from these tools will be aggregated and transmitted to the Department of Homeland Security via the Department of the Treasury dashboard. When fully implemented, these tools should provide full network coverage for continuous monitoring. However, the IRS Continuous Diagnostic and Mitigation project sensor tools do not currently provide complete and accurate data.

WHAT TIGTA RECOMMENDED

The Chief Information Officer should continue the development and implementation of a data consistency and quality plan and performance metrics to allow management to readily monitor Continuous Diagnostics and Mitigation project status and progress; continue collaboration with the segmented network administrators to obtain complete and accurate data; and complete the installation, configuration, and testing of sensor tools to ensure the accuracy of data transmitted to the Department of the Treasury dashboard.

The IRS agreed with all our recommendations. The IRS plans to finalize a data consistency and quality plan and establish performance metrics, and will complete the installation, configuration, and testing of the sensor tools to ensure the accuracy of data transmitted to the Department of the Treasury dashboard. The IRS also stated it has completed work to implement the endpoint management sensor tool in all segmented networks and is currently monitoring to ensure that the sensor tool obtains complete and accurate data.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 18, 2020

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Continuous Diagnostics and Mitigation Project Effectiveness Would Be Improved by Better Performance Metrics and Tools Data (Audit # 201920003)

This report presents the results of our review to determine the effectiveness and efficiency of the Continuous Diagnostics and Mitigation project implementation. This review is included in our Fiscal Year 2020 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of Internal Revenue Service (IRS) Resources.

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

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

Table of Contents

Abbreviations

AWARE	Agencywide Adaptive Risk Enumeration
CDM	Continuous Diagnostics and Mitigation
DHS	Department of Homeland Security
IRS	Internal Revenue Service

Background

In Calendar Year 2013, the Department of Homeland Security (DHS) established the Continuous Diagnostics and Mitigation (CDM) Program as an implementation approach for continuously monitoring information systems. According to the National Institute of Standards and Technology,[1] the DHS CDM Program is designed to facilitate automated security control assessment and continuous monitoring that is consistent with established guidance by providing a robust, comprehensive set of monitoring tools, a continuous monitoring dashboard,[2] and implementation assistance. On October 25, 2018, the Office of Management and Budget issued guidance[3] on Federal Information Security and Privacy Management Requirements. According to the Office of Management and Budget, the CDM Program enhances the overall security posture of the Federal Government by providing agencies with capabilities to monitor vulnerabilities and threats to their networks in near real-time. This program will increase situational awareness and allow agencies to prioritize actions to mitigate or accept cybersecurity risks based on an understanding of the potential impacts to their mission.

According to the Information Systems Audit and Control Association,[4] a CDM program provides information technology managers with a comprehensive and up-to-date inventory of assets and configurations so that they understand what is on their networks and where there may be vulnerabilities. An industry paper[5] explains that, while it is impossible for a CDM program to close all security gaps, it does enable centralized reporting of network activity with automated responses when applicable, thus freeing time to respond to infrastructure vulnerabilities.

Per the Internal Revenue Service's (IRS) CDM Project Management Plan dated April 1, 2016, the objectives of the DHS CDM Program were to automate security controls and deficiency management and standardize risk reporting across Federal agencies. The CDM Program covers 15 continuous diagnostic capabilities, which will be delivered in four phases (the IRS plan only included three of the phases):

- Phase 1 - What is on the network (manage assets)?
- Phase 2 - Who is on the network (manage accounts for people and services)?

[1] National Institute of Standards and Technology, *Interagency Report 8011, Volume 1, Automation Support for Security Control Assessments* (June 2017).
[2] See Appendix IV for a glossary of terms.
[3] Office of Management and Budget, *Memorandum M-19-02 Guidance on Federal Information Security and Privacy* (Oct. 25, 2018).
[4] Information Systems Audit and Control Association Journal, *Implementing an Information Security Continuous Monitoring Solution-A Case Study* (Jan. 2015).
[5] Fortinet, *Continuous Diagnostics and Mitigation in the Dynamic and Evolving Federal Enterprise* (May 14, 2018).

- Phase 3 – What is happening on the network (manage events)?
- Phase 4 – What role exists for emerging tools and technologies? Phase 4 was not included in the IRS's CDM Project Management Plan.

The CDM Program posted revised program objectives, dated April 24, 2019, to provide cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security posture. CDM Program objectives are to:

- Reduce agency threat surface.
- Increase visibility into the Federal cybersecurity posture.
- Improve Federal cybersecurity response capabilities.
- Streamline Federal Information Security Modernization Act reporting.

The CDM Program delivers capabilities in five key program areas.

- Dashboard.
- Asset management.
- Identity and access management.
- Network security management.
- Data protection management.

The DHS tasked Booz Allen Hamilton with implementing the CDM Program for six Federal agencies, including the Department of the Treasury (hereafter referred to as the Treasury Department) and the IRS. The IRS's implementation of the CDM Program is a major project sponsored by the Information Technology organization's Cybersecurity function and supported by the Cybersecurity Architecture and Implementation function.

The IRS established the CDM project in December 2015 and completed the required steps in the Enterprise Life Cycle commercial off-the-shelf development path[6] in July 2018. While the DHS did not establish due dates for the program phases, IRS CDM project management organized the Phase 1 implementation into two waves. The first wave, completed in July 2018, entailed installing sensor tools to identify authorized hardware and software assets and ensure that they are properly configured with vulnerabilities mitigated. Data from these sensor tools will be aggregated and reported to the DHS via the Treasury Department dashboard. When fully implemented, these sensor tools should provide full network coverage.

There are several tools involved in delivering the final CDM project solution. The IRS developed a Phase 1 schedule summary that outlines critical milestones for CDM project tools

[6] Internal Revenue Manual 2.16.1, *Enterprise Life Cycle Guidance* (Nov. 26, 2019).

implementation, data flow, configuration settings management, and organizational readiness. For example, one milestone involved an upgrade to one of the sensor tools that the CDM project team completed on May 13, 2019. A milestone involving data quality review was completed on September 24, 2019. The IRS reported that it successfully completed key milestones on schedule for the first implementation wave, which included the deployment of the following sensor tools:

- The IRS purchased and implemented the first sensor tool prior to the CDM project in Calendar Year 2011. The tool's functionality is incorporated into the CDM project. This sensor tool conducts vulnerability scanning of applications installed on a host. It includes a reporting component that allows customers to prioritize security weaknesses.
- The DHS purchased the second sensor tool in September 2016 as part of the DHS CDM project procurement. The IRS implemented the tool in Calendar Year 2017. The sensor tool detects and classifies all information technology assets on the network. It collects information from and about each device and maintains a real-time inventory.
- The IRS purchased a third sensor tool in Calendar Year 2017 and implemented it in Calendar Year 2018. This tool was designed to provide software inventory, compliance reporting, and endpoint management.

The DHS purchased an application management software tool for use in the CDM project. This tool allows the management of application access and user privileges across desktops and servers. It uses whitelists to allow user access to trusted applications as well as blacklists, which are used to deny user access to applications. The DHS suspended the implementation of this application management tool due to technical difficulties within the IRS environment and at other Treasury Department bureaus. The IRS is awaiting guidance from the DHS concerning the use of this application management tool.

The IRS CDM project uses two additional software tools to manage the information collected from the sensor tools. The first tool is a data management tool that sorts, filters, and indexes real-time data collected from the three sensor tools into a searchable repository. The IRS purchased this data management tool in September 2016, implemented it in Criminal Investigation in March 2018, and then implemented it to the rest of the enterprise in July 2018. The original purchase included one license for Criminal Investigation and a larger license for the enterprise.

The IRS and the Treasury Department use the second tool to organize and display CDM project information at the Federal level in a dashboard format. Using visualizations and business intelligence tools, the dashboard tool consolidates monitored and historical data to gain a holistic view that will help identify patterns and abnormal activity. The DHS pays for the dashboard tool software license for all Federal agencies.

According to the IRS, the second wave of CDM Phase 1 will involve continued efforts to improve data accuracy and deploy the remaining capabilities. Activities involved in the second

wave include device boundary and assignment integration, upgrades to CDM project tools, and organizational readiness. IRS CDM project management initially estimated the second wave of Phase 1 would be complete by December 31, 2019. However, at the December 12, 2019, Associate Chief Information Officer meeting, the scheduled completion date for the second wave of CDM Phase 1 was changed to May 1, 2020, to avoid risk to Filing Season operations.

For Fiscal Years 2016 through 2018, the IRS spent almost $13.5 million on hardware, software, and services for CDM Phase 1 project implementation. The IRS budgeted nearly $8 million for Fiscal Year 2019. By the end of Fiscal Year 2019, the total costs of the IRS CDM project will be approximately $21.5 million.

This review was performed at the IRS Cybersecurity office in Lanham, Maryland, during the period March through November 2019. 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. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Data Quality Has Improved, but Performance Metrics Have Not Been Fully Implemented

In June 2019, we requested the plan used to manage the CDM project data consistency effort. IRS CDM project management explained that they had not developed an IRS-specific plan and were relying on the DHS March 28, 2019, guidance.[7] This guidance describes the identification of data consistency concerns and the potential causes for these anomalies. The DHS document provides guidance to agencies and integrators[8] intended to resolve these concerns and prevent further occurrences of the inconsistencies. The DHS document provides 11 data consistency problems reported by integrators and 18 data consistency concerns reported by agencies.

- Of the 11 problems reported by the integrators, the IRS has five of the same concerns. These concerns include increased network device count because network switches register each device address on the switch as a separate uniquely identified device, and incomplete hardware and software asset management and vulnerability scanning tool deployments resulting in incomplete data integration and reporting visibility.
- Of the 18 concerns reported by the agencies, the IRS has 10 of the same concerns. These concerns include misidentified or inaccurately categorized assets, inaccurate or not current asset records, and undefined data consistency monitoring standards.

We requested evidence of the performance measures or metrics used by the CDM project to monitor implementation progress. However, the IRS was unable to provide adequate support. For example, in response to our request, we received a spreadsheet developed by Booz Allen Hamilton that appears to provide relevant status information and data totals for each CDM project sensor tool at one point in time. CDM project management explained that this spreadsheet was only used one time to determine if data were adequately flowing through the process from the sensor tools. The CDM project did not incorporate the spreadsheet as a tool to be used to manage or monitor implementation progress on an ongoing basis. The IRS did provide evidence for the testing of sensor tools.

After we presented our findings to management in November 2019, the IRS provided documentation as evidence of baselines and performance metrics that included:

[7] DHS, *Continuous Diagnostics and Mitigation Data Consistency Management Guidance* (Mar. 2019).
[8] The March 2019 DHS CDM Agency Dashboard Concept of Operations identifies Booz Allen Hamilton contractor employees as 'integrators' to provide support for implementing a common set of CDM project capabilities.

- A draft *Data Consistency and Quality Plan* dated August 27, 2019, which explains the methodology for data consistency and quality review.
- A data consistency briefing document dated October 6, 2019, which describes the methodology, tools, metrics, and target data quality goals.
- A spreadsheet dated November 6, 2019, that describes the monitoring of the data quality results.

CDM project management stated that these metrics were recently implemented and were considered to be still evolving in an effort to improve the data quality presented on the Treasury Department dashboard.

The Treasury Department dashboard presents the Agencywide Adaptive Risk Enumeration (AWARE) risk indicator score. This score is based on software vulnerabilities, configuration settings vulnerabilities, and endpoints. The AWARE score measures basic elements of an organization's cybersecurity posture, including unauthorized hardware, software vulnerabilities, and configuration management. The AWARE score does not reflect risk acceptance or other technical mitigation. It provides a raw score for an asset. The AWARE score is designed to determine an entity's performance and security posture. The IRS AWARE score improved from 5.27 per device to 0.30 per device from March to June 2019. Contributing factors to the improvement of the AWARE score were the removal of duplicate devices and device patching activities. While the IRS is working with the AWARE score checklist developed by Booz Allen Hamilton to identify opportunities to continue the improvement of the score, it has yet to develop an acceptable target score.

Due to the continuous adjustment and improvement of factors affecting the AWARE scores, such as the implementation and upgrading of sensor tools, device patching, and data filtering, CDM project management did not establish preliminary baselines or targets for the CDM project. When asked why baselines or targets had not been established for data consistency, CDM project management described the difficulty in establishing baselines and targets in such a fluid environment in which the baselines are continuously changing. For example, devices such as switches register each address on the switch as a separate uniquely identified device. Eliminating multiple duplicative records for a single device will affect the dashboard risk-indicator scoring. IRS CDM project management stated that the DHS has not established targets for CDM project data consistency.

According to the Government Accountability Office,[9] a performance measure is a means of evaluating the entity's performance in achieving objectives. The establishment and review of performance measures and indicators are examples of common control activities. The standards state that management establishes activities to monitor performance measures and indicators.

[9] Government Accountability Office, *Standards for Internal Control in the Federal Government* (Sept. 2014).

These may include comparisons and assessments relating different sets of data to one another so that analysis of the relationships can be made and appropriate actions taken.

Without established performance metrics or measurement tools, management is unable to determine the project's status or improvement over time. Without this information, management risks errors in decisionmaking while implementing the project. We were unable to determine the effectiveness of the IRS CDM project implementation because no performance measurement tools were developed or implemented that might be used to gauge the current progress of the data consistency effort.

Recommendation

Recommendation 1: The Chief Information Officer should continue the development and implementation of a data consistency and quality plan, and performance metrics to allow management to readily monitor CDM project status and progress.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will finalize a data consistency and quality plan and establish performance metrics that will allow management to monitor progress.

Continuous Diagnostic and Mitigation Sensor Tools Do Not Provide Complete and Accurate Data

The IRS is using CDM project sensor tools to identify and report data on its information technology assets. However, the reported data are incomplete and require quality improvement. For example, the IRS has not completely identified all of the information technology assets in the segmented networks not managed by the Enterprise Operations function.

In a September 27, 2019, briefing to Cybersecurity function management, the project team reported[10] on the quality of CDM project data. Of the nine metrics reported, six metrics were categorized as below acceptable quality. These metrics identified missing device data from the endpoint management and the asset detection sensor tools. Therefore, the device data from the tools are incomplete. The other metrics stated that total device counts were inaccurate and vulnerable devices were missing.

The IRS is in the process of implementing an upgrade to the endpoint management tool that communicates with the tool that transmits data to the Treasury Department dashboard. The tool upgrade will provide increased functionality and performance for the delivery of hardware, software, and configuration management settings information on devices with sensor tool endpoints. According to the IRS, the endpoint management sensor tool has been implemented in five of the six segmented networks. The remaining network segment for the Research Applied

[10] IRS, *CDM Data Consistency and Quality Review – Draft* (Sept. 2019).

Analytics and Statistics, Statistics of Income is approximately 18.3 percent completed. The IRS CDM project data for the segmented networks will be incomplete until full deployment of the tool is completed. In addition, due to technical difficulties with segmented networks' firewalls and ports, the asset detection sensor tool is unable to capture all the detailed information of each endpoint in the segmented networks. The IRS is currently investigating this challenge in each segmented network. CDM project management estimates that the asset detection sensor tool covers approximately 80 percent to 90 percent of information technology assets on the IRS network.

According to the CDM Agency Dashboard Concept of Operations,[11] data quality is considered a key to success. In addition to strong governance and asset management, agencies must also ensure that data collected by CDM project tools are accurate, thorough, and timely. Ensuring data quality is a major building block for the CDM project and is fundamental to ensuring that stakeholders have the correct information to make informed risk decisions and prevent misrepresentation of the cybersecurity landscape.

Incomplete data and insufficient data quality can adversely affect decisions related to cybersecurity risks. Management needs accurate information on an ongoing basis to prioritize and minimize risks based on potential impacts.

Recommendations

The Chief Information Officer should:

Recommendation 2: Continue collaboration with the segmented network administrators to obtain complete and accurate data for CDM.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has completed work to implement the endpoint management sensor tool in all segmented networks. The IRS is currently monitoring to ensure that the sensor tool obtains complete and accurate data.

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

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will complete the installation, configuration, and testing of the CDM sensor tools to ensure the accuracy of data transmitted to the Treasury Department dashboard.

[11] DHS, *Continuous Diagnostics and Mitigation Agency Dashboard Concept of Operations* (Mar. 2019).

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine the effectiveness and efficiency of the CDM project implementation. To accomplish our objective, we:

I. Determined whether the IRS is following Federal Government criteria and requirements, and non-Government best practices while implementing the CDM project.

   A. Reviewed, analyzed, and summarized criteria and requirements from sources such as legislation, the Office of Management and Budget, the DHS, Internal Revenue Manuals, and the National Institute of Standards and Technology.

   B. Reviewed, analyzed, and summarized non-Government industry best practices.

   C. Determined whether the IRS is completing the required steps in the Enterprise Life Cycle commercial off-the-shelf development path.

II. Determined whether the IRS is effectively leveraging DHS procurement capabilities to acquire and maintain tools for the CDM project and verified those tools effectively meet CDM project function goals and the capacity and performance needs of the IRS.

   A. Determined what tools the IRS implemented for CDM project functions.

   B. Determined whether the tools the IRS implemented are effectively meeting CDM project function goals.

   C. Determined whether the IRS performed testing to determine performance issues prior to installing and using CDM project sensor tools.

III. Determined the effectiveness of the IRS's approach to ensuring the integrity and reliability of data used in the CDM project dashboard.

   A. Determined whether the IRS has developed a data consistency plan that includes the definition of data consistency requirements, metrics, and business rules.

   B. Determined whether the IRS is using unreliable data to determine the AWARE score and any potential impact that may have on identifying security vulnerabilities.

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: DHS, Department of the Treasury, IRS, and Booz Allen Hamilton policies, procedures, processes, and best practices for CDM project implementation and data consistency. We evaluated these controls by reviewing the Government Accountability Office *Standards for Internal Control in the Federal Government* and evaluating IRS processes against these standards; interviewing officials; and reviewing CDM project status reports, executive briefings, and performance measures and metrics for the data consistency process.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Jena Whitley, Director
Myron Gulley, Audit Manager
Corey Brown, Lead Auditor
Avery Dortch, Information Technology Specialist

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Strategy and Planning
Director, Security Risk Management
Director, Enterprise Audit Management

Appendix IV

Glossary of Terms

Term	Definition
Agencywide Adaptive Risk Enumeration Score	A score based on software vulnerabilities, configurations setting vulnerabilities, and endpoints unassociated with Federal Information Security Modernization Act of 2014[1] boundaries.
Blacklist	List of applications to which users should not have access.
Continuous Diagnostics and Mitigation Program	Provides tools, integration services, and dashboards to all participating agencies to improve their respective agency security postures to defend against cybersecurity threats and vulnerabilities.
Cybersecurity Function	Responsible for ensuring IRS compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of electronic systems, services, and data.
Dashboard	Receives, aggregates, and displays information from CDM project tools at the agency or Federal level.
Enterprise Operations Function	Responsible for providing server and mainframe computing services for all IRS business entities and taxpayers.
Whitelist	A list of known and trusted applications that can execute on a system.

[1] Pub. L. No. 113-283, 128 Stat. 3073. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

February 21, 2020

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Acting, Chief Information Officer

SUBJECT: Draft Audit Report – The Continuous Diagnostics and Mitigation Project Effectiveness Would be Improved by Better Performance Metrics and Tools Data (Audit # 201920003) (e-trak #2020-19376)

Thank you for the opportunity to review your draft audit report and to discuss draft report observations with the Cybersecurity Continuous Diagnostics and Mitigation (CDM) project team.

CDM is an important Federal program with the goal of improving capabilities to manage risk to computer systems and networks. IRS has made significant progress in implementing the Phase 1 capabilities to manage devices connected to the computer network working with our partners across Treasury and the Department of Homeland Security. We are encouraged by your acknowledgement of the progress we have made and will continue the work to meet IRS, Departmental and DHS goals. We will incorporate your recommendations into our processes moving forward.

We are committed to continuously improving IRS cybersecurity capabilities and processes. The continued support, assistance, and guidance your team provides is very valuable to us in this regard. Our corrective action plan for the recommendations is attached. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Jamie Plummer at (704) 299-7339.

Attachment

Attachment

Draft Audit Report - The Continuous Diagnostics and Mitigation Project Effectiveness Would be Improved By Better Performance Metrics and Tools Data (Audit #201920003)

Recommendation 1: The Chief Information Officer should continue the development and implementation of a data consistency and quality plan, and performance metrics to allow management to readily monitor CDM project status and progress.

CORRECTIVE ACTION #1: We agree with this recommendation. The IRS will finalize a data consistency and quality plan and establish performance metrics that will allow management to monitor progress.

IMPLEMENTATION DATE: September 15, 2020

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

Recommendation 2: The Chief Information Officer should continue collaboration with the segmented network administrators to obtain complete and accurate data for CDM.

CORRECTIVE ACTION #2: We agree with this recommendation. Since the audit review, the IRS has completed work to implement the endpoint management sensor tool in all segmented networks. We are currently monitoring to ensure the sensor tool obtains complete and accurate data.

IMPLEMENTATION DATE: June 15, 2020

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

Recommendation 3: The Chief Information Officer should complete the installation, configuration, and testing of sensor tools to ensure the accuracy of data transmitted to the Department of Treasury dashboard.

CORRECTIVE ACTION #3: We agree with this recommendation. The IRS will complete the installation, configuration and testing of the CDM sensor tools to ensure accuracy of data transmitted to the Department of Treasury dashboard.

IMPLEMENTATION DATE: September 15, 2020

Attachment

Draft Audit Report - The Continuous Diagnostics and Mitigation Project Effectiveness Would be Improved By Better Performance Metrics and Tools Data (Audit #201920003)

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.