TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Vulnerability Disclosure Policy Has Been Implemented; However, Actions Are Needed to Improve the Program

September 4, 2024

Report Number: 2024-200-046

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

HIGHLIGHTS: The Vulnerability Disclosure Policy Has Been Implemented; However, Actions Are Needed to Improve the Program

Final Audit Report issued on September 4, 2024 **Report Number 2024-200-046**

Why TIGTA Did This Audit

In September 2020, the Office of Management and Budget issued Memorandum M-20-32 requiring Federal agencies to obtain and manage their vulnerability research programs. In support of this memorandum, the Department of Homeland Security issued Binding Operational Directive 20-01, requiring each agency to develop and publish a Vulnerability Disclosure Policy (VDP) and maintain supporting handling procedures.

The VDPs enhance the resiliency of the Government's online services by encouraging meaningful collaboration between Federal agencies and the public. They make it easier for the public to know where to send a report, what types of testing are authorized for which systems, and what communication to expect.

This audit was initiated to determine whether the IRS has effectively implemented its VDP Program.

Impact on Tax Administration

A VDP is an essential element of an effective enterprise vulnerability management program and critical to the security of Internet-accessible Federal information systems. With a clear VDP in place, the IRS could clearly notify the public where to report vulnerabilities and set an expectation for communications regarding timely remediation. The primary purpose of fixing vulnerabilities is to protect people and maintain or enhance their safety, security, and privacy.

What TIGTA Found

In May 2022, the IRS published a VDP on its public website. However, the VDP was not published within 180 calendar days as required by Federal requirements and did not have an origination date or a version history.

IRS Vulnerability Disclosure Program Standard Operating Procedures were issued in February 2022, which was one year after the due date. In addition, the Standard Operating Procedures were missing required items based on Federal requirements. Missing required items included communication with the public (also called reporters), acknowledgement to the reporters, notification of the outcome to the reporter, and making vulnerability reports available to system owners within 48 hours of submission.

The IRS contractor was not communicating potential vulnerabilities identified to the IRS. In addition, 13 (8 percent) of the 163 submissions of potential vulnerabilities were not processed timely by the contractor.

8 percent
of the submissions for potential vulnerabilities were not processed timely by the contractor.

The IRS stated that these 13 submissions did not pose a risk to the IRS. The remaining 150 (92 percent) of the 163 potential vulnerabilities were processed timely.

Furthermore, the Department of Homeland Security required 10 metrics that the IRS did not report externally as required. These 10 metrics were collected; however, the IRS did not report these metrics to the Department of the Treasury (hereafter referred to as the Treasury Department). As such, the Treasury Department did not report these metrics to CyberScope.

The IRS improved its Vulnerability Disclosure Program by taking the following management actions during our review: 1) the VDP published on the IRS's public website was updated to include an issuance date and version history, and 2) the Standard Operating Procedures were updated to include Federal requirements.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer: 1) implement procedures to periodically review the tracking logs of submissions received by the contractor to ensure timely processing and 2) coordinate with the Treasury Department so that the required metrics are submitted quarterly.

The IRS agreed with both recommendations. The Chief Information Officer plans to implement procedures to periodically review the tracking logs of submissions to ensure timely processing and ensure ongoing coordination with the Treasury Department so that the required metrics are collected and submitted quarterly.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 4, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Danny R. Verneuille
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Vulnerability Disclosure Policy Has Been Implemented; However, Actions Are Needed to Improve the Program (Audit No.: 202320021)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has effectively implemented its Vulnerability Disclosure Policy Program. This review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenge of *Protection of Taxpayer Data and IRS Resources.*

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

Table of Contents

Background ..... Page 1

Results of Review ..... Page 3

The IRS Made Improvements to Its Vulnerability Disclosure Policy After Being Posted on Its Website ..... Page 3

Vulnerability Disclosure Program Standard Operating Procedures Were Lacking Required Elements ..... Page 3

Submissions of Potential Vulnerabilities Were Not Addressed Within the Required Timelines ..... Page 4

Recommendation 1: ..... Page 6

Required Metrics Are Not Being Reported Externally As Required ..... Page 6

Recommendation 2: ..... Page 7

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 8

Appendix II – Outcome Measures ..... Page 10

Appendix III – Management's Response to the Draft Report ..... Page 11

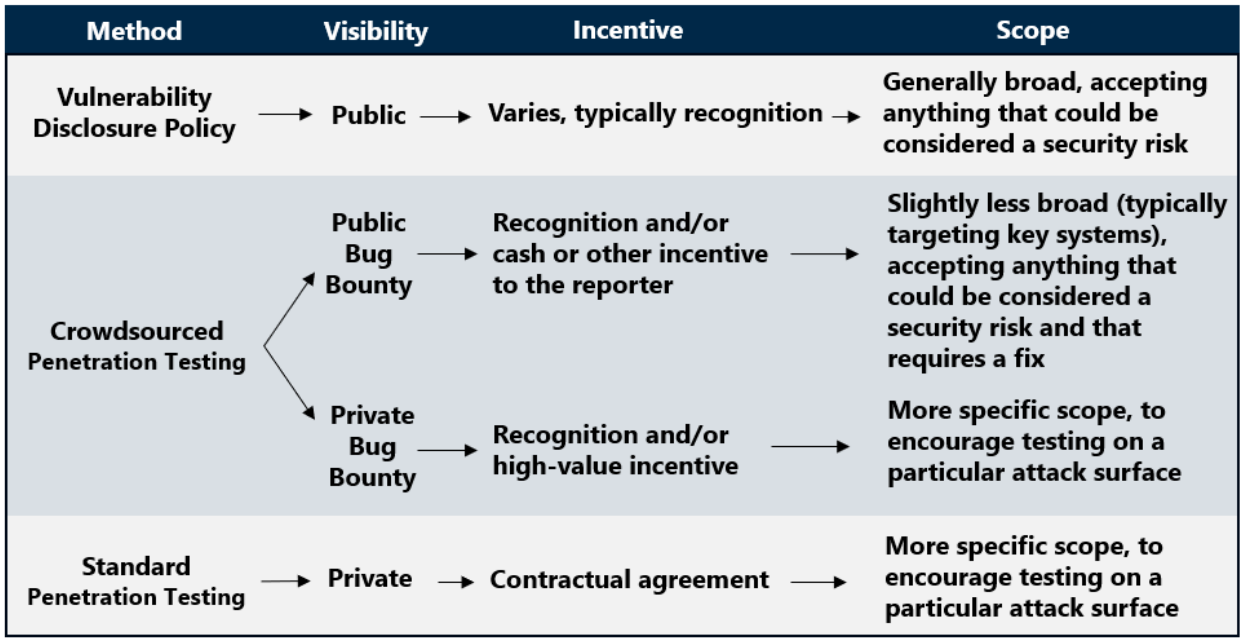
Appendix IV – Glossary of Terms ..... Page 13

Appendix V – Abbreviations ..... Page 14

Background

In September 2020, the Office of Management and Budget (OMB) issued Memorandum M-20-32, requiring Federal agencies to obtain and manage their vulnerability research programs.[1] Figure 1 depicts the vulnerability research program methods.

Figure 1: Vulnerability Research Program Methods



Source: OMB, Memorandum M-20-32.

In support of this memorandum, the Department of Homeland Security (DHS) issued Binding Operational Directive (BOD) 20-01, requiring each agency to develop and publish a Vulnerability Disclosure Policy (VDP) and maintain supporting handling procedures.[2] According to the DHS, the VDPs enhance the resiliency of the Government's online services by encouraging meaningful collaboration between Federal agencies and the public. They make it easier for the public to know where to send a report, what types of testing are authorized for which systems, and what communication to expect. When agencies integrate vulnerability reporting into their existing cybersecurity risk management activities, they can weigh and address a wider array of concerns. This helps safeguard the information the public has entrusted to the Government and gives Federal cybersecurity teams more data to protect their agencies.

Furthermore, a VDP is an essential element of an effective enterprise vulnerability management program and critical to the security of Internet-accessible Federal information systems. The primary purpose of fixing vulnerabilities is protecting people, and maintaining or enhancing their safety, security, and privacy. Since Fiscal Year 2021, the Internal Revenue Service (IRS) has used contracted services to manage its VDP web page and triage any vulnerabilities reported. These contractors also manage the penetration testing solution for the IRS's various areas.

[1] OMB, Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation* (Sept. 2020). See Appendix IV for a glossary of terms.

[2] DHS, BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy* (Sept. 2020).

According to the OMB, the VDPs and bug bounties are two types of coordinated VDP programs that Federal agencies are currently incorporating into their security efforts. A VDP is a publicly available statement that defines terms and methods preferred by the authoring organization so that a member of the public may report a vulnerability within the scope defined by an organization. Bug bounty programs differ from the VDPs by offering compensation based on established parameters to security researchers who report the vulnerabilities. The directive does not require agencies to establish bug bounty programs; therefore, the IRS has not established one.

According to Executive Order 13800, the President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises.[3]

> *Cybersecurity risk management comprises the full range of activities undertaken to protect information technology and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting information technology and data, and to mitigate the impact of, respond to, and recover from incidents. Information sharing facilitates and supports all of these activities. Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of information technology and data.*

DHS, BOD 20-01, applies to the 102 Federal Civilian Executive Branch agencies listed on the DHS's Cybersecurity and Infrastructure Security Agency's (CISA) website. The Department of the Treasury's (hereafter referred to as the Treasury Department) Vulnerability Disclosure Program achieved full compliance with DHS, BOD 20-01, on August 31, 2022, two days before the deadline. As of March 2024, it is the Treasury Department's position that the IRS is compliant with DHS, BOD 20-01, under the umbrella of the Treasury Department's Vulnerability Disclosure Program.

The Treasury Department's Vulnerability Disclosure Program provides a single point of entry for security researchers (ethical hackers) to submit security vulnerabilities regarding Internet-accessible Treasury Department systems to mitigate vulnerabilities before potential exploitation by a malicious actor. Although communication ensued between the Treasury Department and the IRS regarding the VDP deadlines, there was confusion in implementing the VDP website. Treasury Department personnel stated in January 2022 that the IRS could leverage its VDP website so the public could report any potential vulnerabilities to the Treasury Department. In February 2022, the IRS had a contractor create its own IRS VDP website. This website is in addition to the Treasury Department's Vulnerability Disclosure Program. Both the Treasury Department's Vulnerability Disclosure Program and the IRS's VDP were published in May 2022, with the goal of ensuring compliance with DHS, BOD 20-01.

With a clear VDP in place that addresses the above considerations, agencies could clearly notify the public (also called reporters) where to report vulnerabilities and set an expectation of communications with vulnerability reporters regarding timely remediation.

[3] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017).

Results of Review

The IRS Made Improvements to Its Vulnerability Disclosure Policy After Being Posted on Its Website

The IRS developed a VDP and published it on its public website on May 23, 2022. However, the website was not published timely, and we determined that the IRS did not include two of the required elements in its VDP. Specifically, OMB, Memorandum M-20-32, and DHS, BOD 20-01, required the IRS to publish a VDP by March 2021 and required the VDP posted on its website to provide an origination date and a version history.

The IRS stated that it did not initially stand up a VDP Program because the Treasury Department was standing up a departmental-wide program for all bureaus. The IRS also stated that the issuance date was not included on its VDP because it did not have any changes or updates to the VDP. However, we determined that the IRS's omissions were not in compliance with Federal guidance.

A VDP facilitates good-faith security research, commits the agency to respond to vulnerability notifications, and creates an environment where researchers are more comfortable disclosing vulnerabilities. Without a defined policy, researchers may be more reluctant to disclose suspected vulnerabilities, whether for legal, logistical, or accessibility reasons. Likewise, if a policy is not defined, there are no governing mechanisms to ensure that disclosures are coordinated, leading to scenarios where vulnerabilities are made public prior to the impacted agency being made aware of or able to remediate them. In addition, without the issuance date of the VDP, the public cannot determine if the policy is up to date.

Management Action: After we informed IRS management of our results, they stated that the VDP web page was updated on January 11, 2024, to include an origination date and version history. We subsequently verified that the IRS's VDP web page was updated with the origination date and a version history.

Vulnerability Disclosure Program Standard Operating Procedures Were Lacking Required Elements

We reviewed the IRS's Vulnerability Disclosure Program Standard Operating Procedures (SOP) and determined that the SOP were not developed by March 1, 2021, as required by DHS, BOD 20-01. The IRS issued the SOP on February 28, 2022, which was one year after the due date.

In addition, the DHS lists specific requirements for establishing a VDP. For example, within 180 calendar days after the issuance of DHS, BOD 20-01, the IRS was required to develop or update vulnerability disclosure handling procedures to support implementation of the VDP. The guidance also provides required items to be included in the procedures. We reviewed the SOP and determined that several required items were missing. Specifically,

- Handling of reports for systems and services that are out-of-scope.
- How communication with the reporter and other stakeholders, *e.g.*, service providers, the CISA, will occur.

- Acknowledgement to the reporter (where known) that their report was received. The CISA recommends no more than three business days from the receipt of the report.
- Resolution of vulnerabilities, including notification of the outcome to the reporter. The CISA recommends no more than 90 days from the receipt of the report.
- Initial assessment, *i.e.*, determining whether disclosed vulnerabilities are valid, including impact evaluation. The CISA recommends this assessment take no more than seven days from the receipt of the report.
- Any current or past impact of the reported vulnerabilities (not including impact from those who complied with the agency VDP) will be assessed and treated as an incident or breach, as applicable.

Also, the OMB requires Federal agencies to streamline communication and collaboration by ensuring that vulnerability reports are available to system owners within 48 hours of submission and establishing a channel for system owners to communicate with vulnerability reporters, as appropriate. This requirement was also missing from the SOP.

IRS personnel stated that the missing procedures only needed to be listed if IRS personnel were fulfilling them. We disagree with the IRS's statement. Without clear procedures, IRS employees and contractors will be unsure of their roles and responsibilities. IRS personnel stated that the contractor fulfilled: the handling of out-of-scope reports; communication with reporters; acknowledgement to the reporters; and notification of the outcome to the reporters. In addition, IRS personnel failed to include the number of days that the initial assessment should take in the SOP because their turnaround time for this assessment was shorter than the CISA recommendation of seven days. However, we determined that the SOP should include the number of days allowed for assessment.

Lastly, the IRS stated its SOP describes how any current or past reported vulnerabilities will be assessed and treated as an incident/breach. However, we did not identify any verbiage on how it would assess or treat an incident or breach. If the SOP is missing the required vulnerability disclosure handling procedures, the VDP Program cannot establish processes and procedures to appropriately handle reported vulnerabilities and cannot set target timelines and track activities.

Management Action: After we informed management of our results, the IRS finalized its SOP on March 6, 2024, to include handling of out-of-scope reports, communication with reporters, acknowledgement to the reporters, initial assessment to take no more than seven days, how incidents or breaches are assessed and treated, notification of the outcome to the reporter, and vulnerability reports are available to system owners within 48 hours of submission. We subsequently verified that the missing requirements we presented were updated in its SOP.

Submissions of Potential Vulnerabilities Were Not Addressed Within the Required Timelines

The IRS uses contractors to triage and validate the submissions of potential vulnerabilities from reporters. We determined that the IRS contractor was not communicating submissions of potential vulnerabilities identified by the reporters within 48 hours to the IRS. In addition, as shown in Figure 2, we reviewed contractor tracking logs from March 21, 2022, through September 24, 2023, and found that 13 (8 percent) of the 163 submissions of potential

vulnerabilities were not processed timely by the contractor. The IRS stated that these 13 submissions did not pose a risk to the IRS. The remaining 150 (92 percent) of the 163 potential vulnerabilities were processed timely.

Figure 2: Potential Vulnerability Submissions Not Processed Timely by the Contractor

Source: Treasury Inspector General for Tax Administration's analysis of the contractor's tracking logs.

According to the OMB, Federal agencies shall ensure that vulnerability reports are available to system owners within 48 hours of submission and establish a channel for system owners to communicate with vulnerability reporters, as appropriate.

In addition, DHS, BOD 20-01, contains the requirements for establishing target timelines for handling submissions. Specifically, the guidance describes how vulnerability reports will be tracked to resolution, sets target timelines, and requires tracking to include acknowledgement to the reporter that their report was received, initial assessment, and resolution of vulnerabilities, which includes notification of the outcome to the reporter. Specifically,

- Acknowledgement to the reporter (where known) that their report was received (three business days).
- Initial assessment, *i.e.*, determining whether disclosed vulnerabilities are valid, including impact evaluation within seven days.
- Resolution of vulnerabilities, including notification of the outcome to the reporter in 90 days.

Furthermore, we identified eight of the 163 submissions with inactivity for over 100 days and brought them to the contractor and the IRS's attention. After reviewing the eight submissions, the contractor stated that they were all resolved and therefore should have been closed within the seven days of validation. Figure 3 shows the reasons why the deadlines were missed for the remaining five (3 percent) of the 163 potential vulnerabilities.

Figure 3: Reasons Why Five Submissions Did Not Meet Timelines

Number of Submissions	Deadline Missed by	Reasons
1	Not acknowledged in 3 business days and was not determined to be valid within 7 days.	The contractor took longer to triage and resolve the issue.
1	Not valid within 7 days.	The contractor took longer to triage and resolve the issue.
2	Not valid within 7 days.	Additional information was requested; however, none was received by the submitter.
1	Not valid within 7 days.	Submitter re-opened the ticket.

Source: Treasury Inspector General for Tax Administration's analysis of the contractor's tracking logs.

The IRS did not have sufficient oversight of submissions received by the contractor, resulting in IRS personnel being unaware of the untimely responses. If a reporter receives no response from the agency or gets a response deemed unhelpful, they may assume the agency will not fix the vulnerability. This may prompt the reporter to resort to making the vulnerabilities public prior to the IRS being made aware of or able to remediate them. The reporter may default to this approach in the future.

Recommendation 1: The Chief Information Officer should implement procedures to periodically review the tracking logs of submissions received by the contractor to ensure timely processing.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will implement procedures to periodically review the tracking logs of submissions received by the contractor to ensure timely processing.

Required Metrics Are Not Being Reported Externally As Required

The IRS did not report the 10 metrics required by DHS, BOD 20-01, to the Treasury Department, and the Treasury Department did not report the IRS's metrics through CyberScope from May 2021 through December 2023.

DHS, BOD 20-01, requires agencies to report on the 10 metrics after 270 calendar days (by May 30, 2021) following the issuance of this directive, and within the first Federal Information Security Modernization Act of 2014 reporting cycle and quarterly thereafter, through CyberScope.[4] Figure 4 lists the 10 metrics required by the DHS to be reported through CyberScope.

[4] 44 U.S.C. §§ 3551-3558 (2018).

Figure 4: 10 Metrics Required to Be Reported Through CyberScope

10 Metrics Required by DHS, BOD 20-01	
1.	The number of vulnerability disclosure reports.
2.	The number of reported vulnerabilities determined to be valid, *e.g.,* in scope and not false-positive.
3.	The number of currently open and valid reported vulnerabilities.
4.	The median age (in days from receipt of the report) of currently open and valid reported vulnerabilities.
5.	The number of currently open and valid reported vulnerabilities older than 90 days from the receipt of the report.
6.	The number of all reports older than 90 days by risk/priority level.
7.	The median age of reports older than 90 days.
8.	The median time to validate a submitted report.
9.	The median time to remediate/mitigate a valid report.
10.	The median time to initially respond to the reporter.

Source: DHS, BOD 20-01.

During our review, we determined that the IRS contractor collected the 10 metrics for each quarter from April 2022 through October 2023. According to our interviews with IRS and Treasury Department personnel, the Treasury Department was instructed by the CISA not to report the metrics through CyberScope. The Treasury Department in turn informed the IRS not to report the metrics. As such, the IRS did not report these metrics based on the instruction it received from the Treasury Department.

On January 11, 2024, we received additional information from the IRS and the Treasury Department indicating that the CISA instructed the Treasury Department to report the 10 metrics through CyberScope starting with the second quarter of Fiscal Year 2023. The Treasury Department reported through CyberScope what was collected from the Treasury Department's Vulnerability Disclosure Program; however, it did not request information on the 10 metrics from the IRS. Therefore, the data reported through CyberScope did not include the data collected by contractors responsible for collecting the metrics for the IRS.

The CISA leads the national effort to understand, manage, and reduce risk to the IRS's cyber and physical infrastructure. By not reporting IRS metrics via CyberScope, the CISA cannot monitor the IRS's compliance with this directive and help reduce risk to the IRS cyber physical infrastructure, and the efficiency and transparency of the Vulnerability Disclosure Program will be in question.

Recommendation 2: The Chief Information Officer should ensure ongoing coordination with the Treasury Department so that the required metrics are collected by the IRS and submitted appropriately, from the third quarter of Fiscal Year 2024, and quarterly thereafter.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will ensure ongoing coordination with the Treasury Department so that the required metrics are collected and submitted appropriately, from the third quarter of Fiscal Year 2024, and quarterly thereafter.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS has effectively implemented its VDP Program. To accomplish our objective, we:

- Determined whether the IRS's VDP is in compliance with both DHS, BOD 20-01, and OMB, Memorandum M-20-32, by comparing the Federal requirements to the VDP.
- Determined whether the IRS Vulnerability Disclosure Program SOP had the necessary updates to address DHS and OMB requirements by comparing the IRS Vulnerability Disclosure Program SOP to DHS, BOD 20-01, and OMB, Memorandum M-20-32, requirements.
- Determined whether the IRS effectively implemented the requirements of the Vulnerability Disclosure Program by reviewing the submission reports from March 21, 2022, through September 24, 2023, and identifying any submissions that were not timely resolved, were not reported to the IRS or overlooked for evaluation or were miscategorized by the contractor.
- Determined whether the IRS was reporting the required metrics to the Treasury Department, and if it was in compliance with DHS, BOD 20-01, by interviewing IRS and Treasury Department personnel.

Performance of This Review

This review was performed with information obtained from the IRS Cybersecurity, Security Risk Management Office located in Martinsburg, West Virgina, during the period August 2023 through June 2024. 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 Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Midori Ohno, Audit Manager; Cari Fogle, Lead Auditor; Charles Ekunwe, Senior Auditor; Ruth Chen, Auditor; and Laura Christoffersen, Information Technology Specialist (Data Analytics) – Applied Research and Technology.

Data Validation Methodology

We performed tests to assess the reliability of the submission data obtained from the contractor. We evaluated the data by 1) interviewing the contractor and IRS personnel knowledgeable about the data; 2) ensuring that the information was legible and contained alphanumeric characters; 3) reviewing required data elements; and 4) reviewing the data to detect obvious errors, duplicate values, and unexpected missing data. We determined that the data were sufficiently reliable for purposes of this report.

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: IRS Vulnerability Disclosure Program SOP; OMB, Memorandum M-20-32; DHS, BOD 20-01; and Executive Order 13800. We evaluated these controls by interviewing IRS management and staff, reviewing data and artifacts from applicable systems, and reviewing program documentation.

Appendix II

Outcome Measures

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

Type and Value of Outcome Measure:

- Reliability of Information: Potential; Eight potential vulnerability submissions were not disclosed to the IRS (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We reviewed contractor tracking logs from March 21, 2022, through September 24, 2023. We identified eight of the 163 submissions with inactivity for over 100 days and brought them to the contractor and the IRS's attention.

Type and Value of Outcome Measure:

- Reliability of Information: Potential; 10 metrics provided in DHS, BOD 20-01, were not reported to the Treasury Department from May 2021 through December 2023 (see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

We determined that IRS contractors collected the 10 metrics required by DHS, BOD 20-01; however, they were not reported to the Treasury Department by the IRS. As such, the Treasury Department did not report IRS metrics to CyberScope.

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

August 1, 2024

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Rajiv Uppal,
Chief Information Officer

Rajiv K. Uppal
Digitally signed by Rajiv K. Uppal
Date: 2024.08.01 13:52:44 -04'00'

SUBJECT: Draft Audit Report – The Vulnerability Disclosure Policy Has Been Implemented; However, Actions Are Needed to Improve the Program (Audit #202320021)

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. In May 2022, the IRS established a Vulnerability Disclosure Program in addition to the Treasury program to allow security researchers the additional avenues to report security vulnerabilities in IRS externally facing applications. The IRS has already made positive progress in addressing the recommendations called out in the Report.

We agree with the Treasury Inspector general for Tax Administration's two recommendations, and our corrective action plan is attached. 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 Zobaida Sharafeldin, Director, Security Risk Management, at (703) 244-2180.

Attachment

Recommendations

RECOMMENDATION 1: The Chief Information Officer should implement procedures to periodically review the tracking logs of submissions received by the contractor to ensure timely processing.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will implement procedures to periodically review the tracking logs of submissions received by the contractor to ensure timely processing.

IMPLEMENTATION DATE: February 15, 2025

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

RECOMMENDATION 2: The Chief Information Officer should ensure that ongoing coordination with the Treasury Department so that the required metrics are collected by the IRS and submitted appropriately, from the third quarter of Fiscal Year 2024, and quarterly thereafter.

CORRECTIVE ACTION 2: The IRS agrees with this Recommendation. The Chief Information Officer will ensure that ongoing coordination with the Treasury Department so that the required metrics are collected by the IRS and submitted appropriately, from the third quarter of Fiscal Year 2024, and quarterly thereafter.

IMPLEMENTATION DATE: May 15, 2025

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

Appendix IV

Glossary of Terms

Term	Definition
Binding Operational Directive	A compulsory direction to Federal, Executive Branch, departments, and agencies for purposes of safeguarding Federal information and information systems. CISA within the DHS is authorized to develop and oversee the implementation of DHS BODs. Federal agencies are required to comply with directives except for statutorily defined national security systems.
CyberScope	Launched by the OMB to provide for secure and efficient Federal Information Security Modernization Act of 2014 reporting by Federal agencies. Agencies use it to report a wide variety of information. CyberScope also provides for meaningful analysis of agency security postures.
Cybersecurity and Infrastructure Security Agency	Develops and oversees the implementation of "binding operational directives" and "emergency directives," which require action on the part of certain Federal agencies in the civilian Executive Branch.
Department of the Treasury	The Federal agency that manages Federal finances by collecting taxes and paying bills and by managing currency, Government accounts, and public debt. The Department also enforces finance and tax laws.
Federal Information Security Modernization Act of 2014	An amendment to the Federal Information Security Management Act of 2002 that allows for further reform to Federal information security. This bill amends Chapter 35 of Title 44 of the United States Code. The original statute (Federal Information Security Management Act of 2002) requires agencies to assess risks to information systems and provide information security protections commensurate with the risks, integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to the OMB.
Office of Management and Budget	Serves the President of the United States in overseeing the implementation of their vision across the Executive Branch. The OMB's mission is to assist the President in meeting policy, budget, management, and regulatory objectives and to fulfill the agency's statutory responsibilities.
Standard Operating Procedures	A set of step-by-step instructions compiled by an organization to help workers carry out complex routine operations.
Vulnerability Disclosure Policy	An essential element of an effective enterprise vulnerability management program and critical to the security of Internet-accessible Federal information systems.

Appendix V

Abbreviations

BOD	Binding Operational Directive
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
IRS	Internal Revenue Service
OMB	Office of Management and Budget
SOP	Standard Operating Procedures
VDP	Vulnerability Disclosure Policy

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.