TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls

September 30, 2022

Report Number: 2022-20-065

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

HIGHLIGHTS: The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls

Final Audit Report issued on September 30, 2022 **Report Number 2022-20-065**

Why TIGTA Did This Audit

A database is a data structure that stores organized information. Databases are generally maintained within database management systems and provide users and programmers with a systematic way to create, retrieve, update, and manage data. The IRS databases store sensitive information, including Federal tax information (*i.e.*, taxpayer data) and Personally Identifiable Information.

TIGTA identified issues with database vulnerability scanning during our prior Federal Information Security Modernization Act reviews. This audit was initiated to determine whether the IRS is adequately assessing the risks to its databases when performing vulnerability scans and installing timely patches.

Impact on Tax Administration

Since taxpayer data is stored on the IRS's databases, vulnerability scanning is required and necessary to determine if vulnerabilities exist on the systems. Without scanning, the IRS does not know what vulnerabilities exist on its databases. Therefore, taxpayer information could be at risk of exploitation, especially if the system has critical vulnerabilities that the IRS has not detected and mitigated.

What TIGTA Found

In Calendar Year 2018, the IRS made an executive decision, without following proper procedures or policy, to reduce vulnerability scanning of databases, resulting in only [redacted] being scanned monthly in Fiscal Year 2020. The IRS allowed the noncompliant scanning strategy to continue until TIGTA started its review in Fiscal Year 2021. During the course of our audit, by March 2022, the IRS increased the scope of its database vulnerability scanning [redacted] systems. Still, the IRS does not perform database vulnerability scanning [redacted] systems. Therefore, the IRS is not fully aware of the risks associated with those mainframes.

Of the 27 Federal Information Security Modernization Act cloud systems, the IRS is only performing privileged vulnerability scans on [redacted] and inconsistently received or was unable to review vulnerability details from cloud service providers on the others. The IRS also does not receive monthly vulnerability reports for [redacted]

In addition, the IRS is not timely patching database vulnerabilities. As of March 2022, the IRS has not patched a total of [redacted] of [redacted] database instances. Our analysis showed that Microsoft database patches remained uninstalled from [redacted] calendar days and that Oracle database patches remained uninstalled from [redacted] calendar days.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that: (1) [redacted] is performed on all International Business Machines mainframe databases; (2) the Internal Revenue Manual is updated to reflect the *Mainframe Product Security Requirements Guide;* (3) the Information System Security Officers have a formal process for recommending approval or disapproval of policy deviations; (4) privileged vulnerability scans are performed on cloud systems when possible; (5) the IRS provides oversight to cloud service providers and obtains detailed scan results; (6) Plans of Action and Milestones are created for unresolved issues from database vulnerability scans; and (7) databases are patched or upgraded to the latest version or risk acceptance is appropriately documented.

The IRS agreed with all seven recommendations. The IRS plans to (1) [redacted] (2) address the inconsistency regarding the title and applicability of the Security Requirements Guide, (3) review the current formal process for recommending approval or disapproval of policy deviations, (4) ensure that privileged vulnerability scans are performed on the cloud systems; (5) ensure that oversight is provided to cloud service providers; (6) ensure that corrective actions are documented for unresolved aged database vulnerabilities scans; and (7) ensure that databases are patched or upgraded to the latest version or risk acceptance is properly documented.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 30, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls (Audit # 202120003)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) is adequately assessing the risks to its databases when performing vulnerability scans and installing timely patches. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS Resources*.

Management's complete response to the draft report is included as Appendix IV. In its response, the IRS takes issue with our presentation of findings, in one example stating that "the audit team relied on a tool that fails to distinguish between security and non-security vulnerabilities" for determining whether patching was completed timely. However, the IRS provided this specific report when we requested a report of any open critical database vulnerabilities. Further, the IRS disagrees with our stance on updating databases. Our stance that databases should be updated to the latest available version is in alignment with Oracle and Microsoft best practices.

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

Background

A database is a data structure that stores organized information. Hackers find and target vulnerabilities in software, including database management software. Databases are generally maintained within database management systems and provide users and programmers with a systematic way to create, retrieve, update, and manage data. The database management system is useful for providing a centralized view of data that can be accessed by multiple users from multiple locations in a controlled and organized manner.

Within the database management environment, the major types of risk activities include:

- Misuse: Failure to maintain access rights to the database could lead to abuse of privileged access, such as unauthorized disclosures, inserts, updates, or deletions.
- Malicious action: Failure to maintain a secure, logical setup of the database could lead to data theft or a denial-of-service attack.

The Internal Revenue Manual (IRM)[1] establishes the minimum baseline security policy and requirements for all Internal Revenue Service (IRS) Information Technology organization assets to:

- Protect IRS critical infrastructure and assets against attacks that exploit them.
- Prevent unauthorized access to IRS assets.
- Enable IRS information technology computing environments that meet the security requirements of this policy and support the business needs of the organization.

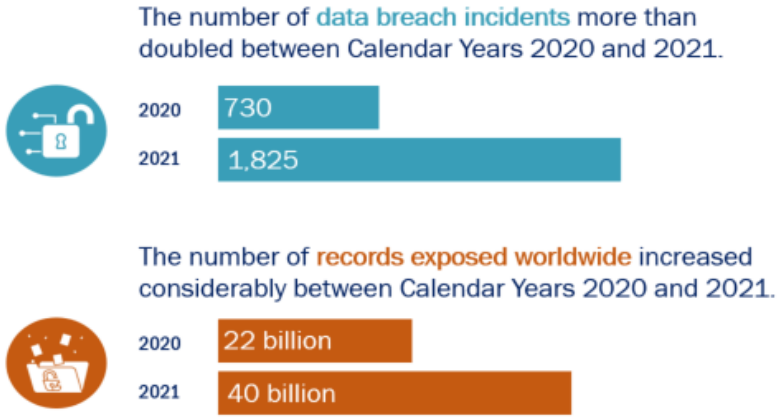
According to research by Tenable,® due to 1,825 data breach incidents publicly disclosed between November 2020 and October 2021, at least 40 billion records were exposed worldwide in Calendar Year 2021.[2] This is a considerable increase over the same period in Calendar Year 2020, which saw 730 publicly disclosed events[3] with just over 22 billion records exposed. By understanding threat actor behavior, organizations can effectively prioritize security efforts to disrupt attack paths and protect critical systems and assets. The Tenable research analysis found that many events are readily mitigated by patching legacy vulnerabilities and addressing misconfigurations to help limit attack paths.

[1] IRM 10.8.21, *Information Technology (IT) Security, Database Security Policy* (Sept. 2021).

[2] Help Net Security, *Exposed Records Exceeded 40 Billion in 2021* (Jan. 2022). This research cited Tenable Network Security, which is in the business of cybersecurity.

[3] See Appendix V for a glossary of terms.

Figure 1: Comparison of Calendar Years 2020 and 2021 Data Breaches and Records Exposed



Source: Tenable® research analysis.

Database security refers to the range of tools, controls, and measures designed to establish and preserve database confidentiality, integrity, and availability. Confidentiality is the element that is compromised in most data breaches. Database security must address and protect the data in the database, the database management system, any associated applications, the physical and virtual database servers and the underlying hardware, and the computing and network infrastructure used to access the database.

In the IRS, the following individuals and offices are responsible for database security:

- The Cybersecurity function's Security Risk Management office ensures compliance with Federal statutory, legislative, and regulatory requirements to assure the confidentiality, integrity, and availability of IRS electronic systems, services, and data.
- Security Risk Management's Enterprise Database Scanning office is responsible for database scanning enterprise-wide in support of the security assessment and authorization, the annual security control assessment, the enterprise life cycle, and designated Filing Season Critical systems. The Enterprise Database Scanning office focuses on database vulnerability scanning using a commercial off-the-shelf database vulnerability scanning tool. The tool is able to identify exposures such as missing patches, weak passwords, unauthorized changes, and misconfigured privileges. The tool also detects behavioral vulnerabilities such as account sharing, excessive administrative logins, and unusual after-hours activity. The IRS is required to perform database vulnerability scans monthly, but it performs the scans twice a month.
- The Authorizing Official is the accrediting official with the authority to assume responsibility for operating a system at an acceptable level of risk.
- The Information System Security Officer (ISSO) reports the control impact assessment results to the Authorizing Official and/or the owner of the General Support System/application system to address any security concerns.
- The business unit's Security Program Management Office is responsible for implementing and managing IRS information technology security policies, procedures, and practices within their respective business units.

- The Information Technology organization and business units are responsible for the operations and maintenance of the IRS systems and their databases to include implementation of security controls around the mainframes and their databases.

The IRS databases store sensitive information, including Federal tax information (*i.e.,* taxpayer data) and Personally Identifiable Information. Vulnerability scanning of the databases is required and necessary to determine if vulnerabilities exist on the system. We previously[4] made recommendations to improve vulnerability scanning and the security of the IRS's databases.

- In Fiscal Year 2011, we recommended that the IRS fully implement its database vulnerability scanning tool. The database vulnerability scanning tool was implemented on March 1, 2016.
- In Fiscal Year 2014, we recommended that processes and procedures be developed to provide direction on how to review and mitigate weaknesses identified by database vulnerability scanning tool's scans run on all databases.

In addition, prior Treasury Inspector General for Tax Administration (TIGTA) Federal Information Security Modernization Act[5] (FISMA) reviews[6] identified database vulnerability scanning issues.

Results of Review

Databases Lack Necessary Vulnerability Scans

The IRS strategically decided to reduce database vulnerability scanning without formally documenting its deviation from policy

While the IRS agreed with previous TIGTA recommendations and completed the planned corrective actions to perform database vulnerability scanning enterprise-wide by 2016, the IRS subsequently reduced the monthly database vulnerability scanning. [redacted]

[4] Treasury Inspector General for Tax Administration (TIGTA), Report No. 2011-20-099, *The Mainframe Databases Reviewed Met Security Requirements; However, Automated Scans Were Not Being Performed* (Sept. 2011), and TIGTA, Report No. 2014-23-072, *Affordable Care Act: Improvements Are Needed to Strengthen Security and Testing Controls for the Affordable Care Act Information Returns Project* (Sept. 2014).

[5] Pub. L. No. 113-283.

[6] TIGTA, Report No. 2018-20-082, *TIGTA – Federal Information Security Modernization Act Evaluation Report for Fiscal Year 2018* (Sept. 2018); TIGTA, Report No. 2019-20-082, *Fiscal Year 2019 Evaluation of the IRS's Cybersecurity Program Against the Federal Information Security Modernization Act* (Sept. 2019); TIGTA, Report No. 2020-20-073, *Fiscal Year 2020 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act* (Sept. 2020); and TIGTA, Report No. 2021-20-072, *Fiscal Year 2021 IRS Federal Information Security Modernization Act* (Sept. 2021).

[redacted]

[redacted]

After we started our review in November 2020, the IRS officially announced the reduction in database vulnerability scanning, three years after it had actually reduced database vulnerability scanning. Although the strategy is outlined in a memorandum signed by an executive in February 2021, the IRS never changed its formal written policy related to database vulnerability scans. The IRS's written policy remained in compliance with National Institute of Standards and Technology guidance and a Department of the Treasury Directive.[7] However, the new strategy to not perform privileged database vulnerability scanning on all the system databases, including the mainframe applications that are considered High Value Asset systems, was not compliant with the IRS's formal written policy or Federal guidance.

National Institute of Standards and Technology guidance states that agencies should monitor and scan for vulnerabilities in the system and hosted applications at an organizationally defined frequency and when new vulnerabilities potentially affecting the system are identified and reported. In addition, the guidance states that organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities are not overlooked.

According to the IRS, the executive decision was made [redacted] because the IRS could not address the vulnerabilities of all databases in a timely manner. When privileged vulnerability scanning is not performed on all databases, the IRS could have vulnerabilities that are not detected and therefore are unknown to the system owner.

Management Action: During the course of our audit in April 2021, the IRS began increasing database vulnerability scanning. By March 2022, it increased scanning to [redacted] systems. However, the increased scanning capabilities did not include the [redacted]

The IRS has not performed database vulnerability scanning on the International Business Machines (IBM) mainframes since 2018

During Calendar Year 2014, the IRS determined that the database vulnerability scanning tool was not compatible with the IBM Resource Access Control Facility® (RACF) on the mainframes.[8] IBM's RACF for z/OS® enables the protection of mainframe resources by making access control decisions through resource managers. RACF retains information about users, resources, and

[7] National Institute of Standards and Technology, Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* Revision 5 (Sept. 2020), and Department of the Treasury, Treasury Directive Policy 85-01, *Department of the Treasury Information Technology (IT) Security Program Appendix A* (Sept. 2019).

[8] See Appendix III for a timeline.

access authorities in its database. This database determines access to protected mainframe system resources based on the security policy.

During Calendar Year 2015, the IRS began RACF implementation. Although the mainframes are considered a High Value Asset, [redacted] The IRM[9] states the mainframe shall implement privileged access authorization to all information systems and infrastructure components for selected vulnerability scanning activities as defined in the system security documentation. In January 2021, after we started our review, the IRS created a risk-based decision that impacted databases on the IBM mainframes. The risk-based decision describes the following two weaknesses:

- [redacted]
- [redacted]

The IRM states that acceptable reasons for a risk-based decision include:

- Technically not possible.
- Cost prohibitive.
- Operationally not feasible and would cause an undue burden to the system and/or seriously hinder its capability to accomplish its mission.

The IRS stated that mitigation for its [redacted] However, we determined that the justification the IRS used in its risk-based decision[10] was not compliant with the IRM requirements for risk acceptance because it was [redacted]

National Institute of Standards and Technology guidance states that the capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. A commercial database vulnerability scanning component works with the IRS database vulnerability scanning tool, allowing the full scanning of the mainframe databases, including the mainframes installed with RACF. The IRS has known about this component since 2019. [redacted]

[9] IRM 10.8.33, *Information Technology (IT) Security, Mainframe System Security Policy* (Aug. 2022).

[10] The IRS let this risk-based decision expire on March 2, 2022.

In addition, we determined that the risk-based decision regarding [redacted] is misinterpreting the Department of Defense's *Mainframe Product Security Requirements Guide*.[11] The Guide states that the "mainframe product" must implement [redacted] to all information systems and infrastructure components for selected vulnerability scanning activities as defined in the site security plan. We determined the IRM does not fully support the intent of the *Mainframe Product Security Requirements Guide* because the IRM states the "mainframe," while the guide describes the "mainframe product." This discrepancy allows for the interpretation that the requirement is referring to the mainframe rather than a product on the mainframe. The IRM should fully align with the *Mainframe Product Security Requirements Guide*.

Despite the risk-based decision, the National Institute of Standards and Technology Vulnerability Monitoring and Scanning control is still applicable, [redacted]

The Chief Information Officer should ensure that:

Recommendation 1: [redacted] is performed on all IBM mainframe databases.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, [redacted]

Recommendation 2: IRM 10.8.33 is updated to accurately reflect the *Mainframe Product Security Requirements Guide*.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, stated that IRM 10.8.33 accurately reflects the Defense Information Systems Agency Mainframe Product Security Requirements Guide. Security Policy has opened a ticket with the Defense Information Systems Agency to address the inconsistency in their language regarding the title and applicability of the Security Requirements Guide and will update IRM 10.8.33 accordingly.

ISSOs did not recommend approval or disapproval of deviations from policy

[redacted]

[11] Department of Defense, *Mainframe Product Security Requirements Guide, version 1 release 4* (January 24, 2020).

[redacted]

In accordance with Department of the Treasury Directive Publication 85-01, the ISSO shall:

- Ensure that operational security posture consistent with current system security policy is maintained. This includes monitoring compliance with system security policy and providing guidance and recommendations to correct deficiencies.
- Ensure that changes to the system are controlled in accordance with applicable change management policies.
- Ensure that security impacts of proposed changes are evaluated by or reported to officials responsible for change control.
- As the principal advisor to the Authorizing Official, Information System Owner, Senior Agency Information Security Officer, or Chief Information Security Officer on all matters, technical and otherwise, involving the security of an information system, the ISSO shall provide: Interpretation and clarification of security policy, guidance, and new or changing IRM requirements.

The ISSO is responsible for the security of the system and informing the Authorizing Official of security issues. The ISSO is also responsible for recommending approval or disapproval of deviations from policy.[12] [redacted]

- [redacted]
- [redacted]

According to Information System Security Management, a formal process for recommending disapproval of deviations from policy that have a significant impact on IRS systems does not exist. The ISSOs would have to express their concerns through their management chain either verbally or through e-mail. Without any formal process for ISSOs to address the security risks from changes in policy, the IRS is putting itself at risk for exploitation of vulnerabilities.

Recommendation 3: The Chief Information Officer should ensure that the ISSOs have a formal process for recommending approval or disapproval of policy deviations to ensure that the operational security posture is consistent with current system security policy. This would include monitoring compliance with system security policy and providing guidance and recommendations to correct deficiencies.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will review the current formal process for recommending approval or disapproval of policy deviations to ensure that the operational security posture is consistent with current system security policy. This will

[12] IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities* (Sept. 2021).

include monitoring compliance with system security policy and providing guidance and recommendations to correct deficiencies.

The IRS Is Not Effectively Providing Oversight of Cloud Databases' Vulnerability Scan Results

We surveyed the IRS to determine:

- If the IRS's FISMA cloud system databases were being scanned with a vulnerability scanning tool using privileged credentials.
- If the IRS was receiving monthly scan results.

We identified [redacted] IRS FISMA cloud systems and determined that the IRS conducted monthly privileged vulnerability scans [redacted] of the [redacted] systems. The Enterprise Database Scanning office conducted these three scans on the cloud system databases with its database vulnerability scanning tool. [redacted], the IRS relies on the cloud service provider to provide monthly scanning reports. According to the IRS, the reports were high level and did not have the details of the vulnerabilities. Depending on the vendor, the IRS was able to download the reports in some instances but not in others. As a result, the IRS inconsistently received or was unable to review vulnerability details from cloud service providers across its FISMA cloud systems. We also determined that the IRS does not receive monthly vulnerability reports [redacted]

Based on the Federal Risk and Authorization Management Program (FedRAMP) Continuous Monitoring Guide, one of the deliverables of the cloud service provider to the agency is monthly database vulnerability scanning results. However, we determined the IRS was receiving vendor-designed reports and not the raw, detailed scanning data. Although the guide is unclear on the format of the deliverable, the IRS cannot accurately determine the vulnerabilities of the system without the detailed scanning data.

Amazon Web Services allows the agency to run an independent scan on its data in the cloud. Therefore, the IRS could be running privileged vulnerability scans on those cloud systems. Based upon IRS responses, we identified [redacted] cloud systems on the Amazon Web Services Government platforms that the IRS could be scanning but is not.[13]

Systems not being scanned could have vulnerabilities that are not detected and thus are unknown to the system owner. Rather than completing its own privilege vulnerability scans or receiving detailed vulnerability scan results, the IRS is relying on the FedRAMP requirements for ensuring that vulnerabilities are addressed in the majority of its cloud systems. Also, ISSOs cannot effectively perform their jobs with due diligence when they do not know the latest vulnerabilities on the databases they are accountable for. The IRS needs to have full access to the scan results and assurance that privileged scans are being performed. The IRS increases its risk of having its data compromised by not knowing what vulnerabilities exist on its databases.

[13] According to the IRS, since field work completed, it expanded the scanning scope of Amazon Web Service hosted applications.

The Chief Information Officer should ensure that:

Recommendation 4: Privileged vulnerability scans are performed on the cloud systems when possible.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will ensure that privileged vulnerability scans are performed on the cloud systems, when applicable.

Recommendation 5: The IRS provides oversight to cloud service providers and obtains detailed scan results so the IRS can assess the database vulnerabilities.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will ensure that oversight is provided to cloud service providers, which will include obtaining detailed scan results as part of database vulnerability management in the Continuous Monitoring Process when applicable.

Plans of Action and Milestones Were Not Created for Database Vulnerabilities

The IRM states that the IRS shall develop POA&Ms for IRS systems to document the planned remediation action to correct weaknesses. The POA&M Standard Operating Procedures state that critical and high-risk vulnerabilities that cannot be remediated within 30 or 60 calendar days should be documented as POA&Ms in the Treasury Department's FISMA Information Management System or the Authorizing Official should pursue a risk-based decision. Once documented in this system, the POA&M must comply with the guidance of the Standard Operating Procedures.

We judgmentally sampled[14] 10 FISMA systems from the IRS's database vulnerability scanning tool's report that required POA&Ms on outdated software patches that need to be applied to the databases. We found that the IRS only created POA&Ms for [redacted] FISMA systems we reviewed. For [redacted], the IRS provided various reasons for not creating POA&Ms, such as database administrator error or a vendor patch installation issue. However, it did not explain why POA&Ms were not created for the remaining [redacted]

Overall, we concluded that the IRS lacked managerial oversight to ensure that it appropriately documented corrective actions. Without a sound remediation process, the IRS cannot ensure that it is correcting and managing its information security weaknesses. Without sufficiently documenting POA&Ms, the IRS may not effectively remediate information security deficiencies in a timely manner, thereby exposing its systems to increased risks that nefarious actors will exploit the deficiencies to gain unauthorized access to information resources.

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

Recommendation 6: The Chief Information Officer should ensure that IRS policy is followed and create POA&Ms for unresolved issues from database vulnerability scans.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that POA&Ms are documented for unresolved aged database vulnerabilities scans and adhere to the Cyber POA&Ms Standard Operating Procedure.

Untimely Patching Leaves Databases Vulnerable

Treasury Directive Publication 85-01 requires agencies to remediate vulnerabilities on a timeline in accordance with the severity level of the vulnerability. According to the IRM,[15] the remediating organization shall remediate vulnerabilities based on when a vulnerability is detected. Critical vulnerabilities shall be remediated within 30 days of detection. In addition, the IRM[16] states that database management systems' products shall be a version supported by the vendor, including Oracle Database Server and Microsoft Structured Query Language (SQL) Server products.

In addition, Microsoft recommends ongoing, proactive installation of cumulative updates as they become available. Microsoft SQL Server cumulative updates are certified to the same levels as service packs and should be installed at the same level of confidence. Cumulative updates may contain value over and above hot fixes. This includes supportability, manageability, and reliability updates. Oracle Critical Patch Update Advisory states a critical patch update is a collection of patches for multiple security vulnerabilities and recommends that customers remain on actively supported versions and apply critical patch update security patches without delay.

Security faults with software applications and operating systems are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations are required to promptly install security-relevant software updates. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

Microsoft SQL and Oracle databases were not patched to the latest security patch

In October 2021, we requested a database vulnerability scanning report to show us open critical database vulnerabilities. The IRS provided a database vulnerability scan report for Microsoft SQL and Oracle databases executed on October 21, 2021, showing only critical vulnerabilities across the production, disaster recovery, test, and development environments, [redacted] Figure 2 shows unpatched weaknesses on Microsoft SQL and Oracle databases.

[15] IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (Sept. 2021).

[16] IRM 10.8.50, *Information Technology (IT) Security Servicewide Security Patch Management* (Nov. 2020).

[redacted]

[redacted]

Our analysis determined that the vulnerabilities [redacted] Based on the database vulnerability scanning results, the current version, *i.e.*, build, needs to be upgraded to the most recent version.

As of March 2022, the IRS has not patched a total of [redacted]

Microsoft SQL database vulnerabilities were not timely patched

In reference to Figure 2, the [redacted] Microsoft SQL database instances were not patched to the recommended security updates, service packs, and cumulative updates.[17] Of the [redacted] Microsoft SQL database instances, the Research, Applied Analytics, and Statistics (RAAS) office is responsible for patching [redacted] database instances. The Enterprise Operations function's Data Management Services and Support office is responsible for patching security and cumulative updates on the remaining [redacted] database instances; however, it stated that it is not responsible for installing service packs.

In March 2022, we met with the IRS to discuss its vulnerability remediation efforts. According to the Data Management Services and Support office, it already recognized gaps relative to the

[17] According to the IRS, the database vulnerability scanning tool defaults all databases without patches to "critical," and the cumulative updates recommended by the database vulnerability scanning tool were not required because they did not contain any security patches. Microsoft updates include service packs, security updates, and cumulative updates. These terms are defined within the glossary.

Microsoft SQL databases and worked collaboratively with all the stakeholders to resolve the gaps and install the latest cumulative and security updates to bring the databases into compliance. To corroborate the IRS's statement, we requested documentation to support that the IRS is in compliance with patching requirements. The Data Management Services and Support office responded that the majority of the findings are at the current patch level because:

- The recommended cumulative updates did not contain security patches.
- The IRM did not require patches to be installed within a specific time frame even though the database vulnerability scan results show it to be critical.

The Data Management Services and Support office added that, if the cumulative update does not include any security patches and the previous cumulative update was installed containing all the latest security patches, then it is compliant with the IRM. The IRM explicitly defines only security patches and does not refer to cumulative updates. In addition, the IRS stated that the databases were patched to the current patch available for the service pack.

We disagree with the IRS's statement because its database vulnerability scan report showed some cumulative updates were installed and some were not, while some security updates were installed and some were not. As Microsoft moved away from the service pack model and onto a continuous cumulative update model, the Microsoft SQL Server cumulative updates are certified to the same levels as service packs and should be installed at the same level of confidence.

The Data Management Services and Support office stated that it is not responsible for updating service packs. According to the IRS, the responsibility lies with application owners. In addition to the inconsistent patching of databases with cumulative updates, the IRS stated that the databases did not get patched due to resource issues. Further, the IRS has an individual project team that does not receive support from the Data Management Services and Support office. This project team manages systems that do not follow a normal patching process. If the IRS does not apply patches in a timely manner, it increases the risk of an attacker exploiting a known vulnerability on its information systems.

Management Action: According to the RAAS office, as of March 8, 2022, it patched the seven database instances and clarified responsibilities of the RAAS database administrators. Another component of the RAAS office, Statistics of Income, uses the Microsoft Windows Server Update Services to deploy and track updates to all Microsoft products in use in its environment. The System Administrators viewed the four Statistics of Income database instances as being up to date (and all security patches were applied) but did not look into the cumulative update patching aspect. Upon researching the cumulative update aspects and seeing that Microsoft has modified its SQL Server patching process, the RAAS office will apply cumulative updates to the databases. Going forward, the RAAS office's new executive leadership is prioritizing patch management and other objectives of the new security and privacy program. The RAAS office immediately corrected the patching issues and provided detailed information on a plan to mitigate its patching issues.

The Oracle database vulnerabilities were not timely patched

In reference to Figure 2, the Oracle database vulnerabilities were not patched timely to the appropriate level. Of the [redacted] Oracle database instances, the Data Management Services and Support office is responsible for patching [redacted] database instances and the RAAS

office is responsible for patching the remaining [redacted] database instances. The Data Management Services and Support and RAAS offices provided an explanation regarding the patches for the [redacted] database instances that remained uninstalled from [redacted] days as of October 21, 2021.

According to the Data Management Services and Support office, [redacted] of the Oracle database instances were not properly documented with a formal risk-based decision. The remaining database instances were not timely patched due to various reasons, including reliance on vendor patches that are bundled and an incorrect assumption that the database was covered by a Risk Acceptance Form and Tool. For the three RAAS Oracle databases, the causes for not timely patching databases included limited staffing resources, data center relocation, and efforts to upgrade Oracle databases and host system transitions. The RAAS office then retired two databases and patched the other Oracle database. It plans to use the database vulnerability scanning tool's scans to address patching deficiencies, prioritize assignments and scheduling, and attempt to hire additional staffing.

Recommendation 7: The Chief Information Officer should ensure that databases are patched or upgraded to the latest version or appropriately document risk acceptance with a risk-based decision or Risk Acceptance Form and Tool.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that databases are patched or upgraded to the latest version or appropriately document risk acceptance with a risk-based decision or Risk Acceptance Form and Tool.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the IRS is adequately assessing the risks to its databases when performing vulnerability scans and installing timely patches. To accomplish our objective, we:

- Identified the Federal guidance and IRS policy and procedures by reviewing National Institute of Standards and Technology guidance and the Department of Defense *Mainframe Product Security Requirements Guide* and reviewing the IRM regarding the identification (*i.e.,* vulnerability scanning) and resolution of database vulnerabilities.
- Determined whether databases are being properly scanned monthly by surveying stakeholders. We also reviewed the database vulnerability scanning tool's monthly vulnerability scan reports and obtained documentation on Filing Season Critical and High Value Asset systems from the Cybersecurity function. For database systems that are not being scanned for vulnerabilities, we determined whether the responsible party for the database is aware that vulnerabilities are not being identified.
- Determined whether the project teams are aware of and timely resolving or mitigating identified vulnerabilities by reviewing all Microsoft SQL and Oracle database instances database vulnerability scan reports for the production, disaster recovery, test, and development environments and interviewing the patching team.
- Determined whether POA&Ms were created to review, resolve, and mitigate identified weaknesses by interviewing the appropriate personnel. We also selected a judgmental sample[1] of 10 systems to determine whether POA&Ms were created for systems requiring critical patches.
- Determined if the IRS addressed previously reported issues, including the scanning of databases and the creation of an action plan for all of the database vulnerability scanning tool's findings, by reviewing corrective actions taken to address TIGTA database security findings.

Performance of This Review

This review was performed with information obtained from the Office of the Chief Information Officer located in the New Carrollton Federal Building in Lanham, Maryland, during the period November 2020 through May 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Kasey Koontz, Audit

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

Manager; Cari Fogle, Lead Auditor; Charles Ekunwe, Senior Auditor; Linda Nethery, Senior Auditor; and Midori Ohno, Senior Auditor.

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 policies and procedures related to information technology security, database security, and mainframe security; National Institute of Standards and Technology guidance; the Department of Defense *Mainframe Product Security Requirements Guide;* and Microsoft and Oracle best practices. We evaluated these controls by interviewing IRS management and staff, reviewing data and reports 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:

- Protection of Resources – Potential; the IRS is not completing database vulnerability scans on [redacted] IBM mainframe systems (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We compared the Filing Season Critical system list dated October 26, 2021, to the vulnerability scanning reports dated March 18, 2021, and December 1, 2021. Our analysis determined that the databases on [redacted] IBM mainframe systems were not scanned for vulnerabilities.

Type and Value of Outcome Measure:

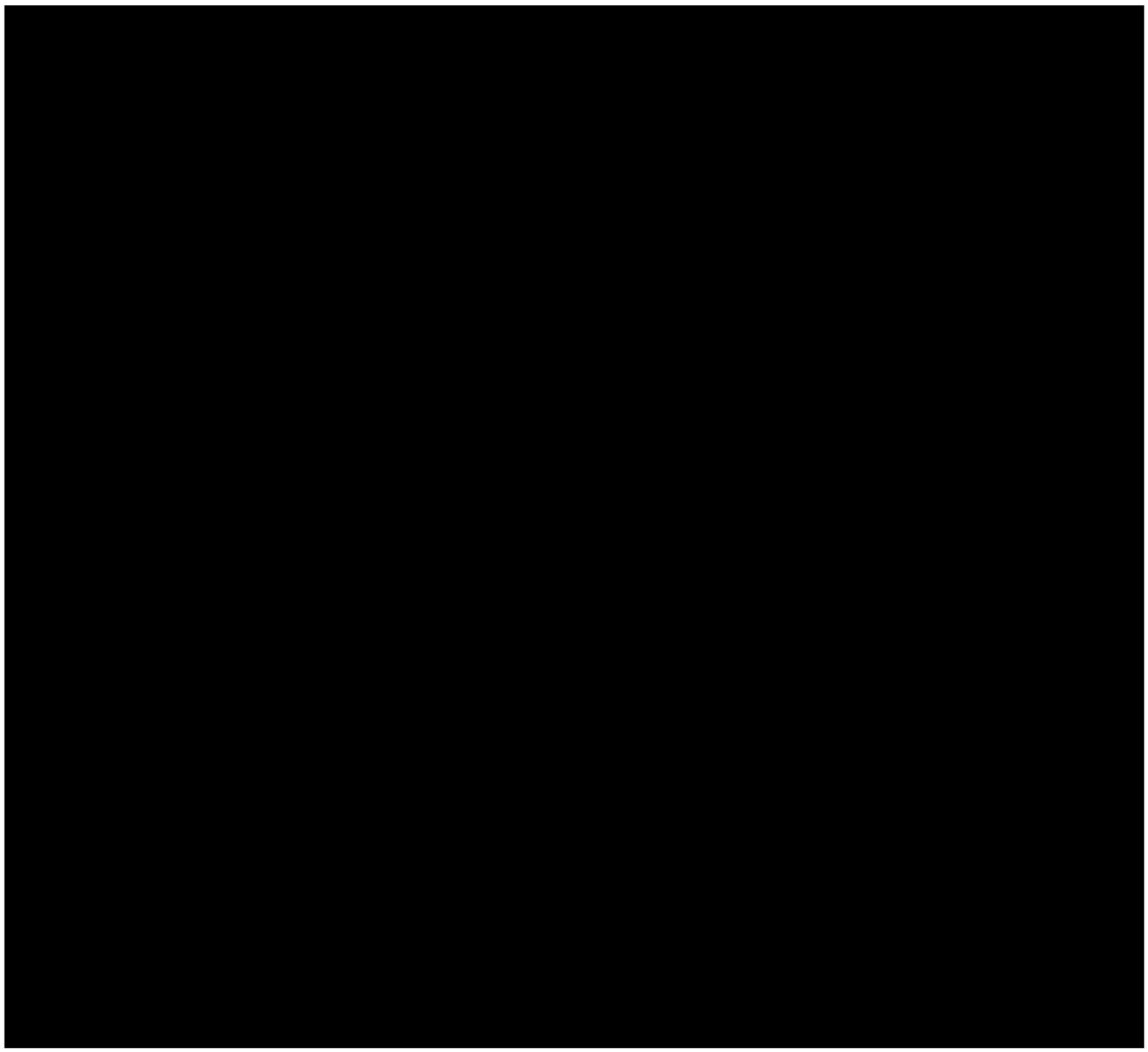
- Protection of Resources – Potential; [redacted] database instances had critical vulnerabilities that exceeded the IRS policy for timely remediation (see Recommendation 7).

Methodology Used to Measure the Reported Benefit:

We analyzed the October 21, 2021, security vulnerability scan report for Oracle and Microsoft SQL databases and determined there [redacted] calendar days in the production, disaster recovery, test, and development environments. According to the IRS, it has brought the systems to the correct patch level or decommissioned [redacted] database instances were not patched or decommissioned as of March 2022.

Appendix III

Database Scanning Timeline



Appendix IV

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 27, 2022

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer
Digitally signed by B3CCB
Date: 2022.09.27
16:42:35 -04'00'

SUBJECT: Draft Audit Report –The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls (Audit 202120003)

Thank you for the opportunity to review the draft audit report. We are once again disappointed that the IRS and the TIGTA team proved unable to correct and improve the audit report at the discussion draft stage. Unfortunately, this draft audit report does not accurately reflect database security at the IRS or the multi-faceted approach we use to identify and remediate vulnerabilities in accordance with established processes. We have completed numerous upgrades and security improvements over the past several years to ensure full visibility into the security risks impacting operating systems, commercial off-the-shelf products and databases.

The IRS uses multiple scanning tools and compensating controls, in addition to following the vendor-recommended timeline for patching. Our approach remains consistent with the applicable federal guidelines, and although we agree with the audit team's recommendations to continuously improve, we disagree with the presentation of certain findings in this report. For example, to determine the number of database instances with outdated patches, the audit team relied on a tool that fails to distinguish security and non-security vulnerabilities. As a result, the number of outdated instances appears significantly inflated. Based on the IRS's analysis, approximately 62 percent of the instances identified by TIGTA related to Microsoft SQL databases were not valid. TIGTA also adopts a position inconsistent with best practices by suggesting that Microsoft Cumulative Updates should be applied in all situations. Our approach to patching Microsoft database service packs, including cumulative updates, is standard, effective, secure and driven by application-level releases.

The IRS is committed to continuously improving database security. We have begun taking steps to address the procedural gaps identified in the draft audit report and have prioritized remediation efforts based on the severity level of the vulnerability risk. We agree with the recommendations and outcome measures in this report and have included a corrective action plan.

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 Frank Henderson, director, Security Operations and Standards, at 681-260-3680.

Attachment

Attachment

Audit 202120003, *The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Control*

RECOMMENDATION 1: The Chief Information Officer should ensure that [redacted] is performed on all International Business Machine (IBM) mainframe databases.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The IRS will [redacted]

IMPLEMENTATION DATE: June 15, 2023

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The IRS will [redacted].

IMPLEMENTATION DATE: October 15, 2024

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

RECOMMENDATION 2: The Chief Information Officer should ensure that Internal Revenue Manual (IRM) 10.8.33 is updated to accurately reflect the Mainframe Product Security Requirements Guide.

CORRECTIVE ACTION 2: The IRS agrees with the recommendation; however, IRM 10.8.33 accurately reflects the Defense Information Systems Agency (DISA) Mainframe Product Security Requirements Guide. Security Policy has opened a ticket with DISA to address the inconsistency in their language regarding the title and applicability of the Security Requirements Guide (SRG) and will update IRM 10.8.33 accordingly.

IMPLEMENTATION DATE: April 15, 2023

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

Attachment

Audit 202120003, *The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Control*

RECOMMENDATION 3: The Chief Information Officer should ensure that the Information System Security Officers (ISSOs) have a formal process for recommending approval or disapproval of policy deviations to ensure that the operational security posture is consistent with current system security policy. This would include monitoring compliance with system security policy and providing guidance and recommendations to correct deficiencies.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The IRS will review the current formal process in place for recommending approval or disapproval of policy deviations to ensure that the operational security posture is consistent with current system security policy. This will include monitoring compliance with system security policy and providing guidance and recommendations to correct deficiencies.

IMPLEMENTATION DATE: February 15, 2023

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

RECOMMENDATION 4: The Chief Information Officer should ensure that privileged vulnerability scans are performed on the cloud systems when possible.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The IRS will ensure that privileged vulnerability scans are performed on the cloud systems, when applicable.

IMPLEMENTATION DATE: October 15, 2023

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

RECOMMENDATION 5: The Chief Information Officer should ensure that the IRS provides oversight to cloud service providers and obtains detailed scan results so the IRS can assess the database vulnerabilities.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. The IRS will ensure oversight is provided to cloud service providers which will include obtaining detailed scan results as part of database vulnerability management in the Continuous Monitoring Process, when applicable.

Attachment

Audit 202120003, *The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Control*

IMPLEMENTATION DATE: October 15, 2023

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

RECOMMENDATION 6: The Chief Information Officer should ensure that IRS policy is followed and create Plan of Action & Milestones (POA&Ms) for unresolved issues from database vulnerability scans.

CORRECTIVE ACTION 6: The IRS agrees with this recommendation. The IRS will ensure POA&Ms are documented for unresolved aged database vulnerabilities scans and adhere to the Cyber POA&Ms Standard Operating Procedure (SOP).

IMPLEMENTATION DATE: May 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Operations

RECOMMENDATION 7: The Chief Information Officer should ensure that databases are patched or upgraded to the latest version or appropriately document risk acceptance with a risk-based decision or Risk Acceptance Form and Tool.

CORRECTIVE ACTION 7: The IRS agrees with this recommendation. The IRS will ensure that databases are patched or upgraded to the latest version or appropriately document risk acceptance with a risk-based decision or Risk Acceptance Form and Tool.

IMPLEMENTATION DATE: August 20, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Operations

Appendix V

Glossary of Terms

Term	Definition
Build	A version of a program that, as a rule, is a prerelease version and is identified by a build number rather than by a release number.
Business Unit	A title for major IRS organizations such as the Independent Office of Appeals, Wage and Investment Division, Office of Professional Responsibility, and Information Technology organization.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including a means for protecting personal privacy and proprietary information.
Cumulative Updates	Both Windows client and Windows Server use the cumulative update mechanism, in which many fixes to improve the quality and security of Windows are packaged into a single update. Each cumulative update includes the changes and fixes from all previous updates.
Database Instance	A set of memory structure and background processes that access a set of database files.
Database Vulnerability Scanning Tool	Scans database infrastructures on a scheduled basis to detect vulnerabilities to include in security patch updates and suggests remedial actions.
Denial-of-Service Attack	Actions that strive to make a computer resource unavailable to authorized users, generally consisting of the concerted efforts of an attacker to prevent an information resource from functioning efficiently or at all, temporarily or indefinitely.
Event	Any action that happens on a computer system. Examples include logging in to a system, executing a program, and opening a file.
General Support System	Sets of resources that provide necessary information technology infrastructure support to applications and business functionality such that compromise would have a severe adverse effect on the IRS mission, tax administration functions, or employee welfare.
Hot Fixes	A single, cumulative package that includes one or more files that are used to address a problem in a product.
Infrastructure	The hardware, software, and network resources and services required for the existence, operation, and management of an enterprise information technology environment. It allows an organization to deliver information technology solutions and services to its employees, partners, and customers and is usually internal to an organization and deployed within owned facilities.

Term	Definition
Local User Accounts	User accounts stored locally on the server. These accounts can be assigned rights and permissions on a particular server, but on that server only. Local user accounts are security principals that are used to secure and manage access to the resources on a standalone or member server for services or users.
National Institute of Standards and Technology	A nonregulatory Federal agency within the Department of Commerce responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
Oracle	An object-relational database management system.
Patch	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
Privileged Access	A right granted to an individual, a program, or a process.
Risk Acceptance Form and Tool	Used in an organization's approval processes to clearly document business decisions in the context of risk and acceptance.
Risk-Based Decision	A decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analyses, assessments, and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase, and a decision is made taking the entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis assessments, recommended risk mitigation strategies, and business impact.
Security Update	A widely released fix for a product-specific, security-related vulnerability.
Service Pack	A software package that contains several updates for an application or operating system.
Structured Query Language	The standard language for relational database management systems. SQL statements are used to perform tasks such as update data on a database or retrieve data from a database.
Unauthorized Disclosure	Any disclosure or release not permitted by Federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

Appendix VI

Abbreviations

FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
IBM	International Business Machines
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISSO	Information System Security Officer
POA&M	Plan of Action and Milestones
RAAS	Research, Applied Analytics, and Statistics
RACF	Resource Access Control Facility
SQL	Structured Query Language
TIGTA	Treasury Inspector General for Tax Administration

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

(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.