TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Are Needed to More [redacted] the Virtual Host Infrastructure Platform

June 3, 2021

Report Number: 2021-20-024

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

HIGHLIGHTS: Improvements Are Needed to More [redacted] the Virtual Host Infrastructure Platform

Final Audit Report issued on June 3, 2021 **Report Number 2021-20-024**

Why TIGTA Did This Audit

Server virtualization is now an established standard for enterprise information technology infrastructure in data centers and cloud services as it provides better utilization of hardware resources, reduces physical space required, and reduces power consumption and administrative overhead.

This audit was initiated to determine whether the IRS virtual host infrastructure platform is effectively managed and secured.

Impact on Taxpayers

The virtual host infrastructure platform of [redacted] servers provides the virtualization infrastructure running [redacted] virtual systems at the IRS. Protecting critical assets and infrastructure helps reduce the risk of internal and external attacks on IRS assets that could potentially expose taxpayer data and information.

What TIGTA Found

The IRS is performing security scans of the virtual host infrastructure platform. However, TIGTA reviewed vulnerability scan reports from an old and new application spanning several months in Calendar Year 2020 and found that the IRS did not [redacted] TIGTA reviewed reports from August through November 2020 and found that [redacted] However, they are managing patch compliance on [redacted] servers using a virtualization application. In addition, [redacted]

The IRS inventory system does not accurately reflect all of the virtual host infrastructure platform servers. For example, [redacted] virtual host servers were uncategorized and incorrectly recorded. In addition, TIGTA identified clerical errors and servers that were classified as administratively lost or had an uncertified status. In response to this finding, the Virtualization Branch team submitted documentation to classify three servers as administratively lost and updated the inventory system to correctly categorize [redacted] platform servers. Finally, the IRS did not provide evidence that it is following a standardized process for decommissioning platform servers.

What TIGTA Recommended

The Chief Information Officer should ensure that critical and high-risk vulnerabilities are [redacted]

The IRS agreed with our recommendations and plans to [redacted]

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

June 3, 2021

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed to More [redacted] the Virtual Host Infrastructure Platform
(Audit # 202020003)

This report presents the results of our review to determine whether the virtual host infrastructure platform is effectively managed and secured. This review is part of our Fiscal Year 2021 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of Internal Revenue Service Resources*.

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

Copies of this report are also being sent to the Internal Revenue Service 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

According to the National Institute of Standards and Technology, server virtualization[1] is now an established standard for enterprise information technology infrastructure in data centers and cloud services as it provides better utilization of hardware resources, reduces physical space required, and reduces power consumption and administrative overhead.[2] In Calendar Year 2007, the Internal Revenue Service (IRS) concluded that its diverse and widely deployed server infrastructure would benefit from a consolidation and virtualization project. As a result, the IRS established the Virtualization Project Office to design and implement a virtual host infrastructure environment. Previously, the IRS's computing environment consisted of a combination of earlier server consolidations resulting from organizational changes and lacked a single enterprise standard. Collectively, this resulted in higher operational costs, reduced security, and systems that were not flexible enough to support rapid rollout of new services. The IRS initiated the Server Consolidation and Virtualization project in February 2007 and completed it in December 2010.

[3]

Results of Review

**********2**********

The IRM states that vulnerabilities shall be prioritized for remediation based on risk (highest to lowest) using the Common Vulnerability Scoring System scores provided by the scanning tools. Figure 1 shows vulnerability severity risk-level score ranges and their associated remediation time frames.

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

[2] National Institute of Standards and Technology, Special Publication 800-125A, *Security Recommendations for Server-based Hypervisor Platforms*, (Revision 1, June 2018).

[3]

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

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

Source: IRM 10.8.1.

We initially reviewed vulnerability scan reports from January through May 2020 from the IRS's previous enterprise vulnerability scanning tool, which the IRS replaced during our audit. [redacted] In September 2020, we met with officials in the Enterprise Operations and Cybersecurity functions to discuss the results of our analysis. During the meeting, the IRS confirmed it implemented a new vulnerability scanning tool in August 2020 to replace the prior tool, which produced differing results. [redacted] In addition, we reviewed monthly scanning reports from the new vulnerability scanning tool for September through November 2020. [redacted]

[redacted]

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]

[4] [redacted]

According to the IRS, [redacted]

Recommendation 1: The Chief Information Officer should ensure that [redacted]

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that [redacted]

[redacted]

The National Institute of Standards and Technology provides security controls that are designed to facilitate compliance with applicable Federal laws, Executive orders, directives, policies, regulations, standards, and guidance.[5] Two such controls include risk assessment and configuration management.

The National Institute of Standards and Technology[6] also states that the configuration of a system and its components has a direct impact on the security posture of the system. How the configurations are established and maintained requires a disciplined approach for providing adequate security. Changes to the configuration of a system are often needed to stay up to date with changing business functions and services and information security needs. However, changes can adversely affect the previously established security posture; therefore, effective configuration management is vital to the establishment and maintenance of security of information and systems. The security-focused configuration management process is critical to maintaining a secure state under normal operations, contingency recovery operations, and reconstitution to normal operations.

In addition, the IRM provides guidance to:

- Protect the critical infrastructure and assets of the IRS against attacks that exploit them.
- Prevent unauthorized access to IRS assets.
- Enable computing environments that meet security requirements and support the business needs of the organization.[7]

[5] National Institute of Standards and Technology, Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013). Revision 5 of this publication was released in September 2020. We assessed the Risk Assessment and Configuration Management controls required during our audit fieldwork. Because we had completed the majority of our analysis by September 2020, we used the criteria established in Revision 4.

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

[7] IRM 10.8.15, *Information Technology Security – General Platform Operating System Security Policy* (Nov. 27, 2019).

Configuration compliance management for [redacted]

The IRS implemented a new software configuration compliance scanning application in April 2020 to replace the prior application that was outdated. On December 15, 2020, we met with officials in the Cybersecurity and Enterprise Operations functions for a demonstration of the new application. We observed that the new application scanned [redacted] We reviewed monthly configuration compliance reports from August through November 2020 [redacted] According to the Cybersecurity function officials, a server is noncompliant if it has one high-risk issue or the overall compliance score is below 90 percent. [redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

According to the IRS, [redacted]

In addition to our review of the monthly compliance reports, we reviewed the August 2020 Preliminary Security Assessment Report[8] prepared by the Cybersecurity function that reported an analysis of compliance scans [redacted]. The Security Assessment Report summarizes the risks associated with the vulnerabilities identified during the security assessment activities that were performed on the system and provides IRS officials with a more holistic view of risk regarding the system. [redacted][9]

[8] IRS, *Virtual Host Infrastructure Enterprise Container Platform* (Aug. 26, 2020).
[9] [redacted]

[redacted]

[redacted]

[redacted][10]

[redacted][11]

The Chief Information Officer should:

Recommendation 2: Ensure that [redacted]

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure [redacted] using the new Continuous Diagnostics and Mitigation tool and ensure that [redacted] The Chief Information Officer found that, of the [redacted] of known false positives identified incorrectly by the new scanning tool as vulnerabilities. This false positive situation is being addressed with the product supplier.

Office of Audit Comment: The IRS provided no documentation to support the false positives described above. The Continuous Diagnostics and Mitigation

[10] In Calendar Year 2013, the Department of Homeland Security established the Continuous Diagnostics and Mitigation Program as an implementation approach for continuously monitoring information systems. The program is designed to facilitate automated security control assessment and continuous monitoring that is consistent with established guidance by providing a robust, comprehensive set of monitoring tools, a continuous monitoring dashboard, and implementation assistance.

[11] IRM 2.150.2, *Configuration Management Process* (Aug. 19, 2020).

Program [redacted]

Recommendation 3: [redacted]

Management's Response: [redacted]

**********2**********

According to the IRS Enterprise Security Audit Trails Project Management Office, a Platform Audit Plan is designed to assist the Enterprise Operations and Cybersecurity functions to achieve the following:

- Understand which system events are associated with significant security risk (*i.e.*, actionable events).
- Configure systems to monitor auditable events.
- Log events and capture an audit trail of relevant data.
- Deliver audit data to the enterprise solution for security information and event management.
- Respond to security incidents.
- Analyze and report on event trends.

A Platform Audit Plan helps ensure that systems meet auditing requirements in the IRM and National Institute of Standards and Technology guidance. However, as of February 2021, the Platform Audit Plan for the virtual host infrastructure platform had not been approved.

*****2*****

[redacted] The IRS created a Plan of Action and Milestones in May 2017 that stated there was no evidence of review and analysis of information system audit records or reporting of findings to IRS officials [redacted] However, between August 2017 and April 2019, there were several requests, including management escalations, from the Cybersecurity function to the Virtual Host Infrastructure team asking for milestone updates. As a result of these unanswered requests, the planned completion date for this Plan of Action and Milestones has been delayed, with a new target completion date of June 15, 2021. [redacted]

[redacted] Protecting critical assets and infrastructure helps reduce the risk of internal and external attacks on IRS assets.

The Chief Information Officer should:

Recommendation 4: Finalize, approve, and implement a Platform Audit Plan for the virtual host infrastructure platform.

Management's Response: The IRS agreed with this recommendation and will address Recommendations 4 and 5 together in the response to Recommendation 5.

Recommendation 5: [redacted]

Management's Response: [redacted]

Server Inventories **********2**********

The IRM[12] documents a multistep process for information technology asset management that includes maintaining an asset once it has been implemented. Managing inventory data includes issuing the annual inventory certification plan, updating the repository (move/add/change requests), managing anomalies (resolving discrepancies in the repository), and recommending corrective actions. The Enterprise Operations function is responsible for annually certifying asset records under their organizational control, including servers. The Enterprise Messaging and Virtualization Branch (hereafter referred to as the Virtualization Branch team) is responsible for submitting updates to key fields in the asset record for existing platform servers. The Virtualization Branch team provided copies of change requests to add, update, and retire asset records throughout this review. We found inventory discrepancies and server decommissioning inconsistencies.

Physical inventory

The IRS inventory system does not accurately reflect all of the virtual host infrastructure platform servers. [redacted]

[12] IRM 2.149.3, *Information Technology Asset Management, Asset Management Hardware Procedures* (Sept. 18, 2018).

[redacted][13] [redacted]

In September 2020, we performed a physical inventory [redacted][14] [redacted][15]

[redacted]

The Virtualization Branch team follows the User and Network Services Hardware Asset Management User Guide[16] to manage its platform server inventory. However, [redacted]

Management Actions

In response to this finding, the Virtualization Branch team performed the following actions:

- August 26, 2020, [redacted].
- September 21, 2020, submitted a change request to update the inventory system [redacted].
- October 20, 2020, prepared a [redacted].
- December 15, 2020, submitted a new change request to update the inventory system [redacted] as a result of the September 21, 2020, change request. [redacted].

[13] Uncertified assets are those that are still uncertified after two or more inventory cycles and any high-risk assets not certified in the current inventory cycle.

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

[15] [redacted]

[16] IRS, *Asset Management – User and Network Services Hardware Asset Management User Guide* (Sept. 27, 2019).

Decommissioning

The IRM states that there are three required activities for disposing of information technology assets: determine information technology assets at end of life, manage disposal activities, and update the repository. The Enterprise Operations function's [redacted] has a server retirement checklist that contains 28 sequential steps to retire a server. [redacted][17] [redacted]

The Chief Information Officer should:

Recommendation 6: Update the asset management guidance to [redacted]

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that the IRS follows [redacted] established asset management process for inventory revision.

Office of Audit Comment: The IRS's established inventory policy [redacted]

Recommendation 7: Ensure that standard operating procedures are [redacted]

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that the IRS [redacted]

[17] IRS, *Retirement, Excess, and Disposal of Enterprise Operations Information Technology Equipment Standard Operating Procedures*, (Oct. 2020).

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the virtual host infrastructure platform is effectively managed and secured. To accomplish our objective, we:

- Reviewed and analyzed multiple security vulnerability reports to identify critical and high-risk vulnerabilities and interviewed IRS employees to review and validate our analysis to determine whether security vulnerabilities were timely remediated according to guidance established by the IRM.
- Reviewed server security configuration policy compliance reports to identify high vulnerabilities and interviewed IRS employees regarding security policies and procedures to determine whether configuration vulnerabilities were remediated within agency security policies.
- Reviewed audit monitoring policies, the System Security Plan, and evidence of audit log existence to assess whether audit monitoring controls were effective to ensure secure operations and oversight of the platform in accordance with the National Institute of Standards and Technology and the IRM.
- Reviewed relevant IRMs and inventory reports and performed a physical inventory review to determine the completeness and accuracy of the virtual host infrastructure platform server inventory. We selected a judgmental sample[1] of [redacted].
- Reviewed relevant IRMs, server retirement checklists, standard operating procedures, and screen shots from the inventory system to evaluate the server decommissioning process. We selected a judgmental sample [redacted] from the retired asset report and reviewed documentation to support checklist steps completion.

Performance of This Review

This review was performed during the period March 2020 through February 2021. We performed work [redacted] and worked closely with the Enterprise Operations and Cybersecurity functions. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jena Whitley, Director; Mike Mohrman, Audit Manager; Corey Brown, Lead Auditor; Jamillah Hughes, Auditor; Avery Dortch, Information

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

Technology Specialist; and Johnathan D. Elder, Information Technology Specialist (Data Analytics).

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: National Institute of Standards and Technology requirements and IRM policies and procedures for the management and security of virtual host servers. We evaluated these controls by interviewing IRS employees, reviewing data obtained from IRS systems, and analyzing relevant documentation provided by the IRS.

Appendix II

Outcome Measure

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

Type and Value of Outcome Measure:

- Reliability of Information – Actual; [redacted] on the September 2020 official inventory report (see Recommendation 6).

Methodology Used to Measure the Reported Benefit:

We performed a site visit [redacted] and judgmentally selected a sample of servers to trace back to the IRS inventory report. [redacted] Upon further analysis, [redacted]

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CHIEF INFORMATION OFFICER

April 13, 2021

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger /s/ Nancy A. Sieger
Chief Information Officer

SUBJECT: Draft Audit Report – Improvements Are Needed to More [redacted] the Virtual Host Infrastructure Platform (Audit #202020003) (e-trak #2021-33208).

Thank you for the opportunity to review your draft audit report and to discuss draft report observations with Enterprise Operations and the Cybersecurity organization. The IRS is committed to [redacted] Virtual Host Infrastructure Platform and the continued support, assistance, and guidance your team provides is very valuable to us in this regard.

We appreciate the opportunity your team has given us to examine the host infrastructure in order to produce a comprehensive corrective action plan [redacted] As the IRS looks to modernize its legacy systems and infrastructure, maintaining the privacy and security of our data remains our top priority.

Even in the face of the myriad challenges presented by the pandemic and our processing EIP1, EIP2 & EIP3, the Virtual Host Infrastructure Platform has responded rapidly to any exposures and/or vulnerabilities, decreasing the possibility of cyberattacks. This included migrating from unsupported to supported hardware to support filing session 2020 and remediation of vulnerabilities. We have provided tools and patching across the Enterprise that will identify and address further cyberattacks.

We concur with the recommended measurable benefits on tax administration, as noted in the March 12th memo and the draft report. In response to your recommendations, we have attached our corrective action plan. We are committed to implementing the corrective actions.

The IRS values the continued support and assistance provided by your office. Should you have any questions, please contact me at (801) 388-6456, or a member of your

staff may contact Jignesh Gandhi, Director, Enterprise Operations, Infrastructure Services Division, at (571) 439-9705.

Attachment

Attachment

Draft Audit Report – Improvements Are Needed to More [redacted]
the Virtual Host Infrastructure Platform (Audit # 202020003)

RECOMMENDATION 1
The IRS agrees with this recommendation. The Chief Information Officer will ensure that [redacted]

CORRECTIVE ACTION
ACIO, EOPs will ensure that [redacted]
The ACIO, EOPs found that [redacted] The ACIO, EOPs [redacted]

IMPLEMENTATION DATE
August 15, 2022

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

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 2
The IRS agrees with this recommendation. Ensure that [redacted]

CORRECTIVE ACTION

The ACIO, EOPs will ensure [redacted] using the new CDM tool and that [redacted] The Chief Information Officer found that of the [redacted] known false positives identified incorrectly by the new scanning tool as vulnerabilities. This false positive situation is being addressed with the product supplier.

IMPLEMENTATION DATE
November 15, 2023

Attachment

Draft Audit Report – Improvements Are Needed to More [redacted]
the Virtual Host Infrastructure Platform (Audit # 202020003)

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

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 3
IRS agrees with the recommendation. [redacted]

CORRECTIVE ACTION 3a

The ACIO, Cybersecurity [redacted]

IMPLEMENTATION DATE
November 15, 2023

CORRECTIVE ACTION 3b

The ACIO, Cybersecurity [redacted]

IMPLEMENTATION DATE
November 15, 2023

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 4
The IRS agrees with the recommendation for Platform Auditing [redacted] and is addressing Recommendations 4 and 5 together in Corrective Action 5. Finalize, approve, and implement a Platform Audit Plan for the virtual host infrastructure platform.

Attachment

Draft Audit Report – Improvements Are Needed to More [redacted]
the Virtual Host Infrastructure Platform (Audit # 202020003)

CORRECTIVE ACTION
The IRS will address Recommendations 4 and 5 together in Corrective Action 5.

IMPLEMENTATION DATE
June 15, 2022

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Enterprise Operation

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 5
IRS agrees with this recommendation. [redacted]

CORRECTIVE ACTION
Audit Process Corrective Actions for Recommendations 4 and 5 are underway.

- [redacted]

[redacted]

IMPLEMENTATION DATE
June 15, 2022

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

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 6
The IRS agrees with this recommendation. Update the asset management guidance [redacted]

Attachment

Draft Audit Report – Improvements Are Needed to More [redacted]
the Virtual Host Infrastructure Platform (Audit # 202020003)

CORRECTIVE ACTION

The ACIO, EOPs will ensure the IRS follows the [redacted] established asset management process for inventory revision.

IMPLEMENTATION DATE

September 15, 2022

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN

IRS will monitor this corrective action as part of our internal management system of controls.

OUTCOME MEASURE – Appendix II

Type and Value of Outcome Measure: We concur

Reliability of Information – Potential; [redacted] on the September 2020 official inventory report (see Recommendation 6).

RECOMMENDATION 7

The IRS agrees with this recommendation. Ensure standard operating procedures are [redacted]

CORRECTIVE ACTION

The ACIO, EOPs will ensure the IRS [redacted]

IMPLEMENTATION DATE:

November 15, 2022

RESPONSIBLE OFFICIAL(S)

Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN

IRS will monitor this corrective action as part of our internal management system of controls.

Appendix IV

Glossary of Terms

Term	Definition
Decommission	An approach to accomplishing data center consolidation that involves turning off servers that are not being used or are used infrequently.
Exploit	A general term for any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.
Host	Any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, servers, personal electronic devices, thin clients, and multifunctional devices.
[redacted]	[redacted]
[redacted]	[redacted]
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Virtualization	The simulation of the software and hardware upon which other software runs.
Vulnerability	Weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten network security.

Appendix V

Abbreviations

[redacted]	[redacted]
IRM	Internal Revenue Manual
IRS	Internal Revenue Service

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.