TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Cyber Threat Hunting Program Properly Conducts Analysis to Identify Threats; However, Guidance, Documentation, and Controls Need to Be Improved

July 20, 2023

Report Number: 2023-20-040

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

HIGHLIGHTS: The Cyber Threat Hunting Program Properly Conducts Analysis to Identify Threats; However, Guidance, Documentation, and Controls Need to Be Improved

Final Audit Report issued on July 20, 2023 **Report Number 2023-20-040**

Why TIGTA Did This Audit

Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. These threats include unusual network traffic, unusual file changes, and the presence of malicious code. The Advanced Threat Analysis team performs threat hunting for the IRS and operates under the Computer Security Incident Response Center.

The overall objective of this audit was to determine whether the cyber threat hunting program is effectively monitoring, detecting, and addressing indicators of attack or compromise to the IRS network.

Impact on Tax Administration

As the Nation's tax agency, the IRS collects and stores substantial amounts of Personally Identifiable Information, including all tax records for individuals and corporations. In addition, IRS systems contain information about planned or ongoing examinations, collection actions, and criminal investigation cases.

A successful attack could significantly impact tax administration and possibly national security. The IRS uses hundreds of different computer systems to perform different functions, from storing tax records to consolidating print files for notices. Depending on which systems are infected, the result could vary from minor to catastrophic.

What TIGTA Found

The IRS monitors 29 primary sources of data as part of the threat hunting process. However, the IRS's Internal Revenue Manual does not contain any threat hunting requirements. IRS management stated that they are aware that the manual needs to be updated; however, they did not have a timeline for the update. By not having established policies and procedures, the IRS risks its employees not meeting Federal requirements for cyber threat hunting. Federal guidelines require agencies to conduct cyber threat hunting activities, including conducting risk assessments, performing threat hunting, and participating in cyber threat information sharing.

TIGTA reviewed 25 threat hunting intelligence tickets and determined that IRS analysts properly conducted the threat hunts. However, the results of the threat hunts were not documented completely. Specifically, 10 (40 percent) of the 25 tickets did not contain sufficient information regarding the threat hunt process, results, or severity of the risk, and seven (28 percent) of the 25 tickets did not contain all necessary documentation. By not fully documenting the results of the threat hunt, other analysts, IRS management, and outside reviewers who assess the threat intelligence tickets will not be able to independently draw a conclusion as to the severity of the threat nor determine if the proper actions were taken to mitigate potential risks to the IRS network.

In addition, IRS analysts do not have a formal review and approval process for removing device or program blocks that restrict access to the IRS network. All analysts within the threat hunting group have the ability to add and remove device or program blocks without a review or approval process. By not having a formal or documented review and approval process for removing blocks from the server, the IRS risks an analyst accidentally removing a block to or from external sources that still pose a threat to the IRS network or intentionally removing a block to cause harm to the IRS network.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that: 1) the Internal Revenue Manual is updated with the National Institute of Standards and Technology requirements for conducting threat hunts at the IRS; and 2) the Cybersecurity function develops a formalized process for the review and approval of proposed device or program block removals.

The IRS agreed with both recommendations. The Chief Information Officer plans to update the Internal Revenue Manual to align with the National Institute of Standards and Technology Threat Hunting controls and create a formal process and associated procedures for malicious category block removals.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

July 20, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Cyber Threat Hunting Program Properly Conducts Analysis to Identify Threats; However, Guidance, Documentation, and Controls Need to Be Improved
(Audit # 202220005)

This report presents the results of our review to determine whether the cyber threat hunting program is effectively monitoring, detecting, and addressing indicators of attack or compromise to the Internal Revenue Service (IRS) network. This review is part of our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS Resources.*

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

Table of Contents

Appendices

Background

Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. A threat is any circumstance or event with the potential to adversely impact organizational operations; organizational assets, individuals, other organizations; or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. These threats include unusual network traffic, unusual file changes, and the presence of malicious code. The objective of cyber threat hunting is to track and disrupt cyber adversaries as early as possible in the attack and to improve the speed and accuracy of organizational responses to protect the security and privacy of sensitive information. Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as:

Cyber threat hunting proactively searches for advanced threats.

- Firewalls.
- Intrusion detection and prevention systems.
- Quarantining malicious code in sandboxes.
- Security Information and Event Management technologies and systems.

As the Nation's tax agency, the Internal Revenue Service (IRS) collects and stores substantial amounts of Personally Identifiable Information, including all tax records for individuals and corporations. In addition, IRS systems contain information about planned or ongoing examinations, collection actions, and criminal investigation cases. A successful attack on the IRS network could significantly impact tax administration and possibly national security. The IRS uses hundreds of different computer systems to perform different functions, from storing tax records to consolidating print files for notices. Depending on which systems are infected, the result could vary from minor to catastrophic.

The National Institute of Standards and Technology (NIST) requires Federal organizations to conduct cyber threat hunting activities, including conducting risk assessments, performing threat hunting, and participating in cyber threat information sharing.[1] It also states that organizations should conduct cyber threat hunting activities to search for indicators of compromise and detect, track, and disrupt threats that evade existing controls.

Threat hunting teams leverage existing threat intelligence and create new threat intelligence to share with peer organizations, relevant information sharing organizations, and relevant government departments and agencies.[2] The IRS's Emerging Threat team, now known as the Advanced Threat Analysis team, originally started in Calendar Year 2008, and evolved over time.

[1] NIST, Special Publication 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information* (Feb. 2021). See Appendix III for a glossary of terms.

[2] NIST, Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (Revision 5; Sept. 2020).

The Advanced Threat Analysis team performs threat hunting for the IRS and operates under the Computer Security Incident Response Center. The results of any identified threat hunts are documented in a cyber threat management system. As of August 2022, the Advanced Threat Analysis team consists of 12 Government employees and two contractors. Of this team, five employees and both contractors are analysts who conduct threat hunting.

Results of Review

The Advanced Threat Analysis Team Has Access to Primary Data Sources and Properly Conducts Threat Hunts

We identified 29 primary data sources used to identify potential threat activity within the IRS network by reviewing network diagrams of connections between the IRS and outside networks. In addition, when a threat is identified by an organization outside of the IRS, the Advanced Threat Analysis team searches its data sources on the IRS network to determine if signs of the threat are present. To determine if the Advanced Threat Analysis team had access to all primary data sources, we reviewed a list of IRS system logs that the Advanced Threat Analysis team could access. Our analysis determined that the Advanced Threat Analysis team has access to all 29 primary data sources, across the IRS network, for review and analysis in their threat hunting process. NIST guidance requires agencies to establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems; to detect, track, and disrupt threats that evade existing controls; and to employ the threat hunting capability.

We reviewed the threat hunting intelligence tickets documented in the cyber threat management system and identified 125 tickets from October 1, 2020, through September 30, 2022. A threat hunting intelligence ticket is the record created by the Advanced Threat Analysis Team analysts documenting the threat hunting steps performed and any evidence gathered. Figure 1 provides the number of recorded incidents by fiscal year. Figure 2 provides the number of recorded incidents by the threat intelligence source.

Figure 1: Threat Hunting Intelligence Tickets by Fiscal Year

Fiscal Year	Threat Hunts Recorded
2021	56
2022	69
Total	**125**

Source: IRS cyber threat management system.

Figure 2: Threat Hunting Intelligence Tickets by Originating Source Organization

Threat Intelligence Source	Threat Hunts Recorded
Computer Security Incident Response Center Analysis	111
Online Fraud Detection and Prevention	1
Other	3
Treasury Government Security Operations Center	2
United States Computer Emergency Readiness Team	8
Total	**125**

Source: IRS cyber threat management system.

The goal of threat hunting is to perform an iterative review of different data sources and identify anomalies that may lead to a potential compromise or a security breach. The IRS refers to these data sources as the logs, system events, network traffic, or activities that provide insight into the flow of data and activities on the IRS network. The Advanced Threat Analysis team has two primary documents that guide the threat hunting process. The first document provides a high-level overview of what threat hunting is, the elements of a threat hunt, data sources for threat hunts, and techniques for conducting the threat hunts.[3] The second document is a desk guide that provides a more detailed description of the procedures that the analysts should follow when conducting threat hunts.[4] The desk guide lists a 13-step process for threat hunting, separated into four phases:

1. Pre-Stage Collection.
2. Techniques, Tactics, and Procedure Operationalization.
3. Hunting.
4. Post-Threat Hunting.

We selected a judgmental sample of 25 tickets (20 percent) of the 125 documented threat hunts for review. For the first three phases of the threat hunting process, we found that the Advanced Threat Analysis team properly conducted the threat hunts for each sampled ticket.[5] For the fourth phase, post-threat hunting, we determined that improvements were needed.

[3] IRS Computer Security Incident Response Center: Advanced Technical Analysis Cell, *Threat Hunting Operations* (August 21, 2022).

[4] IRS Computer Security Incident Response Center: Advanced Technical Analysis Cell, *Threat Hunting Desk Guide* (August 22, 2022).

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

The Advanced Threat Analysis Team Documentation and Guidance Are Incomplete

Threat hunting documentation is incomplete

During our sample review of documented threat hunts, we also analyzed the fourth phase called Post-Threat Hunting. We found that 10 (40 percent) of the 25 threat intelligence tickets did not contain sufficient information regarding the threat hunt process, results, or severity of the risk, and seven (28 percent) of the 25 tickets did not contain all necessary documentation.

Our judgmental sample of 25 tickets found **10** with **insufficient information** and **seven** with **insufficient documentation**.

The desk guide requires analysts to record all steps and thought processes during the hunt and immediately report important findings to the Computer Security Incident Response Center and management. In the Post-Threat Hunting phase, there is a requirement to document and submit the results to management. However, the desk guide does not specify what should be included, such as actions taken to address the potential threat.

We discussed the lack of completeness of information in the threat intelligence tickets with the IRS. An IRS official stated that the threat hunting tickets are informational, and that if an actual threat exists, the IRS will open an incident response ticket. The IRS official agreed to work on developing additional guidance for the analysts regarding the threat hunting documentation. The lack of detailed requirements in the threat hunting desk guide contributed to the lack of sufficient documentation in the threat intelligence tickets.

We provided IRS management a list of the threat hunts reviewed and requested further information for the tickets that lacked complete information. The IRS provided additional information for the tickets to satisfy our questions regarding the threat hunts. However, by not fully documenting the results of the threat hunt (*e.g.*, steps taken to complete the hunt or actions taken as a result of the hunt), other analysts, IRS management, and outside reviewers who review the threat intelligence tickets will not be able to independently draw a conclusion as to the severity of the threat or determine if the proper actions were taken to mitigate potential risks to the IRS network.

Management Action: During our audit work, the IRS provided an addendum to the Threat Hunting Desk Guide that outlines additional steps for analysts to take when documenting threat hunts. This addendum requires that analysts provide a severity level of the threat in a mandatory field within the intelligence ticket. The addendum also states that if needed, analysts will link the threat intelligence ticket to an existing device or program block ticket.

Internal Revenue Manual guidance is incomplete

We reviewed the Internal Revenue Manual to determine if the IRS had added the appropriate language to document a baseline of security controls for threat hunting. The IRS had not identified threat hunting security controls for inclusion in the Internal Revenue Manual.

NIST guidance recommends agencies establish a security control baseline for information systems within its network. Security control baselines serve as a starting point for the protection of information systems and taxpayer information.[6] In addition, NIST requires Federal organizations to conduct cyber threat hunting activities such as:

- Searching for indicators of compromise in organization systems.
- Detecting, tracking, and disrupting threats that evade existing controls.
- Sharing new threat intelligence with relevant government departments and agencies.[7]

IRS management stated that they are aware that the manual needs to be updated; however, they did not have a timeline for the update. IRS management also stated that the Advanced Threat Analysis team was just being formed at the time the Internal Revenue Manual was last updated. By not establishing security controls within policies and procedures, the IRS risks its employees not meeting Federal requirements for cyber threat hunting, placing IRS data and systems at risk.

Recommendation 1: The Chief Information Officer should ensure that the Internal Revenue Manual is updated with NIST requirements for conducting threat hunting at the IRS.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will update the Internal Revenue Manual to align with NIST Threat Hunting controls.

The Advanced Threat Analysis Team Does Not Formally Review and Approve Access to Devices or Programs Previously Restricted

The Advanced Threat Analysis team's analysts conduct threat hunts on the IRS network based on internal and external information obtained from various sources. When an analyst concludes there is a risk to the IRS network from an outside domain, the analyst may submit a request to restrict access to the domain involved. Analysts restrict access to the IRS network through device or program blocks to stop possible malicious traffic, attack attempts, or any other intrusions. The blocks are placed on the server through an automated process once the analyst submits the request.

Analysts can independently remove device or program blocks without management's review.

Guidance used by the analysts does not require management review and approval to add and remove device or program blocks from a server.[8] Analysts can independently remove device or

[6] NIST, Special Publication 800-53B, *Control Baselines for Information Systems and Organizations* (Oct. 2020).

[7] NIST, Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (Sept. 2020).

[8] IRS, *Desk Guide on Block and Unblock Process via the Content Filtering Recategorization Requests.*

program blocks (designed to restrict access to malicious sites) without management's review. Management from the Advanced Threat Analysis team stated that removal of malicious code device or program blocks is a stringent analysis and peer review process, but there is no formal documentation to support this review process.

The Government Accountability Office *Standards for Internal Control in the Federal Government* Principle 10 requires management to divide or segregate key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions and reviewing the transactions so that no one individual controls all key aspects of a transaction or event.

According to IRS management, they chose the current process because it allows a level of agility to their operations. By not having a formal or documented review process in place for removing device or program blocks from the server, the IRS risks an analyst accidentally removing a device or program block from a domain that still poses a threat to the IRS network, or intentionally removing a block to cause harm to the IRS network.

Management Action: During our audit work, we discussed the lack of a formal review and approval process for removing device or program blocks from the servers with IRS management. We expressed our concerns regarding the risk of a block being removed incorrectly. In response, IRS management developed and distributed a desk guide to the analysts that provides a workflow process to follow when creating or removing a device or program block request. We reviewed the steps in the desk guide and found they address the need to ensure that analysts fully investigate any proposed device or program block removal to ensure that no risk continues to exist. These steps include sharing and discussing the findings of the investigation with the other analysts on the team prior to executing the removal of the block. Despite these changes, there is still no requirement for management or senior analyst approval before removing the block.

Recommendation 2: The Chief Information Officer should ensure that the Cybersecurity function develops a formalized process for the review and approval of proposed device or program block removals.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will create a formal process and associated procedures for malicious category block removals.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the cyber threat hunting program is effectively monitoring, detecting, and addressing indicators of attack or compromise to the IRS network. To accomplish our objective, we:

- Identified the Advanced Threat Analysis team's primary sources by reviewing network diagrams of connections from the IRS to outside networks. Afterwards, we determined whether the Advanced Threat Analysis team had access to all primary systems by reviewing a list of IRS system logs that the Advanced Threat Analysis team could access as part of its analysis and review process.
- Evaluated the controls over the management of blocks associated with threat hunting activities by reviewing the block addition and removal process and documented guidance.
- Determined the completeness of the IRS's policies and guidance related to the cyber threat hunting program by comparing them to the Federal, NIST, and other applicable requirements.
- Evaluated threat hunting documentation by reviewing a sample of threat hunt intelligence tickets from the cyber threat management system. We selected a judgmental sample of 25 threat hunting intelligence tickets from the population of 125 tickets documented between October 1, 2020, and September 30, 2022, to review threat hunts that were initiated from a variety of data sources as well as both older and new threat hunts.[1] We selected a judgmental sample because we did not plan to project to the population.

Performance of This Review

This review was performed with information obtained from the Cybersecurity function located at the New Carrollton Federal Building in Lanham, Maryland, and Memphis, Tennessee, during the period August 2022 through March 2023. 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 Manager; Michael Segall, Lead Auditor; and Suzanne Westcott, Senior Auditor.

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

Validity and Reliability of Data From Computer-Based Systems

During this review, we relied on data received from the IRS's cyber threat management system for Fiscal Years 2021 and 2022 that were available on the IRS's network. We evaluated the data by 1) ensuring that the downloaded data was readable and complete; 2) reviewing the data to detect obvious errors, duplicate values, and unexpected missing data; and 3) interviewing IRS subject matter experts about the data. We determined the data were sufficiently reliable to support our conclusions, findings, and recommendations.

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: Advanced Threat Analysis policies and procedures; NIST, Special Publication 800-53, Revision 5; and NIST, Special Publication 800-172. We evaluated these controls by interviewing Cybersecurity function personnel, including the Advanced Threat Analysis team; reviewing the Advanced Threat Analysis Threat Hunting Desk Guide, the Advanced Threat Analysis Threat Hunting Full Guide, and the NIST guidelines; comparing the Advanced Threat Analysis guides to the NIST guidelines; and reviewing a judgmental sample of 25 threat hunting intelligence tickets.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

June 29, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Jeffrey W. King,
Acting Chief Information Officer

Jeffrey King

ffxkb
cn=ffxkb,
email=Jeffrey.W.King@irs.gov
2023.06.29 11:18:16 -04'00'

SUBJECT: Draft Audit Report – The Cyber Threat Hunting Program Properly Conducts Analysis to Identify Threats; However, Guidance, Documentation, and Controls Need to Be Improved (Audit #202220005)

Thank you for the opportunity to review and comment on the subject draft audit report. The IRS strives to continually evolve and sustain the robust and multi-layered cybersecurity program currently protecting taxpayer data and IRS resources.

The IRS Cybersecurity function, including our Cyber Threat Fusion Center, focuses on staying one step ahead of potential threats. Threat hunting is a critical proactive cyber defense strategy with the goal of iteratively searching through networks to detect and isolate advanced threats in an effort to manage risks to computer systems and networks. Malicious cyber actors intent on disrupting U.S. government operations remain a persistent threat. The IRS has made significant progress in continuously adapting and adjusting its processes, procedures, and capabilities. As noted in this draft report, the IRS took immediate actions during the course of the audit to improve our documentation and related processes.

As part of the government-wide effort to strengthen our nation's cyber defenses, we continuously coordinate with the Department of the Treasury and the Cybersecurity and Infrastructure Security Agency. We will continue the work to meet IRS and Departmental goals to keep federal assets secure. While some of your final recommendations have already been implemented, we will incorporate your recommendations into our processes moving forward. We concur with the two recommendations in this draft report and plan to complete implementation of all corrective actions by February 15, 2024.

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 Robert Cox, Associate Chief Information Officer for Cybersecurity, at (202) 923-5923.

Attachment

Audit# 202220005, The Cyber Threat Hunting Program Properly Conducts Analysis to Identify Threats; However, Guidance, Documentation, and Controls Need to Be Improved

RECOMMENDATION 1: The Chief Information Officer should ensure that the Internal Revenue Manual is updated with NIST requirements for conducting threat hunting at the IRS.

CORRECTIVE ACTION 1: The IRS agrees with the recommendation. The Chief Information officer will update IRM 10.8.1 to align with NIST Threat Hunting controls.

IMPLEMENTATION DATE: February 15, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 2: The Chief Information Officer should ensure that the Cybersecurity function develops a formalized process for the review and approval of proposed device or program block removals.

CORRECTIVE ACTION 2: The IRS agrees with the recommendation. The Chief Information Officer will create a formal process and associated procedures for malicious category block removals.

IMPLEMENTATION DATE: October 15, 2023

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

Appendix III

Glossary of Terms

Term	Definition
Block	A process to prevent malicious traffic from entering a network.
Computer Security Incident Response Center	Part of the Cybersecurity function. The Computer Security Incident Response Center's mission is to ensure that the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify and eradicate cyber threats or cyber attacks. One of its primary duties is to provide 24-hour monitoring and support for IRS operations seven days a week, 365 days a year.
Control Baseline	The set of security and privacy controls defined for a low-impact, moderate-impact, or high-impact system or selected based on the privacy selection criteria that provide a starting point for the tailoring process.
Cyber Threat Management System	A commercial-off-the-shelf product that provides a web-based application for cyber threat management. The Computer Security Incident Response Center captures cybersecurity and computer-related security incidents in the cyber threat management system.
Cybersecurity Function	A function within the Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
Online Fraud Detection and Prevention	Part of the IRS's Operations Support. The Online Fraud Detection and Prevention's work includes coordination of surveillance monitoring, identification, and removal of IRS phishing sites in collaboration with Criminal Investigation, the Treasury Inspector General for Tax Administration, and the Computer Security Incident Response Center.
Treasury Government Security Operations Center	Serves as the Department of the Treasury's computer security incident response capability and is responsible for monitoring network traffic.

Term	Definition
United States Computer Emergency Readiness Team	A partnership between the Department of Homeland Security and the public and private sectors, established to protect the Nation's internet infrastructure. The United States Computer Emergency Readiness Team coordinates defense against and responses to cyber attacks across the Nation.

Appendix IV

Abbreviations

IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology

**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.