TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Process, Training, and Awareness Enhancements Can Better Inform Employees on How to Report Taxpayer Assaults and Threats

September 5, 2023

Report Number: 2023-IE-R009

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

HIGHLIGHTS: Process, Training, and Awareness Enhancements Can Better Inform Employees on How to Report Taxpayer Assaults and Threats

Final Evaluation Report issued on September 5, 2023 **Report Number 2023-IE-R009**

Why TIGTA Did This Study

It is a Federal crime to forcibly assault, resist, oppose, impede, intimidate (threaten), or interfere with a Federal employee engaged in or on account of the performance of official duties, particularly with the administration of Internal Revenue laws. When IRS employees endure and report assaults or threats, the IRS and TIGTA review the circumstances surrounding these incidents.

TIGTA initiated this evaluation to evaluate the procedures on reporting employee assaults and threats and ensure that taxpayers who commit these crimes are identified and known to all IRS employees who may need to subsequently interact with these taxpayers.

Impact on Tax Administration

While most Americans respect IRS employees and its mission, taxpayers experiencing financial difficulties may feel increased pressure and act aggressively toward IRS employees. Unfortunately, this at times results in taxpayers assaulting or threatening an IRS employee.

Ensuring the safety and protection of its employees, especially those who have direct contact with the public, is an issue that remains of continued concern for the IRS.

What TIGTA Found

The IRS took timely actions in response to employee reports of assaults and threats. However, TIGTA identified actions to timelier update tax accounts of potentially dangerous taxpayers after an employee was assaulted or threatened. Our review of 790 potentially dangerous taxpayer cases from October 2019 to November 2022 found that it took an average of 30 calendar days from the incident to the potentially dangerous taxpayer indicator posting to the taxpayer's account. The range of time for indicators to be input took from one to 1,058 calendar days.

Also, guidance to employees on how to report assaults and threats contained inaccurate and inconsistent information. For example, a facsimile number listed as a reporting option was no longer operational. In addition, the IRS established a variety of ways for employees to report assaults and threats, including contacting local TIGTA offices, calling various TIGTA or IRS telephone numbers, or completing online incident reporting forms on both TIGTA's public website and the IRS's internal website. Our evaluation found several examples where the IRS cited different combinations of these reporting methods on guidance documents.

Lastly, TIGTA found some issues with training and awareness efforts on reporting assaults and threats. Only two of 205 incident reporting personnel completed a required training course during Fiscal Year 2022. This training highlights the importance of employees reporting incidents and provides information on incident processing and reporting. In addition, our site visits found that not all employees knew how to report assaults and threats.

What TIGTA Recommended

TIGTA made seven recommendations to the IRS to correct the potentially dangerous taxpayer indicator process delays with new processes, address the inaccurate and inconsistent reporting messages to employees, ensure that the required training course is added to all incident reporting employees' profiles and tracked for completion, and submit a request to develop assault and threat reporting guidance in the form of a poster.

The IRS agreed with all seven recommendations. The IRS implemented a process where its information system is updated with notifications of investigation cases for immediate input of potentially dangerous taxpayer indicators. In addition, the IRS developed a list of inaccurate information on reporting of assaults and threats and will update all internal guidance with a unified message instructing employees on processes and procedures for reporting assaults and threats. The IRS also added required training to incident reporting personnel's profiles and will send reminders to employees who have not taken the training, and will publish an incident reporting banner that will be available for business units to order and post at their locations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 5, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Russell P. Martin
Deputy Inspector General for Inspections and Evaluations

SUBJECT: Final Report – Process, Training, and Awareness Enhancements Can Better Inform Employees on How to Report Taxpayer Assaults and Threats (Evaluation # IE-23-001)

This report presents the results of our review to evaluate the procedures that Internal Revenue Service (IRS) employees follow to report and process assaults and threats. This review is part of our Fiscal Year 2023 Annual Program 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 III. If you have any questions, please contact me or James A. Douglas, Director, Inspections and Evaluations.

Table of Contents

Appendices

Background

While most Americans respect Internal Revenue Service (IRS) employees and its mission, taxpayers experiencing financial difficulties may feel increased pressure and act aggressively toward IRS employees. Unfortunately, this at times results in taxpayers assaulting or threatening an IRS employee. In an August 20, 2022, letter to the IRS Commissioner,[1] the President of the National Treasury Employees Union requested that the IRS conduct a comprehensive assessment of the security measures at all IRS facilities. The National Treasury Employees Union letter stated that, "*IRS workers are often targeted due to the nature of their work, which requires close interaction with the public. Too many times in the past, we have seen anti-government, anti-worker statements fuel violent attacks on innocent Federal employees*."[2]

In an August 23, 2022, response to concerns raised by the National Treasury Employees Union, the former IRS Commissioner sent a letter to IRS employees noting, "*there has been an abundance of misinformation and false social media postings, some of them with threats directed at the IRS and its employees. We are aware of these concerning messages, and I want to assure you that your safety is and will continue to be my top priority*." Ensuring the safety and protection of its employees, especially those who have direct contact with the public, is an issue that remains of continued concern for the IRS.

Internal Revenue Code § 7212 and 18 U.S.C. § 111 state that it is a Federal crime to forcibly assault, resist, oppose, impede, intimidate (threaten), or interfere with a Federal employee engaged in or on account of the performance of official duties, particularly with the administration of Internal Revenue laws. The Treasury Inspector General for Tax Administration (TIGTA) has law enforcement authority over the IRS on allegations involving any attempt to corruptly interfere with or impede tax administration and any actions designed to harass IRS employees or interfere with activities or functions of IRS personnel.

Process for IRS employees to report taxpayer assaults and threats

The IRS has developed processes and procedures for IRS employees to report taxpayer assaults and threats. Specifically, IRS employees are required to report incidents of assaults and threats to the IRS Facilities Management and Security Services (FMSS) Situational Awareness Management Center (SAMC) and the TIGTA Office of Investigations (OI) within 30 minutes of incident discovery or identification, or when it is safe to do so. IRS personnel can report these incidents via IRS intranet website, e-mail, and/or can contact the IRS via telephone. SAMC and TIGTA roles include:

- SAMC personnel, *i.e.*, referred to as Watch Standers, who man a 24-hour operation to handle all intake sources for the IRS on reported assaults and threats. Specifically, the Watch Standers enter incident information into the IRS *Threat Response Center System*,

[1] See Appendix II for a copy of this letter.

[2] The Treasury Inspector General for Tax Administration Office of Inspections and Evaluations initiated an interim evaluation on *Employee Safety and Security – Assessment of the IRS's Comprehensive Security Review of Its Facilities* (IE-22-015) to monitor the National Treasury Employees Union's request for the IRS. Specifically, the Office of Inspections and Evaluations will evaluate the adequacy of the IRS's comprehensive review of safety and security measures at its facilities.

which is the system the IRS uses to process and manage all incidents, within 15 minutes of IRS employee reporting.

- TIGTA OI's Operations Division that handles the intake of assault and threat incidents for TIGTA and uses its information management system to track and monitor all complaints, cases, and investigations.

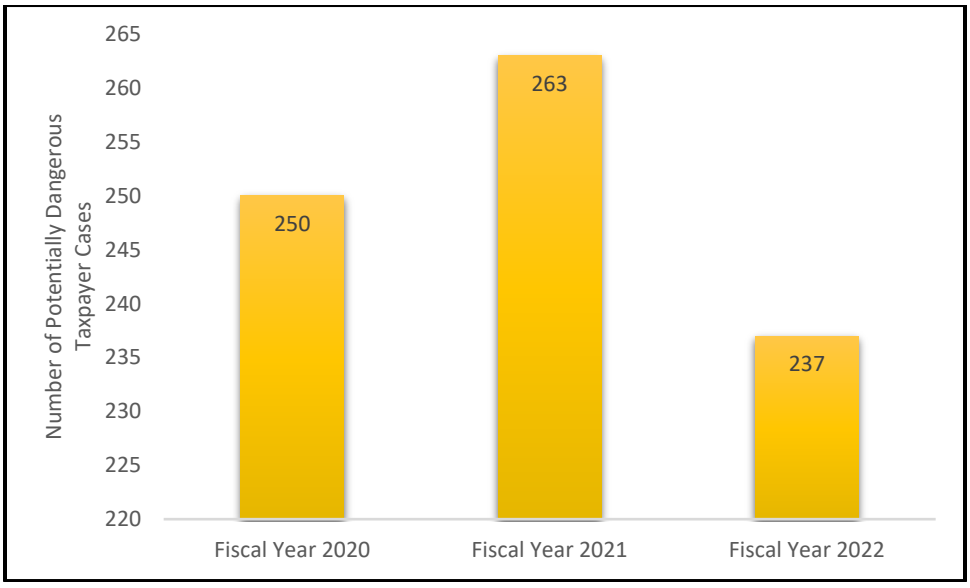
The IRS has also established a unique indicator that is placed on the tax accounts of taxpayers who have demonstrated hostile behavior and could be a threat when contacted again by an IRS employee. This indicator denotes the taxpayer as a potentially dangerous taxpayer (PDT). This account indicator is added to these tax accounts so other IRS employees are aware that the taxpayer has demonstrated hostile behavior and could be a threat when contacted again.

Assignment of complaint to TIGTA OI

Once an assault or threat incident is reported, the case is assigned to a local TIGTA office with geographic responsibility over the area where the incident occurred or where the taxpayer making the threat resides. In addition to TIGTA special agents investigating the assault or threat as a criminal case, special agents will also determine whether a PDT indicator should be added to the taxpayer's tax account. Specifically, is there verifiable evidence that the taxpayer assaulted, threatened, or intimidated the employee, contractor, or their families, and that the taxpayer is identifiable by a Social Security Number or Employer Identification Number, and the incident has a nexus to tax administration.

When the special agent determines the assault or threat meets PDT criteria, TIGTA OI will forward the case to the IRS Privacy, Governmental Liaison, and Disclosure Office of Employee Protection (OEP). When OEP case workers receive the case, they will enter a PDT indicator on the taxpayer's account in the Integrated Data Retrieval System to update the Master File databases within 24 hours of receipt. Figure 1 presents the total number of 750 PDT cases by Fiscal Years 2020, 2021, and 2022.

Figure 1: The Number of PDT Cases by Fiscal Year



Source: TIGTA analysis based on data provided by IRS OEP.

Results of Review

Our evaluation found that the IRS took timely actions in response to employee reports of assaults and threats. This includes timely entering incident information into the IRS's tracking system as well as ensuring that the incidents were referred to TIGTA OI to initiate investigative efforts. However, we identified that program enhancements were needed to timelier add PDT indicators on the tax accounts of taxpayers who assaulted or threatened an IRS employee. Once we notified IRS management of our concern, actions were taken to update processes and procedures to address our concern.

In addition, our evaluation identified that guidance documents contained inaccurate and inconsistent information as to the process for employee reporting of assaults and threats. Finally, FMSS security personnel did not complete required training on how to report assault and threat incidents. We also identified that IRS contract employees did not complete mandatory physical security awareness briefings, and IRS employees did not always know how to report assaults and threats.

Actions Were Taken to Update Processes and Procedures to Timelier Add Indicators on the Accounts of Taxpayers Who Assault or Threaten Employees

The IRS took timely actions in response to IRS employee reporting of assaults and threats. For example:

- SAMC Watch Standers were timely entering incident information into the IRS's *Threat Response Center System*, averaging 13 minutes after the initial reporting.
- SAMC incidents were shared with TIGTA OI to ensure that investigative efforts began on all taxpayers who assaulted or threatened an IRS employee.
- OEP case workers, once they receive PDT investigation cases from TIGTA, input PDT indicators onto taxpayer accounts within 24 hours for 772 (98 percent) of 790 PDT cases from October 2019 to November 2022.

Although each of these actions were taken timely, PDT indicators were not posted on taxpayer accounts immediately after assaults or threats were reported. The ultimate posting of this indicator averaged 30 calendar days after the employee was assaulted or threatened. Specifically, our review of 790 PDT cases initiated during the period October 2019 to November 2022 found that it took on average of 30 calendar days from the reporting of the assault or threat to the PDT posting onto the taxpayer's account. The range of time for posting took from one to 1,058 calendar days.

On March 1, 2023, we issued an e-mail alert and reported that the OEP inputs the PDT indicator on taxpayer accounts after TIGTA special agents complete their preliminary work and initiate an investigation case on the taxpayer. Our concern was that TIGTA OI allows its special agents 60 calendar days to complete this preliminary work before it sends a case to the OEP to have a PDT indicator placed on the taxpayer's account. Timely posting of the PDT indicator is of the utmost importance as the indicator is displayed prominently on various internal tax documents and IRS systems to flag those taxpayers who pose a threat to the safety of IRS employees, contractors, and their families.

Recommendation 1 (E-Mail Alert): On March 1, 2023, we recommended that the Chief Privacy Officer receive notification from TIGTA OI at the time an investigation related to assaults and threats against IRS employees is initiated. Once notified, the PDT indicator should be input immediately on the individual's tax account who assaulted or threatened the IRS employee.

> **Management's Response to E-Mail Alert:** IRS management agreed with this recommendation. On April 4, 2023, the OEP implemented a process with TIGTA OI to update its information system with notifications of investigation cases each night for immediate input of the PDT indicator.

Guidance Documents Need to Be Updated to Ensure That Assault and Threat Reporting Information Is Accurate and Consistent to Reduce Employee Reporting Confusion

Our review of guidance documents that include information on processes and procedures that IRS employees should follow to report assaults and threats identified both inaccuracies and inconsistencies. For example:

- ***Inaccurate messaging*** – Guidance documents include a facsimile number (1-202-317-6129) that was not operational. Just prior to our evaluation, the IRS took action to remove this option as a reporting method for employees but had not updated its guidance.
- ***Inconsistent messaging*** – The IRS established a variety of ways for employees to report assaults and threats. These include reporting via:
  - Contacting local TIGTA OI agents.
  - Calling the TIGTA toll-free hotline number, after-hours toll-free number, or submitting online an Incident Reporting Form.[3]
  - Calling the SAMC toll-free hotline number or telephone number or submitting online or via e-mail an Incident Reporting Form.

As detailed previously, there are many options IRS employees can use to report assaults and threats. Our research of IRS SharePoint sites and internal guidance documents identified several examples of inconsistent messaging on how employees should report these incidents. For example:

- Internal guidance on Incident Reporting indicated that TIGTA needs to be contacted in the event of a threat or assault but did not list the TIGTA hotline number to be used for reporting.
- IRS Source web page titled "Critical Situations in the Workplace" did not have a link for the local TIGTA OI contact information. Also, only one of the two TIGTA hotline numbers was listed.

[3] An Incident Reporting Form is an entry form in which an employee provides specific information about the assault or threat, such as employee information, circumstances about the incident, and taxpayer information.

- IRS Source web page titled "Threat/Assault Reporting" did not have a link for the local TIGTA OI contact information.
- IRS SharePoint web page titled "TIGTA Threat/Assault Reporting" only had one of the two TIGTA hotline numbers. In addition, contact information for the SAMC was not mentioned.
- IRS SharePoint web page titled "TIGTA Threat/Assault Reporting" did not mention the requirement for contacting the SAMC in addition to contacting TIGTA.
- FMSS document titled "Report security threats to the Situational Awareness Management Center" did not mention the requirement for contacting TIGTA after a threat or assault has occurred.

On December 20, 2022, we issued an e-mail alert notifying IRS management of concerns with the inaccurate and inconsistent messaging for employees to report assaults and threats. Being threatened or assaulted is a traumatic experience and being unable to easily identify how to report the incident could adversely compound that ordeal.

Recommendation 2 (E-Mail Alert): On December 20, 2022, we recommended that the Chief, FMSS, evaluate whether the SAMC facsimile number is a viable method to report assaults and threats, and based on this decision, either remove references to this number from all reporting instructions and guidance or ensure that the use of this number is to an operational facsimile machine.

> **Management's Response to E-Mail Alert:** IRS management agreed with this recommendation and has discontinued the option for employees to report assaults or threats via facsimile and removed the number from the Internal Revenue Manual.

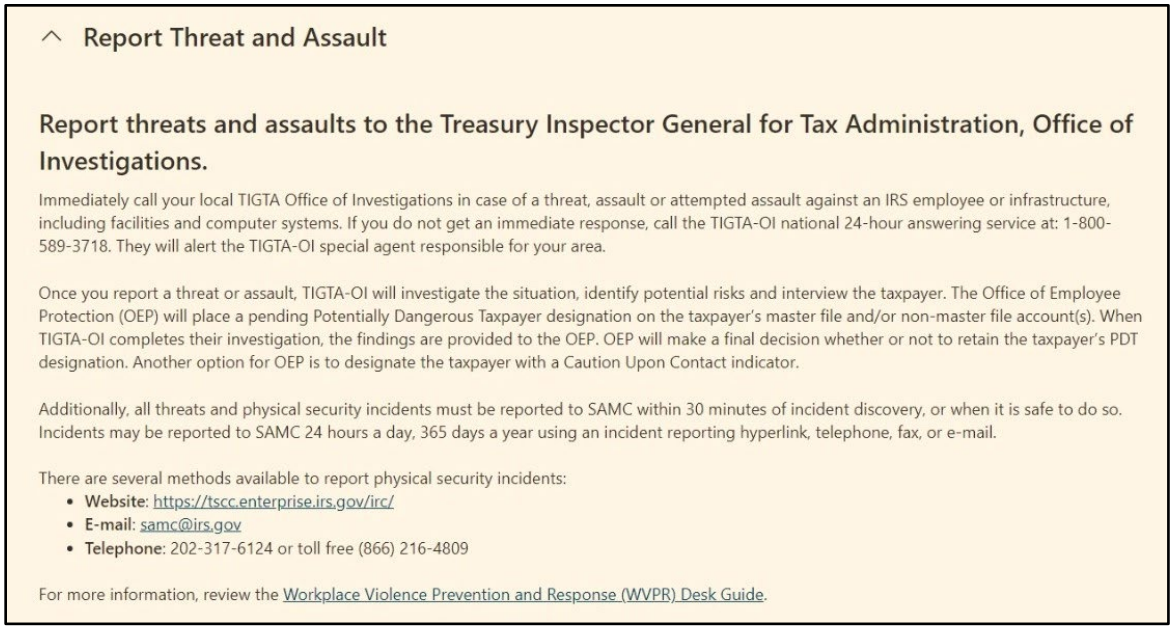
Recommendation 3 (E-Mail Alert): On December 20, 2022, we recommended that the Chief, FMSS, identify all existing instructions and guidance on how to report threats and assaults to ensure consistency and accuracy of this guidance.

> **Management's Response to E-Mail Alert:** IRS management agreed with this recommendation and has worked with Communications and Liaison staff and developed a list of inaccurate information related to reporting assaults and threats.

Recommendation 4 (E-Mail Alert): On December 20, 2022, we recommended that the Chief, FMSS, coordinate with TIGTA OI to create a singular message instructing employees on processes and procedures for the reporting of assaults and threats.

> **Management's Response to E-Mail Alert:** IRS management agreed with this recommendation and will ensure that the unified message is used in any communication instructing employees on processes and procedures for the reporting of assaults and threats.

Figure 2: TIGTA and IRS Agreed Upon Reporting Instructions for Employee Assaults and Threats



Source: IRS Employee Resources site web page.

Recommendation 5 (E-Mail Alert): On December 20, 2022, we recommended that the Chief, Facilities Management and Security Services, update all internal guidance as well as the IRS Source SharePoint site on the correct methods for employees to notify IRS SAMC and TIGTA OI to report assaults and threats.

Management's Response to E-Mail Alert: IRS management agreed with this recommendation and plans to update all internal guidance as well as the IRS Source SharePoint site on the correct methods for employees to notify IRS SAMC and TIGTA OI to report assaults and threats.

Training and Awareness Can Be Improved to Ensure That Employees and Contractors Know How to Report and Process Assaults and Threats

FMSS security personnel and IRS contractors did not complete required training and awareness briefings on the process employees follow to report assaults and threats. For example:

- Of the 205 FMSS security personnel required to complete training course #71555, *SAMC Incident Reporting*, only two employees completed this course in Fiscal Year 2022. For the remaining 203 individuals, SAMC officials found that course #71555 was not loaded in the profiles as a required training in the IRS's training system.

  Internal guidance requires all FMSS security personnel to complete training course #71555, *SAMC Incident Reporting*, on an annual basis. The purpose of the training is to highlight the importance of employees reporting incidents within the IRS. IRS employees will learn the types of incidents and the proper organizations to report them to, employee responsibilities when reporting an incident, how to identify high-priority threats, how to report an incident to the SAMC, key information for inclusion in an

incident report, and how to report an incident to the SAMC using the automated web link.

- An annual IRS awareness briefing on Physical Security contained comprehensive information on IRS security policies, procedures, and actions employees should take to prepare for and respond to potential security incidents and emergencies, including the requirement to report assaults and threats to the SAMC and TIGTA. A TIGTA Office of Inspections and Evaluations report on Active Shooter Readiness and Training[4] found that 78,266 (98 percent) of 79,865 full-time IRS employees completed this Physical Security awareness briefing for the period July 1, 2021, to June 30, 2022. However, the report also cited that only 71 percent of the 9,315 contractors working at IRS facilities completed the mandatory briefing. Because the Active Shooter report included a recommendation for contractors to complete this training, we will not make that same recommendation. However, it highlighted a potential awareness gap for part of the IRS workforce.

Employees did not always know how to report assaults and threats

During this evaluation, we also visited six Taxpayer Assistance Centers and found that while employees generally knew that they should contact either the SAMC or TIGTA to report assaults and threats, they were not exactly sure on the specifics of how to report to the SAMC or TIGTA. Some expressed that they would contact their manager for guidance while others knew the information was on the IRS Source SharePoint site. During our site visits, we also observed that there were no signs or posters on reporting of assaults and threats that an employee could refer to for guidance.

In addition, another TIGTA Office of Inspections and Evaluations report on the Use of Employee Names on Tax Processing Center Correspondence[5] conducted a survey of managers and employees asking the question, "*Are you aware of the procedures to be followed if a taxpayer threatens or assaults you during the performance of your official duties?*" The project team found that three (10 percent) of 30 respondents stated "*No*."

Lastly, the IRS created a carriable emergency card and a smaller detachable card for a key ring that contains instructions for reporting physical security incidents to both TIGTA OI and the SAMC. Prior to our site visits, we were unaware that these cards existed, but no employees showed us these cards during our site visits.

The Chief, FMSS, should:

Recommendation 6: Work with the Employee Development team to ensure that course #71555, *SAMC Incident Reporting*, is added to the profiles of all FMSS Section security chiefs, physical security specialists, and physical security assistants as required training annually in the IRS's training system and develop a process to track the completion of the course.

[4] TIGTA, Report No. IE-23-R005, *Assessment of the Internal Revenue Service's Active Shooter Readiness and Training* (May 2023).

[5] TIGTA, Report No. IE-23-R004, *Actions Are Being Taken to Reduce Risks to Employees Whose Names Are Required to Be Included on Internal Revenue Service Correspondence* (May 2023).

Management's Response: IRS management agreed with this recommendation and has added Training course #71555 as an annual requirement for all FMSS security section chiefs, physical security specialists, and physical security assistants. Management also plans to track course completions using an automated report from its training system and will e-mail a reminder to employees who have not taken the required training.

Recommendation 7: Submit a Publishing Service Request to develop assault and threat reporting guidance in the form of a poster that can be posted at areas accessible by all employees (nonpublic viewing areas) for IRS offices that interact with taxpayers, and make the pocket-size emergency card available to all field employees who interact with taxpayers.

Management's Response: IRS management agreed with this recommendation and plans to publish an Incident Reporting Banner that will be available for business units to order and post at their locations. Management will send an e-mail to business units alerting them that there is a banner available to order. The existing emergency wallet and key chain cards that include incident reporting information are also available for business units to order for field employees.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the procedures that IRS employees follow to report and process assaults and threats. To accomplish our objective, we:

- Evaluated the procedures established for reporting and processing incidents of assaults and threats and inputting the PDT indicator on taxpayer accounts.
- Evaluated the guidance provided to employees on the reporting of assaults and threats to ensure consistent and accurate instructions are provided.
- Determined whether employee assaults and threats are reported and processed in accordance with established criteria.
- Obtained SAMC, TIGTA OI, and OEP data specific to assaults and threats to employees from October 1, 2019, to November 30, 2022, to evaluate whether applicable incidents were being processed timely, shared appropriately with key stakeholders, and resulted in the timely posting of PDT indicators on taxpayer accounts.
- Determined whether employees are provided with adequate training and awareness to identify and report assaults and threats.

Performance of This Review

This review was performed at the FMSS Headquarters in Lanham, Maryland, the FMSS Watch Standers office in Ogden, Utah, the OEP in Detroit, Michigan; and Taxpayer Assistance Centers in Oakland and Walnut Creek, California; Washington, D.C.; Ogden and Salt Lake City, Utah; and Vienna, Virginia. We conducted this evaluation in accordance with the Council of the Inspectors General for Integrity and Efficiency Quality Standards for Inspections and Evaluations during the period December 2022 through June 2023.

Major contributors to the report were James Douglas, Director; Kent Sagara, Supervisory Evaluator; Michelle Griffin, Lead Evaluator; Esther Wilson, Senior Evaluator; and Matthew Pham, Evaluator.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of data from SAMC, TIGTA OI, and OEP systems. We evaluated the data by 1) matching SAMC and OEP data to TIGTA OI data to ensure that the same incidents were maintained in the systems, 2) reviewing existing information about the data and the system that produced them, and 3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.

Appendix II

Letter to the Internal Revenue Service Commissioner

NTEU
National Treasury Employees Union

August 20, 2022

DELIVERED BY EMAIL

Commissioner Charles Rettig
Internal Revenue Service
1111 Constitution Ave., NW
Washington, D.C., 20224

Dear Commissioner Rettig:

I write regarding the safety and security of IRS employees – which I know is a matter of utmost importance to the IRS and NTEU. You have repeatedly demonstrated your support for the dedication and professionalism of the IRS workforce in your public statements and your willingness to listen to NTEU's concerns. I am sure you are aware of the recent dangerous and false rhetoric by some politicians and others. NTEU and our members are increasingly worried about their safety, and we ask that you immediately take steps to enhance security at IRS facilities and take measures to minimize placing employees in settings where they are at risk.

IRS workers are often targeted due to the nature of their work, which requires close interaction with the public. Too many times in the past, we have seen anti-government, anti-worker statements fuel violent attacks on innocent federal employees. I was sickened to read a report of one political candidate who condoned shooting federal employees, including IRS employees "on sight." These public servants are doing the job that Congress asked of them, and they deserve to be protected.

I request that the IRS undertake a comprehensive review of safety and security measures at all IRS facilities. The review should consider whether each facility has, among other things: the proper risk assessment security level designation; sufficient entry control systems, including guards or other armed presence and magnetometers; sufficient perimeter security; exterior lighting; proper designation of restricted areas; and operable security equipment. The last review of this type was done after the bombing of the Alfred P. Murrah Federal Building in 1995.

I also ask that, for the time being, the IRS minimize the amount of field work by IRS employees while these harmful statements circulate on news outlets and on social media and continue to incite violence against federal employees. Additionally, TIGTA and the Federal Protective Service should step up their efforts to protect IRS employees.

800 K Street, NW, Suite 1000, Washington DC 20001-8022 | (202) 572-5500 | NTEU.org

I appreciate your urgent attention to this matter.

Thank you for your efforts on behalf of the dedicated employees of the IRS.

Sincerely,

Anthony M. Reardon
National President

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF
FACILITIES MANAGEMENT AND
SECURITY SERVICES

August 10, 2023

MEMORANDUM FOR RUSSELL P. MARTIN
DEPUTY INSPECTOR GENERAL FOR INSPECTIONS AND EVALUATIONS

FROM: Richard L. Rodriguez
Chief, Facilities Management & Security Services

Digitally signed by Richard L. Rodriguez
Date: 2023.08.10 14:23:05 -04'00'

SUBJECT: Draft Audit Report – Process, Training, and Awareness Enhancements Can Better Inform Employees on How to Report Taxpayer Assaults and Threats (Evaluation # IE-23-001)

Thank you for the opportunity to review and comment on the draft audit report. We appreciate that your report acknowledged that the IRS took timely actions in response to employee reports of assaults and threats. Your recommendations will assist us in our efforts to ensure accurate and consistent information as to the process for employee reporting of assaults and threats. Your recommendations will also assist us in our efforts to ensure all FMSS Security personnel complete required training on how to report assault and threat incidents.

We agree with your recommendations and have developed corrective actions to remediate the report findings. We have already begun making progress on multiple recommendations. For example, FMSS has already discontinued the use of the facsimile (fax) number and updated IRM 10.2.8 to remove the number as a reporting method. Additionally, FMSS added the IRS Incident Reporting course to the training curriculum for all Security Section Chiefs, Physical Security Specialists and Security Assistants and created a banner to put in IRS buildings to provide incident reporting information.

Attached is our corrective action plan describing how we addressed/plan to address your recommendations.

We appreciate the continued support and assistance provided by your office. If you have any questions, please contact me at 202-317-4480, or a member of your staff may contact Brian Soloman, associate director, Security, Facilities Management and Security Services, at 231-493-8977.

Attachment

Attachment

RECOMMENDATION #1 (E-MAIL ALERT)
On March 1, 2023, we recommended that the Chief Privacy Officer receive notification from TIGTA OI at the time an investigation related to assaults and threats against IRS employees is initiated. Once notified, the PDT indicator should be input immediately on the individual's tax account who assaulted or threatened the IRS employee.

CORRECTIVE ACTION #1
We agree with this recommendation and consider it complete. On April 4, 2023, the Office of Employee Protection (OEP) implemented a process with the TIGTA Office of Investigations (OI) where OEP's information system is updated with notifications of investigation cases each night for immediate input of the PDT indicator.

IMPLEMENTATION DATE
Implemented April 4, 2023

RESPONSIBLE OFFICIAL
Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Director, Privacy Policy and Compliance

RECOMMENDATION #2 (E-MAIL ALERT):
On December 20, 2022, we recommended that the Chief, Facilities Management and Security Services, evaluate whether the SAMC facsimile number is a viable method to report assaults and threats, and based on this decision, either remove references to this number from all reporting instructions and guidance or ensure that the use of this number is to an operational facsimile machine.

CORRECTIVE ACTION #2:
We agree with this recommendation and consider it complete. FMSS discontinued the option for employees to report assaults or threats via fax and removed the number from the Internal Revenue Manual.

IMPLEMENTATION DATE:
Implemented June 14, 2023

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #3 (E-MAIL ALERT):
On December 20, 2022, we recommended that the Chief, Facilities Management and Security Services, identify all existing instructions and guidance on how to report threats and assaults to ensure consistency and accuracy of this guidance.

CORRECTIVE ACTION #3:
We agree with this recommendation and consider it complete. FMSS has worked with Communications and Liaison staff and developed a list of inaccurate information on the reporting of assaults and threats.

IMPLEMENTATION DATE:
Implemented July 27, 2023

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #4 (E-MAIL ALERT):
On December 20, 2022, we recommended that the Chief, Facilities Management and Security Services, coordinate with TIGTA OI to create a singular message instructing employees on processes and procedures for the reporting of assaults and threats.

CORRECTIVE ACTION #4:
We agree with this recommendation and consider it closed. FMSS will ensure the unified message is used in any communication instructing employees on processes and procedures for the reporting of assaults and threats.

IMPLEMENTATION DATE:
Implemented July 25, 2023

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #5 (E-MAIL ALERT):
On December 20, 2022, we recommended that the Chief, Facilities Management and Security Services, update all internal guidance as well as the IRS Source SharePoint site on the correct methods for employees to notify IRS SAMC and TIGTA OI to report assaults and threats.

CORRECTIVE ACTION #5:
We agree with this recommendation. FMSS will update all internal guidance as well the IRS Source SharePoint site on the correct methods for employees to notify IRS SAMC and TIGTA OI to report assaults and threats.

IMPLEMENTATION DATE:
December 15, 2023

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #6:
The Chief, Facilities Management and Security Services, should work with the Employee Development team to ensure that course #71555, SAMC Incident Reporting, is added to the profiles of all FMSS Section security chiefs, physical security specialists, and physical security assistants as required training annually in the IRS's training system and develop a process to track the completion of the course.

CORRECTIVE ACTION #6:
We agree with this recommendation and consider it closed. ITM (Integrated Talent Management) Course #71555 was added as an annual Computer Based Training (CBT) requirement for all FMSS Security Section Chiefs, Physical Security Specialists, and Physical Security Assistants. FMSS will track completion of the course using an automated report from ITM. FMSS will email a reminder to employees that have not taken the required training.

IMPLEMENTATION DATE:
Implemented July 27, 2023

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

RECOMMENDATION #7 :
The Chief, Facilities Management and Security Services, should submit a Publishing Service Request to develop assault and threat reporting guidance in the form of a poster that can be posted at areas accessible by all employees (nonpublic viewing areas) for IRS offices that interact with taxpayers, and make the pocket-size emergency card available to all field employees who interact with taxpayers.

CORRECTIVE ACTION #7:
We agree with this recommendation. FMSS will publish an Incident Reporting Banner that will be available for business units to order and post at their locations. An email will go out to business units alerting them that there is a banner available to order. The existing emergency wallet card and key chain card that includes incident reporting information is available for business units to order from the distribution center to provide to employees.

IMPLEMENTATION DATE:
February 15, 2024

RESPONSIBLE OFFICIAL:
Chief, Facilities Management and Security Services

CORRECTIVE ACTION MONITORING PLAN:
Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

Appendix IV

Abbreviations

FMSS	Facilities Management and Security Services
IRS	Internal Revenue Service
OEP	Office of Employee Protection
OI	Office of Investigations
PDT	Potentially Dangerous Taxpayer
SAMC	Situational Awareness Management Center
TIGTA	Treasury Inspector General for Tax Administration

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.