TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The IRS Timely Processed Threat and Assault Cases, but More Education Would Help Employees Properly Report Incidents

September 1, 2026

Report Number: 2026-IE-R012

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

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

HIGHLIGHTS: The IRS Timely Processed Threat and Assault Cases, but More Education Would Help Employees Properly Report Incidents

Final Evaluation Report issued on September 1, 2026 Report Number 2026-IE-R012

Why TIGTA Did This Evaluation

Most Americans understand the IRS's mission and respect IRS employees who help taxpayers meet their tax obligations.

On occasion, taxpayers may act aggressively and threaten or assault an IRS employee. It is a federal crime to forcibly threaten or assault a federal employee engaged in official duties, particularly those employees involved with the administration of Internal Revenue laws. When this occurs, the IRS places a Potentially Dangerous Taxpayer (PDT) indicator on the individual's tax account. Similarly, when taxpayers file or threaten to file a frivolous legal action or lien against an IRS employee, a Caution Upon Contact (CAU) designator is placed on the taxpayers' account. The CAU is also used when taxpayers threaten suicide during an employee interaction.

We assessed the IRS's processes and procedures to monitor and evaluate taxpayers who pose a threat to IRS employees.

Impact on Tax Administration

Between October 2022 and August 2025, the IRS reported over 1,800 cases involving a threat or assault against an IRS employee. Timely input of PDT indicators on taxpayer accounts helps protect employees who may have subsequent direct contact with these taxpayers.

Furthermore, it is important that IRS employees know how to report threats and assaults to ensure that individuals who commit such actions are timely identified and investigated.

What TIGTA Found

We found that Office of Employee Protection (OEP) personnel input the PDT indicator on most threat and assault perpetrators' tax accounts within the one-day requirement. Of the 1,826 threat and assault cases from October 2022 through August 2025, we found that 1,755 (96 percent) were processed timely. For the remaining 71 (4 percent) cases, we determined that 35 had acceptable reasons for the delayed input of the PDT indicator. However, we found that 36 of the 71 cases involved errors and assignment issues:

- 31 cases were assigned to employees who input the PDT indicator after the one-day requirement. Many of these cases involved multiple cases for the same person.
- 5 cases resulted in delayed input of the PDT indicator because of data entry errors and assignment delays.

In December 2025, the OEP implemented a new system called the Case Management Applications Program. Similar to its predecessor, the new system catalogues information and data about PDT and CAU taxpayer cases. In addition, the new system has enhancements that addressed all the exception cases we identified.

OEP specialists review cases after five years to determine whether the PDT or CAU indicator is still warranted on the taxpayer's account. We found that the OEP properly reviewed and documented its five-year review of PDT cases. The OEP took appropriate actions to either remove the PDT indicator when the threat no longer existed or keep it on a taxpayer's account.

We also made unannounced visits to eight taxpayer-facing IRS sites. The IRS employees we interviewed at those locations did not know about the requirement to notify TIGTA's Office of Investigations (OI) about a threat or assault. The sites we visited also did not display any guidance on how to report assaults and threats.

We issued an email alert describing these concerns to the appropriate IRS officials. The IRS subsequently took corrective actions.

IRS officials shared that the IRS had improved its processes for reporting assaults and threats based on a previous report we issued. For example, the OEP implemented a process with TIGTA OI, which instructs OEP personnel to input the PDT indicator on taxpayer accounts nightly and to clarify reporting guidance.

What TIGTA Recommended

Based on actions taken during our evaluation, we made no recommendations in this report.

TREASURY INSPECTOR GENERAL
for Tax Administration

DATE: September 1, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Nancy A. LaManna
Deputy Inspector General for Inspections and Evaluations

SUBJECT: Final Evaluation Report – The IRS Timely Processed Threat and Assault Cases, but More Education Would Help Employees Properly Report Incidents (Evaluation No. IE-25-021-I)

This report presents the results of our review to assess the Internal Revenue Service's (IRS) processes and procedures to monitor and evaluate taxpayers who pose a threat to IRS employees. This review also included evaluating actions the IRS took to address recommendations from a prior TIGTA evaluation. This review is part of our Fiscal Year 2026 Annual Program Plan and addresses the major management and performance challenge of *Managing a Reduced Workforce and Budget.*

No recommendations were made in this report.

If you have any questions, please contact me or Kent Sagara, Director.

Table of Contents

Background

Most Americans understand the Internal Revenue Service's (IRS) mission and respect IRS employees who help taxpayers meet their tax obligations. On occasion, taxpayers may act aggressively and threaten or assault an IRS employee.

Internal Revenue Code § 7212 and 18 U.S.C. § 111 state that it is a federal crime to forcibly threaten or assault a federal employee engaged in official duties, particularly those employees involved with the administration of Internal Revenue laws. In addition, TIGTA has jurisdiction to investigate allegations involving attempts to interfere with or impede tax administration and actions designed to harass IRS employees.

Individuals who threaten or assault IRS employees are generally designated as Potentially Dangerous Taxpayer (PDT) and Caution Upon Contact (CAU). The PDT designation refers to individuals who have demonstrated hostile behavior and could be a threat when an IRS employee contacts them again. The CAU designation is typically used when taxpayers file or threaten to file a frivolous legal action or lien against an IRS employee. The CAU is also used when taxpayers threaten suicide during an employee interaction.

The IRS has processes and procedures for its employees to report taxpayer assaults and threats. Specifically, IRS employees are required to report threat and assault incidents to the:

- IRS Facilities Management and Security Services' (FMSS) Situational Awareness Management Center (SAMC).
- Treasury Inspector General for Tax Administration's Office of Investigations (TIGTA OI).

IRS personnel must report physical security incidents to the SAMC within 30 minutes of incident discovery or identification, or when it is safe to do so. For assault, threat, or forcible-interference incidents, employees must also immediately report the matter to TIGTA OI and notify their manager. IRS personnel can report these incidents via the intranet, email, or telephone. Reporting these incidents to the SAMC allows the IRS to identify and track perpetrators and alert other employees who may engage with these individuals. Reporting to TIGTA OI allows the timely investigation of these individuals.

TIGTA OI forwards threat or assault case information to the Office of Employee Protection (OEP). Through a secured interface, information is electronically transmitted nightly from TIGTA OI to the OEP's Employee Protection System Database (referred to as e-Trak). The IRS uses the e-Trak database to track information about PDT and CAU cases. The e-Trak database tracks information related to when the case was assigned to the OEP and the details of the incident involved. In December 2025, the OEP transitioned from e-Trak to a new system called the Case Management Applications Program (CMAP). The SAMC separately receives and distributes physical security incident reports to appropriate stakeholders based on the SAMC notification matrix.

When OEP specialists receive a notification from TIGTA OI, they place a PDT indicator on the individual's tax account within 24 hours of receipt. The PDT indicator is in "pending" status while TIGTA OI conducts an investigation.

TIGTA OI documents its results in a Report of Investigation (ROI), which is shared with the OEP. Personnel within the OEP review the ROI to determine whether the pending PDT indicator should remain on the taxpayer's account. If confirmed, the pending status is removed, and the PDT indicator remains on tax accounts. OEP personnel also may change the pending PDT indicator to a CAU indicator if the threat against the employee is less severe. Figure 1 lists additional criteria the IRS uses to make PDT and CAU designations.

Figure 1: Criteria the IRS Uses to Make PDT and CAU Designations

Criteria for Potentially Dangerous Taxpayer Designation

- Physical assault of an IRS employee, former employee, contractor, an immediate family member of an IRS employee, or a former employee or contractor;
- Intimidating or threatening an IRS employee, contractor, an immediate family member of an IRS employee, or a former employee or contractor through specific threats of bodily harm, a show of weapons, the use of animals, or through specific threatening behavior (e.g., stalking, etc.);
- Members of or affiliation with groups that advocate violence against IRS employees, where advocating such violence could reasonably be understood to threaten the safety of employees or impede their duties;
- Advocates of violence against IRS employees where advocating such violence could reasonably be understood to threaten the safety of employees or impede their duties;
- Any individual who has committed the acts in any of the preceding criteria, but whose acts have been directed against employees or contractors of other governmental agencies; or
- Any individual who is not classified as a PDT, but whose acts within the past 10 years have demonstrated a propensity for violence.

> Within the Past 10 Years <

Criteria for Caution Upon Contact Designation

- Threats of harm that is less severe or immediate than necessary to satisfy PDT criteria;
- Any individual who has threatened suicide;
- Any individual who has filed or threatened to file a frivolous lien or frivolous civil or criminal legal action against an IRS employee, a former employee, a contractor, or an immediate family member of an IRS employee, former employee, or contractor.

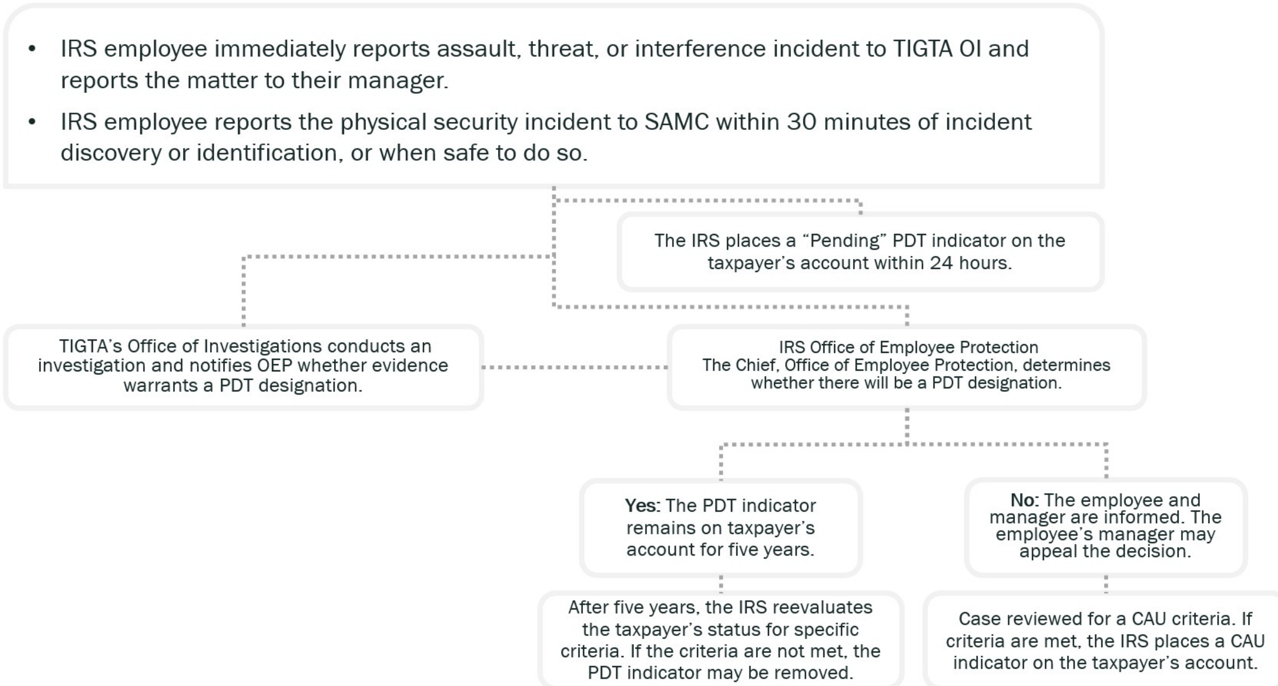
> Within the Past 10 Years <

Source: The Internal Revenue Manual.

OEP specialists review cases after five years to determine whether the PDT or CAU indicator is still warranted on the taxpayer's account.[1] Figure 2 identifies the IRS process for reporting threats and assaults.

[1] For PDT cases, TIGTA OI provides investigative assistance as the OEP evaluates whether the PDT indicator should be renewed on a taxpayer's account.

Figure 2: IRS Process for Reporting PDTs



Source: The Internal Revenue Manual.

According to OEP officials, when an IRS employee has an in-person meeting scheduled with a taxpayer who has a PDT or CAU indicator on their tax account, the employee can request an armed escort from TIGTA OI.

This evaluation also followed up on recommendations in our September 2023 report. That report evaluated IRS processes that employees followed to report threats and assaults to appropriate stakeholders.[2]

Results of Review

In our September 2023 report, we found that OEP specialists took an average of 30 calendar days from the date of the incident to post indicators on the tax accounts of 772 PDT cases from October 2019 through November 2022. However, this evaluation found that OEP personnel timely input the PDT indicator on most threat and assault perpetrators' taxpayer accounts within the one-day requirement. Of the 1,826 threat and assault cases from October 2022 through August 2025, we found that:

- 1,755 (96 percent) were processed timely.
- 71 (4 percent) were processed outside the one-day reporting requirement. Most of these 71 cases resulted from OEP personnel making erroneous updates in the e-Trak database.

[2] TIGTA, Report No. 2023-IE-R009, *Process, Training, and Awareness Enhancements Can Better Inform Employees on How to Report Taxpayer Assaults and Threats* (September 2023).

However, we continued to find that some IRS taxpayer service representatives did not know the complete process for reporting threat and assault incidents. Although these taxpayer service representatives knew about the requirement to report threat and assault incidents to the SAMC, none of them knew they were also required to notify TIGTA OI.

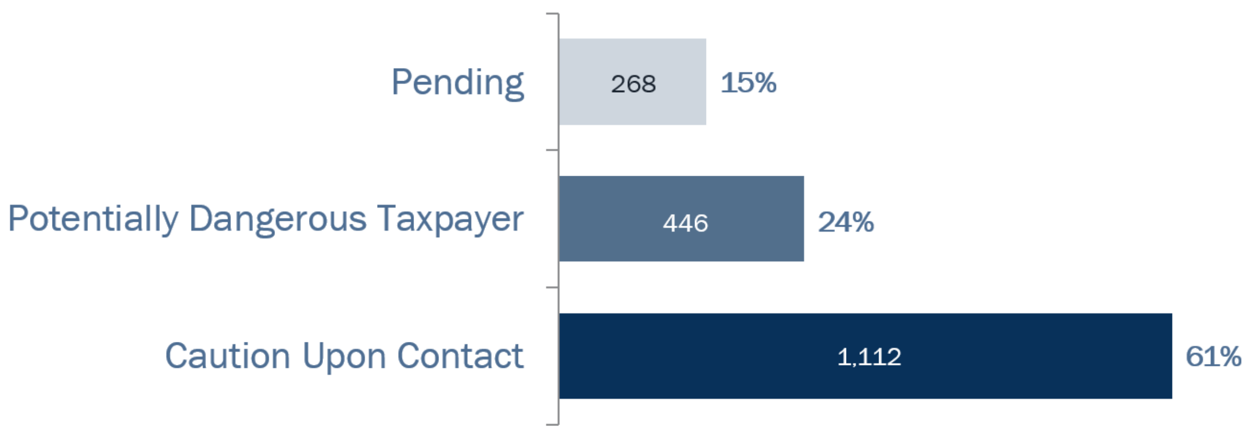
IRS officials shared that the IRS improved its processes for reporting assaults and threats based on a prior TIGTA recommendation. Specifically, the OEP implemented a process with TIGTA OI, which instructs OEP personnel to input the PDT indicator on taxpayer accounts nightly and to clarify reporting guidance. We also recommended that the IRS post guidance on how to report threats and assaults in IRS offices that interact with taxpayers. However, the sites we visited did not display any awareness materials on how to report assaults and threats.

Threat and Assault Cases From the IRS's e-Trak Database Analyzed

We analyzed all PDT cases in the e-Trak database from October 2022 through August 2025. The total number of cases in e-Trak as of August 2025 was 1,826 (see Figure 3). Of that amount:

- 446 were PDT cases.
- 1,112 were PDT cases that converted to CAU cases.
- 268 pending cases were not designated as either PDT or CAU. Since the OEP was still reviewing ROIs related to these incidents, the e-Trak case status was predominantly listed as "PDT Awaiting ROI" or "PDT ROI Received."

Figure 3: Case Status From October 2022 Through August 2025



Source: TIGTA analysis based on e-Trak data.

Indicators Timely Placed on Most Threat and Assault Perpetrators' Tax Accounts

We found that OEP personnel input the PDT indicator on most threat and assault perpetrators' tax accounts within the one-day requirement. Of the 1,826 threat and assault cases from Fiscal Years 2022 through 2025, there were 1,755 (96 percent) that met the one-day requirement. In addition, we found that the OEP properly reviewed and documented its five-year review of PDT cases. The OEP took appropriate actions to either remove the PDT indicator when the threat no longer existed or maintain it on a taxpayer's account.

For the remaining 71 (4 percent) cases, we determined that 35 had acceptable reasons for the delayed input of the PDT indicator. For example, 12 cases occurred during the three-week period from December through January ("dead cycle") when the system used to post PDT indicators to taxpayer accounts is offline due to yearly changes to the system.[3] In addition, some cases were received on a Friday, and the PDT indicator was input the following Monday. Lastly, some cases involved mistaken identities and required additional research or information.

However, we found that 36 of the 71 cases involved errors and assignment issues. We analyzed and discussed the 36 cases that had errors and assignment issues with OEP officials and found that:

- 5 cases resulted in delayed input of the PDT indicator.
- 31 cases showed an assignment date that was after the PDT input date.

Cases involving delayed input of the PDT indicator

The five cases with delayed input of the PDT indicator were caused by e-Trak entry errors and assignment delays. Figure 4 presents IRS explanations for the five cases where the OEP input the PDT indicator on an alleged perpetrator's taxpayer account more than one day after the required date.

Figure 4: IRS Explanations for Cases Involving Delayed Input of a PDT Indicator

Reason	Taxpayers Impacted
PDT Origination Date entered incorrectly in e-Trak by OEP specialist.	**3**
[redacted]	[redacted]
[redacted]	[redacted]

Source: TIGTA analysis of OEP responses.

Cases showing an assignment date after the PDT input date

We identified 31 cases showing an assignment date that was after the PDT input date. Many of these cases involved multiple cases for the same person. For example, in 21 of the cases, a second referral (*i.e.*, another incident) was received on a taxpayer, and the assignment date was changed to the second referral date instead of keeping the first incident assignment date. In 10 of the cases, the assigned date was incorrectly changed. Figure 5 presents IRS explanations for the 31 cases where the OEP assignment date was after the PDT input date.

[3] While the OEP waits for the input of the PDT indicator during the "dead cycle," there are processes and procedures to notify IRS employees of potentially dangerous taxpayers.

Figure 5: IRS Explanations for Cases Involving an Assigned Date Appearing After the PDT Input Date

Reason	Taxpayers Impacted
Received multiple cases and assigned date was erroneously changed by OEP specialist.	21
Case was reassigned and the assigned date was incorrectly changed by the new OEP specialist.	10

Source: TIGTA analysis of OEP responses.

[redacted]:

- [redacted].
- [redacted].
- [redacted].
- [redacted].

[redacted].

For the 10 instances where the assigned date was incorrectly changed, IRS officials stated that discrepancies occurred when e-Trak systemically changed the assigned date after a case was reassigned to a different OEP specialist.

[redacted]:

- [redacted].
- [redacted].

According to IRS policies and procedures, OEP specialists are required to input "pending" PDT indicators on an individual's tax account within 24 hours of receiving a threat or assault incident. Each PDT case is held in a pending status until the OEP receives the ROI from TIGTA OI. Once the ROI is received, OEP specialists review the report and make a recommendation to the Chief, OEP. The Chief, OEP, then decides whether a taxpayer meets PDT criteria.

Incorrect case information can affect the timeliness and accuracy of each case, including when a case undergoes the five-year review. In addition, inaccurate case information could inadvertently affect taxpayer's rights if the PDT indicator is on the taxpayer's account longer than necessary.

On December 16, 2025, the OEP implemented a new system called the CMAP to replace e-Trak. Similar to e-Trak, the CMAP catalogues information and data about PDT and CAU taxpayer cases. The IRS developed the CMAP system in-house using the e-Trak database. According to OEP officials, the CMAP addressed a previously known issue of incorrectly changing the assigned date in certain situations, such as when a case is transferred to another OEP specialist. We verified that the CMAP's systemic enhancements over the e-Trak system addressed the exceptions we identified above. As a result, we made no recommendations in this report.

Some Taxpayer Service Representatives Were Not Aware of the Requirement to Notify TIGTA About Threat and Assault Incidents

In August 2025, we made several unannounced visits to a judgmental selection of eight Taxpayer Assistance Centers (TAC) in the Washington, D.C., area.[4] We wanted to determine whether taxpayer service representatives knew how to report threat and assault incidents.

During our inspections, we found that some taxpayer service representatives knew to report incidents to the SAMC, but none of them knew about the requirement to notify TIGTA OI. For example, at one TAC, a taxpayer service representative reported an incident that occurred in the past year to the manager instead of to the SAMC or TIGTA OI.

IRS policies and procedures require employees to report physical security incidents to the SAMC within 30 minutes of incident discovery or identification, or when safe to do so. For assaults, threats, or forcible-interference, employees must immediately report to TIGTA OI and report the matter to the SAMC. IRS employees, especially those who have direct contact with the public, should be fully aware of the proper procedures for reporting threats and assaults. This helps to ensure employee safety and protection. In addition, if TIGTA OI is not timely notified about threat and assault incidents, it could impede their ability to protect IRS employees and fulfill investigatory responsibilities.

In our September 2023 report, we noted that IRS employees did not always know how to report threats and assaults. We recommended that the IRS develop a poster with information about assault and threat reporting. The poster was to be placed in areas accessible by all employees at IRS offices where employees interact with taxpayers. The IRS agreed with this recommendation and developed IRS Publication 5825, *Incident Reporting*. The agency also developed IRS Publication 5825-A, *Incident Reporting*, which is a banner and poster that directs IRS employees to report incidents to the SAMC and TIGTA OI. Figure 6 illustrates the incident-reporting banner.

[4] We conducted site visits at TACs in Washington, D.C.; Annapolis, Baltimore, Frederick, Landover, and Rockville, Maryland; and Fredericksburg, and Vienna, Virginia.

Figure 6: IRS Publication 5825-A, *Incident Reporting*

Source: IRS.gov.

However, during our on-site inspections, we did not observe incident-reporting posters or banners at any of the TAC locations. Further, taxpayer service representatives at the TACs did not know that incident-reporting publications existed. According to FMSS officials, incident-reporting publications are internal job aids, not policy mandates. Further, the banner and poster were not distributed to any of the TACs or other IRS offices. However, several taxpayer service representatives we interviewed stated that the posters and banners would be useful and expressed interest in obtaining one for display in their office.

In August 2025, we issued an email alert to the FMSS. We expressed our concerns about incident-reporting publications not being on display at TACs, and employees' lack of knowledge about how to report threats and assaults. We recommended that the FMSS increase awareness of incident-reporting publications posted at TACs and other IRS offices where employees are in frequent communication with taxpayers. The FMSS agreed with our recommendation and coordinated with the IRS's Media and Publishing division to create a flyer-sized, locally printable version of the incident-reporting publication.

In December 2025, the FMSS notified the IRS's Taxpayer Services division about the flyer being available to print and then post in TACs. In January 2026, the FMSS also published an article in the *IRS Source*—the agency's internal newsletter.

IRS officials also shared that the IRS improved its processes for reporting assaults and threats based on a previous TIGTA recommendation. Specifically, the OEP implemented a process with TIGTA OI, which instructs OEP personnel to input the PDT indicator on taxpayer accounts nightly and to clarify reporting guidance.

Since IRS took these corrective actions in response to the email alert, we made no further recommendations.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this review was to assess the IRS's processes and procedures to monitor and evaluate taxpayers who pose a threat to IRS employees. This review also included evaluating actions the IRS took to address recommendations from a prior TIGTA evaluation. To accomplish our objective, we:

- Interviewed OEP employees about the processes followed when placing PDT or CAU indicators on taxpayer accounts.
- Obtained and reviewed data from the e-Trak database related to PDT and CAU cases that occurred from October 1, 2022, through August 14, 2025.
- Assessed whether the indicators that OEP employees placed were timely and complete.
- Reviewed the Department of the Treasury's Joint Audit Management Enterprise System report associated with TIGTA Evaluation No. IE-23-001 (*i.e.*, TIGTA Report No. 2023-IE-R009), to assess IRS corrective actions taken on TIGTA's recommendations.
- Performed unannounced site visits to TACs and interviewed IRS taxpayer service representatives.

Performance of This Review

This review was performed at the OEP in Detroit, Michigan. We also conducted site visits at TACs in Washington, D.C.; Annapolis, Baltimore, Frederick, Landover, and Rockville, Maryland; and Fredericksburg, and Vienna, Virginia. Our review occurred from July 2025 through May 2026. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.* Those standards require that the work adheres to the professional standards of independence, due professional care, and quality assurance and followed procedures to ensure accuracy of the information presented. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Data Validation Methodology

We performed tests to assess the reliability of data from the e-Trak database. We evaluated the data by performing electronic testing of required data elements and interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.

Appendix II

Abbreviations

CAU	Caution Upon Contact
CMAP	Case Management Applications Program
FMSS	Facilities Management and Security Services
IRS	Internal Revenue Service
OEP	Office of Employee Protection
OI	Office of Investigations
PDT	Potentially Dangerous Taxpayer
ROI	Report of Investigation
SAMC	Situational Awareness Management Center
TAC	Taxpayer Assistance Center
TIGTA	Treasury Inspector General for Tax Administration

To report fraud, waste, or abuse, contact our hotline on the web at https://www.tigta.gov/reportcrime-misconduct.

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.