



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

25.4.1

MARCH 21, 2025

EFFECTIVE DATE

(03-21-2025)

PURPOSE

- (1) This transmits revised IRM 25.4.1, Employee Protection, Potentially Dangerous Taxpayer.

MATERIAL CHANGES

- (1) 25.4.1.1 (3) Added Policy Owner to Program Scope and Objectives
- (2) 25.4.1.1 (5) Added Primary Stakeholders to Program Scope and Objectives
- (3) 25.4.1.1.1(3) Moved OEP Mission from Program Scope and Objectives to Background
- (4) 25.4.1.1.1 Added IRM Internal Control Component, Authority
- (5) 25.4.1.1.3 Changed IRM Internal Control Component Title from PDT Program Roles to Roles and Responsibilities
- (6) 25.4.1.1.4 Added IRM Internal Control Component, Program Controls
- (7) 25.4.1.1.7 (1) Updated OEP Knowledge Base site link
- (8) 25.4.1.3 (1) Updated OEP Knowledge Base site link

EFFECT ON OTHER DOCUMENTS

This material supersedes IRM 25.4.1, dated March 16, 2021.

AUDIENCE

All Business Operating and Functional Divisions with employees whose duties require them to have contact with taxpayers.

Thomas E. Burger
Director, Privacy Policy & Compliance
Privacy, Governmental Liaison & Disclosure (PGLD)

25.4.1

Potentially Dangerous Taxpayer

Table of Contents

25.4.1.1 Program Scope and Objectives

25.4.1.1.1 Background

25.4.1.1.2 Authority

25.4.1.1.3 Roles and Responsibilities

25.4.1.1.3.1 OEP's Role

25.4.1.1.3.2 TIGTA's Role

25.4.1.1.4 Program Controls

25.4.1.1.5 Terms and Acronyms

25.4.1.1.6 Related Resources

25.4.1.2 The PDT Program

25.4.1.3 Reporting to TIGTA

25.4.1.4 PDT Determination and Appeal

25.4.1.5 PDT Indicator

25.4.1.6 PDT Indicator versus CAU Indicator

25.4.1.7 Power of Attorney (POA) Information

25.4.1.8 Five-Year Review of PDT Records

Exhibits

25.4.1-1 Display of PDT Indicator

25.4.1.1
(03-21-2025)
Program Scope and Objectives

- (1) **Purpose:** This IRM section provides information on OEP and describes the Potentially Dangerous Taxpayer (PDT) program and PDT reporting process.
- (2) **Audience:** The information and procedures in this IRM apply to all IRS employees with duties requiring taxpayer contact.
- (3) **Policy Owner:** The Privacy Policy and Compliance (PPC) Director is responsible for the policy in this IRM. PPC is under the Office of Privacy, Governmental Liaison and Disclosure (PGLD), which is under the Office of the Deputy Commissioner for Operations Support (OS).
- (4) **Program Owner:** The Chief, Office of Employee Protection, reports to the Associate Director, Incident Management and Employee Protection, and oversees the PDT program.
- (5) **Primary Stakeholders:** All employees and contractors of the IRS, in all divisions and functional units, including Flexiplace (Telework) employees (Frequent, Recurring and Ad Hoc) and Mobile employees, are affected by the procedures in this IRM.
- (6) **Program Office Contact Information:** To recommend changes to this IRM, see IRM 1.11.6.6, Providing Feedback About an IRM Section - Outside of Clearance, and send your suggestions to the *PGLD OEP mailbox.

25.4.1.1.1
(03-21-2025)
Background

- (1) In 1984, the IRS Commissioner assigned IRS Inspection the responsibility of developing a program to improve the Service's ability to identify taxpayers who represent a potential danger to employees. Inspection developed the **Potentially Dangerous Taxpayer** (PDT) program, which included the PDT System database. Inspection was then given responsibility for administering the program.
- (2) Inspection became the Treasury Inspector General for Tax Administration (TIGTA) in 1999. Most of Inspection's previous duties, including the administration of the PDT program, were transferred to TIGTA. Due to TIGTA's statutory role and responsibilities, however, it was agreed that the administration and maintenance of the PDT program be transferred back to the IRS. IRS established the Office of Employee Protection (OEP) in February 2000 to administer and maintain the PDT program and fulfill other employee safety recommendations. TIGTA, however, retains its investigatory role in the PDT program.
- (3) **Office of Employee Protection (OEP) Mission:** To effectively administer programs tracking potentially dangerous taxpayers and those taxpayers that should be approached with caution.

25.4.1.1.2
(03-21-2025)
Authority

- (1) This IRM has been developed in accordance with IRS Restructuring and Reform Act of 1998 (RRA98) and IRS 6103(d).

25.4.1.1.3
(03-21-2025)
Roles and Responsibilities

- (1) The following subsections detail OEP's and TIGTA's specific roles and responsibilities within the PDT program.

25.4.1.1.3.1
(12-17-2020)
OEP's Role

- (1) OEP administers the PDT program by:
- Reviewing and analyzing TIGTA's Reports of Investigation (ROI's)
 - Making a determination as to whether or not PDT criteria have been met
 - Inputting and removing the PDT indicator to and from the Integrated Data Retrieval System (IDRS) Master File and/or Non-Master File accounts
 - Maintaining the PDT section of the Employee Protection System (EPS) e-Trak Database
 - Functioning as liaison with General Legal Services (GLS)
 - Providing information and feedback to referring employees and their respective IRS managers
 - Performing PDT five-year reviews

25.4.1.1.3.2
(12-17-2020)
TIGTA's Role

- (1) TIGTA's PDT program role is to:
- Review the facts of the incident
 - Initiate a PDT case
 - Conduct an investigation
 - Forward the ROI to OEP

25.4.1.1.4
(03-21-2025)
Program Controls

- (1) Business Units are responsible for establishing and documenting the program controls developed to oversee their program as well as ensuring employee compliance with all applicable elements of this IRM.

25.4.1.1.5
(03-21-2025)
Terms and Acronyms

- (1) The following terms and definitions are provided to clarify terminology used in the PDT program:
- a. **Assault:** Direct physical contact, with the intent to cause physical harm, including striking or attempting to strike with objects, such as rocks or bottles, or brandishing a weapon.
 - b. **Threat:** Verbal or written expression of intent to cause harm to an IRS employee or contractor or to an IRS employee's or contractor's immediate family member. It also includes preventing an IRS employee or contractor from leaving a taxpayer's business or residence, even if no physical contact actually occurs.
 - c. **Intimidate:** Action intended to cause an IRS employee or contractor to become timid, or to force or deter an IRS employee or contractor from taking actions.
 - d. **Nexus to Tax Administration:** A taxpayer who has some type of open activity or reasonable prospect of future activity on their or their business's IDRS Master File or Non-Master File account, or a taxpayer who, even one with no open activity or reasonable prospect of future activity, initiates contact with the Service or any other tax administration authority.
- (2) The following table contains definitions for the acronyms used in this IRM:

| Acronym | Definition |
|---------|--------------------------------|
| CAU | Caution Upon Contact |
| CAF | Centralized Authorization File |

| Acronym | Definition |
|---------|---|
| EIN | Employer Identification Number |
| EPS | Employee Protection System |
| GLS | General Legal Services |
| IDRS | Integrated Data Retrieval System |
| IRM | Internal Revenue Manual |
| IRS | Internal Revenue Service |
| OEP | Office of Employee Protection |
| PGLD | Privacy, Governmental Liaison & Disclosure |
| POA | Power of Attorney |
| PDT | Potentially Dangerous Taxpayer |
| ROI | Report of Investigation |
| SSN | Social Security Number |
| TIGTA | Treasury Inspector General for Tax Administration |

25.4.1.1.6
(03-21-2025)

Related Resources

- (1) The following resources have additional information on OEP and the PDT program:
 - OEP Knowledge Base site at: *Office of Employee Protection (OEP)*
 - Document 12855, Office of Employee Protection (OEP) Spotlight on Safety
 - Document 12963, A Guide to the Office of Employee Protection (OEP) Programs

25.4.1.2
(12-17-2020)

The PDT Program

- (1) The designation of Potentially Dangerous Taxpayer (PDT) must be based on verifiable evidence or information. There must also be a nexus to tax administration.
- (2) Taxpayers must be identified by Social Security Numbers (SSN) and/or Employer Identification Numbers (EIN).
- (3) Association with a PDT or membership in a group, some of whose members advocate violent protest against our tax system, does not by itself fulfill the criteria for designation as a PDT.
- (4) The following criteria have been established for determining PDT status. The behavior/activity/incidents at issue must have occurred within the ten-year period immediately preceding the time of classification as potentially dangerous:

- Criteria # 1) Individuals who, within the past 10 years, have physically assaulted an IRS employee, a former employee, a contractor, or an immediate family member of an IRS employee, a former employee or a contractor;
- Criteria # 2) Individuals who, within the past 10 years, have intimidated or threatened an IRS employee, a former employee, a contractor, or an immediate family member of an IRS employee, a former employee, or a contractor through specific threats of bodily harm, a show of weapons, the use of animals, or through specific threatening behavior (e.g., stalking, etc.);
- Criteria # 3) Individuals who, within the past 10 years, have been members of, or affiliated with groups that advocate violence against IRS employees, where advocating such violence could reasonably be understood to threaten the safety of Service employees or impede the performance of Service duties;
- Criteria # 3b) Individuals who, within the past 10 years, have advocated violence against IRS employees where advocating such violence could reasonably be understood to threaten the safety of Service employees and/or impede the performance of Service duties;
- Criteria # 4) Individuals who, within the past 10 years, have committed the acts set forth in any of the preceding criteria, but whose acts have been directed against employees or contractors of other governmental agencies; or
- Criteria # 5) Individuals who are not classified as PDT's through application of the above criteria, but whose acts within the past 10 years have demonstrated a propensity for violence.

Note: The preceding criteria were approved by Chief Counsel. Adherence to the criteria is essential to ensure compliance with the Privacy Act. If a particular situation represents a borderline case in the application of the above criteria, the determination should be made in favor of the PDT designation (erring on the side of caution) for the protection of Service employees.

25.4.1.3
(03-21-2025)
Reporting to TIGTA

- (1) Employees will promptly report assaults, threats, harassment, or forcible interference incurred during, or related to, the performance of official duties to their local Treasury Inspector General for Tax Administration (TIGTA) office. Visit the Office of Employee Protection (OEP) website at *Office of Employee Protection (OEP)* for TIGTA Field Division contact information.
- (2) Employees will report the incident to TIGTA if a threat to Service personnel is believed to exist, even if the information does not meet the established criteria.
- (3) Employees will report information to TIGTA about individuals who are dangerous, but where no specific incident has occurred involving an IRS employee, e.g., the taxpayer was recently convicted of assault, if there is a relevance to tax administration.

25.4.1.4
(12-17-2020)
PDT Determination and Appeal

- (1) The Chief, Office of Employee Protection is to make all PDT determinations.
- Note:** In instances where the Chief, Office of Employee Protection determines that a case does not meet any PDT or CAU criteria, the case is sent to the Associate Director, Incident Management and Employee Protection, for concurrence.

- (2) Cases determined to not meet PDT criteria can be appealed by the referring employee's IRS Manager.
- (3) The referring employee's IRS Manager must contact the Chief, Office of Employee Protection, either in writing or by telephone, to discuss the reasons for disagreement.
- (4) If an agreement is not reached between the Chief, Office of Employee Protection and the employee's IRS Manager, the Chief, Office of Employee Protection will forward the appeal to GLS. GLS will make a final decision on the determination.

Note: The information that is sent to GLS, in order for a final determination to be made, includes the ROI received from TIGTA, all IDRS research, and the case write-up completed by the assigned OEP Specialist.

- (5) Cases initiated by TIGTA that result in a "No PDT" determination can be appealed by the referring TIGTA Special Agent-In-Charge.
- (6) In order for TIGTA to appeal a "No PDT" determination, the TIGTA Special Agent-In-Charge must contact the Chief, Office of Employee Protection. If an agreement on the determination cannot be reached, the Chief, Office of Employee Protection will forward the appeal to GLS. GLS will make a final decision on the determination.

25.4.1.5
(03-16-2021)
PDT Indicator

- (1) Input and removal of the PDT indicator to IDRS is restricted to OEP.
- (2) Input of the PDT indicator will result in "PDT" appearing on the systems and documents listed in Exhibit 25.4.1-1.

Note: When an IRS employee discovers a PDT indicator on a taxpayer's account and that employee is unaware of why the taxpayer was designated as a PDT, the IRS employee may utilize the link to OEP's EPS e-Trak Database at: *e-Trak* The IRS employee is to enter the taxpayer's SSN into the SSN search field. The taxpayer's information will appear along with the PDT criteria met. If an IRS employee does not have access to a computer to utilize OEP's EPS e-Trak Database, the IRS employee may contact OEP to obtain background information on the reason(s) for the PDT designation. IRS employees may contact OEP by calling OEP's main line at (313) 234-2490 or sending a secure message to OEP's mailbox *PGLD OEP.

25.4.1.6
(12-17-2020)
**PDT Indicator versus
CAU Indicator**

- (1) If a PDT case meets Caution Upon Contact (CAU) criteria rather than PDT criteria:
 - a. The Chief, Office of Employee Protection will make a "No PDT" determination on the PDT case.
 - b. The referring employee's IRS Manager will be notified of the "No PDT" determination and the intent of initiating a CAU case.
 - c. Once the PDT case is closed, an OEP Specialist will initiate a CAU case.
 - d. The Chief, Office of Employee Protection will make a "Yes CAU" determination on the CAU case.
 - e. The referring employee and his/her manager will be notified of the CAU determination.

25.4.1.7
(01-26-2021)

**Power of Attorney (POA)
Information**

- (1) An IRS employee, who is assigned a case for which there is a POA and there will be contact with that POA, has a "business need to know" whether the POA has been designated as a PDT or CAU. The IRS employee can utilize IDRS to ascertain whether the POA has been designated as a PDT or a CAU, just as the IRS employee does for any taxpayer, as long as the IRS employee does not access any of the POA's other tax information.
- (2) IDRS Command Code "ENMOD" can be used to determine if the POA has been designated as either a PDT or a CAU. If an IRS employee does not know the POA's SSN and/or EIN needed to utilize "ENMOD", he/she can use Command Codes "NAMES" or "NAMEI" to obtain the POA's SSN - OR - "NAMEE" or "NAMEB" to obtain the POA's EIN. For assistance in using these Command Codes, please consult the "IRS Processing Codes and Information" handbook (Document 6209) or other IDRS resources.
- (3) If an IRS employee is unable to determine if the POA has been designated as either a PDT or a CAU utilizing IDRS, the IRS employee may utilize the link to OEP's EPS e-Trak Database at: *e-Trak*. The IRS employee is to enter the POA's Centralized Authorization File (CAF) number into the CAF Number search field.
 - a. If the POA has been designated as a PDT or CAU, or if a case on the POA is in Pending status, the POA's information will appear, along with the PDT or CAU criteria met.
 - b. If the POA has not been designated as a PDT or CAU, or if there are no cases on the POA in Pending status, no information will appear.
- (4) If an IRS employee does not have access to a computer to utilize IDRS or OEP's EPS e-Trak Database, the IRS employee may contact OEP. The IRS employee will give the POA's name, address and CAF number to an OEP Specialist who will utilize OEP's EPS e-Trak Database and determine if the POA has been designated as either a PDT or a CAU.

25.4.1.8
(12-17-2020)

**Five-Year Review of PDT
Records**

- (1) A PDT indicator will remain on a taxpayer's IDRS Master File and/or Non-Master File account for five years, at which time, the status will be reevaluated by an OEP Specialist.
- (2) Any taxpayer, who has been designated as a PDT and meets one or more of the following renewal criteria, will retain the PDT indicator for an additional five-year period:
 - a. An additional PDT referral was made during the five-year period under review;
 - b. The PDT offense was a physical assault on an IRS employee or contractor;
 - c. An arrest by TIGTA or other law enforcement agencies, for a threat to or an assault on an IRS employee or contractor, occurred during the five-year period under review; or
 - d. There is current IRS activity at the time of the review.
- (3) If the taxpayer does not meet the above renewal criteria, an OEP Specialist will remove the PDT indicator from that taxpayer's IDRS Master File and/or Non-Master File account.

Exhibit 25.4.1-1 (12-17-2020)**Display of PDT Indicator**

Once a designation has been made, the PDT indicator will appear in the upper right-hand section of the following documents and systems:

- National Computing Center (NCC) Transcripts (except Privacy Act Transcripts)
- Microfilm Replacement System (MRS) Transcripts
- Audit Information Management System (AIMS)
 - AIMS Display (AMDIS)
 - AIMS Weekly Updates
 - AIMS Charge-Out (Form 5546)
- Federal Tax Deposit (FTD) Alerts (BMF only)
- Integrated Data Retrieval System (IDRS) Transcripts
 - Tax Modules (TXMOD)
 - Entity Modules (ENMOD)
 - Summary Modules (SUMRY)
 - Taxpayer Delinquent Inquiry (TDINQ)
- Corporate Files On Line (CFOL) Modules
 - Individual Master File On Line (IMFOL)
 - Business Master File On Line (BMFOL)
 - Information National On Line Entity (INOLE)
- Balance Due Accounts
- Return Delinquency Accounts
- Daily Transcripts Registers (DTR's)
- Integrated Collection System (ICS) screens
- Automated Collection System (ACS) Web
- Examination Returns Control System (ERCS) screens

